The ISC Int'l Journal of Information Security
ISeCure

January 2023, Volume 15, Number 1 (pp. 1–58)
http://www.isecure-journal.org

Cloud Computing Threats, Vulnerabilities and Countermeasures: A State-of-the-Art

Suryateja S. Pericherla [1,*]
[1] *Deptartment of Computer Science Engineering, Vishnu Institute of Technology, Kovvada, India.*

ARTICLE INFO.

Article history:
Received: October 27, 2021
Revised: April 10, 2022
Accepted: August 1, 2022
Published Online: August 10, 2022

Keywords:
Cloud Computing Security, Cloud Computing Threats, Cloud Security State-of-the-Art, Cloud Security Taxonomy, Cloud Security Countermeasures, Cloud Computing Latest Threats

Type: Review Article

doi: 10.22042/ISECURE.2022.312328.718

dor: 20.1001.1.20082045.2023.15.1.8.5

ABSTRACT

Cloud computing created a revolution in the way IT organizations and IT teams manage their internal digital resources and workloads. One major drawback or limitation of cloud computing, among others, is security. Cloud computing is plagued by a plethora of threats and vulnerabilities, with new ones being identified from time to time. Year by year, minor to significant security incidents are reported across the globe. To the best of my knowledge, no research artifact in the recent past covers the recent advancements in cloud computing security. To address this issue, this paper provides an analysis of the literature in the past few years related to cloud computing security. Taxonomy related to cloud computing threats and vulnerabilities is provided by extending threats proposed by Cloud Security Alliance, which can educate cloud users and guide cloud providers to strengthen or audit their security policies and practices. Finally, state-of-the-art countermeasures and a classification of solutions to safeguard the cloud against different threats are also provided.

1 Introduction

Cloud computing is defined as a computing model which provides a dynamic, self-configurable pool of resources, available on-demand and accessible anywhere through the Internet [1]. Since its inception, organizations are gradually migrating their workloads to the cloud to embrace its advantages that significantly save their capital expenditure. The advantages of cloud computing include elasticity, ubiquitous access, a pay-per-use cost model, and others. Cloud computing offers three deployment models, namely, public cloud, private cloud, and hybrid cloud. In a public cloud, the Cloud Service Providers (CSPs) offer their infrastructure to the public or host software developed by third-party organizations, which will be accessed by the users. A public cloud thus hosts many users who can access the cloud resources simultaneously. In a private cloud, the cloud resources are reserved for a user or organization. The reserved resources are not shared with other users, thereby providing more security. In a hybrid cloud, the user or organization integrates services from multiple CSPs. An organization utilizing a hybrid cloud involves a strategy of dispatching workloads among the cloud resources that belong to different CSPs.

A major hindrance to the adoption of cloud computing is the security of infrastructure, applications, and data available or stored in the cloud. In a survey conducted by Oracle [2], the majority of the respondents conveyed that they had experienced security events due to confusion over the shared responsibility security model, and the top threats they were concerned about were email phishing, email credentials compromise, and ransomware. According to a recent survey

* Corresponding author.
Email address: suryatejapericherla@gmail.com
ISSN: 2008-2045

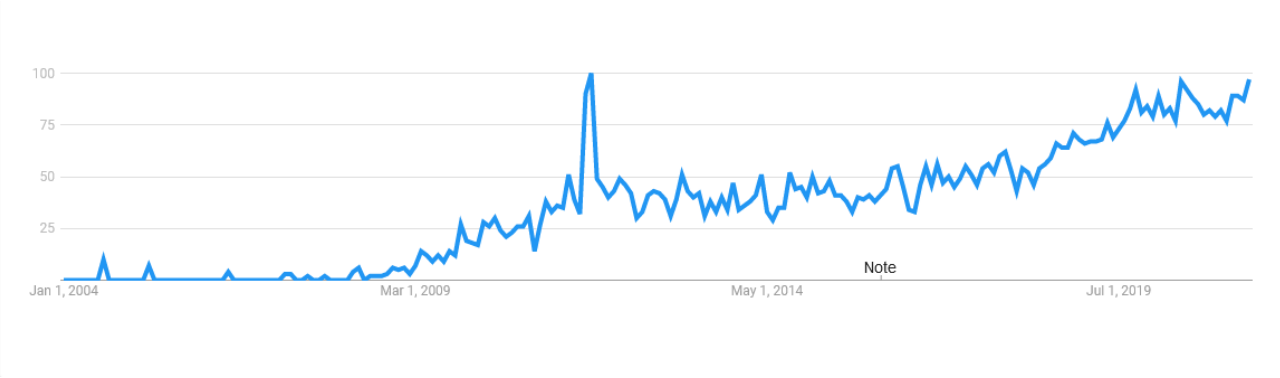

Figure 1. Google trends result for the term "Cloud Computing Security"

conducted by Netskope [3], the major concerns regarding cloud security were data privacy/confidentiality, data loss/leakage, fraud, and accidental exposure of credentials. Also, a major portion of the respondents feels that there is a high risk of security breaches in cloud IT environments when compared to on-premise IT environments. This is due to the lack of transparency in security measures employed by the CSPs and negligence in implementing security measures by cloud users. Apart from security, organizations also have to be concerned with operational headaches like compliance, lack of qualified staff, and setting consistent security policies. There are many threats and vulnerabilities in cloud computing with different levels of severity. Based on the survey [3], the biggest security threats in public clouds are insecure interfaces/Application Programming Interfaces (APIs), misconfiguration of cloud platforms, and unauthorized access. Since the inception of cloud computing, researchers from academia and industry and organizations like Cloud Security Alliance (CSA), Internet Engineering Task Force (IETF), and National Institute of Standards and Technology (NIST) led many efforts for improving various aspects of security in cloud computing. The interest of researchers in cloud computing security can be visualized from Google Trends, as shown in Figure 1.

1.1 Motivation

In the literature related to cloud computing security, the latest state-of-the-art research article was published around the year 2014 [4]. Since then, many research articles have been published to enhance the security of cloud computing. To the best of my knowledge, there is no current state-of-the-art covering various solutions for mitigating cloud threats. Also, there was no clear discrimination between threats and vulnerabilities in the research articles available in the literature. This provided motivation for conducting a literature study of the research conducted after 2014. A total of 300 articles from various repositories like ACM, Elsevier, IEEE, and Springer were collected based on the keywords cloud security, cloud computing security, and cloud computing threats and vulnerabilities. Around 11 articles from years before 2014 were also included based on their significance toward cloud computing security. The year-wise distribution of articles collected is shown in Table 1. The majority of the research articles were published in IEEE and Elsevier. This is evident from the bar graph shown in Figure 2.

Table 1. Year-wise distribution of research articles

Year	ACM	Elsevier	IEEE	Springer	Grand Total
2009	1				1
2011			1	1	2
2012	1	1		3	5
2013	1			2	3
2014	4	2		1	7
2015	1	3	1	5	10
2016	7	6	21	6	40
2017	2	9	24	3	38
2018	2	12	12	5	31
2019	1	4	4	6	15
2020	1	11	7	3	22
2021	0	2	2	5	9
Grand Total	**21**	**50**	**72**	**40**	**183**

1.2 Contributions

The major contributions of this survey are as follows:

- Analysis of literature related to cloud computing security after 2014. To the best of my knowledge, there is no such effort that provides a systematic mapping between threats and vulner-

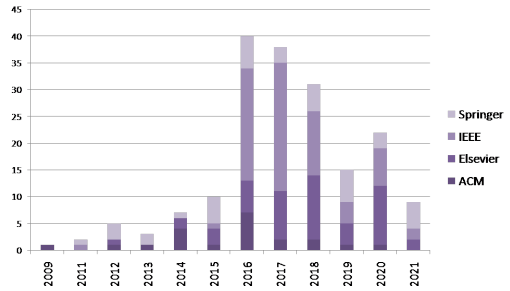

Figure 2. Visualization of research articles distribution in various repositories

abilities, including the latest threats like Ransomware, Spectre and Meltdown, and unprotected IoT devices that are essential for future researchers and cloud stakeholders.

- A graphical taxonomy of cloud computing threats and vulnerabilities that can educate cloud users and guide cloud providers to strengthen or audit their security policies and practices.
- A state-of-the-art of countermeasures and classification of solutions to safeguard the cloud against different threats by studying existing literature.

2 Background

This section compares this research with other similar works in the literature, which is followed up by the analysis of existing literature and also presents a taxonomy of cloud computing threats and vulnerabilities.

2.1 Related Work

In this section, the work done in this paper is compared against similar existing works in the literature. A summary of the comparison is presented in Table 2. Although the focus is on the latest work, two major contributions were included from previous years. The tick mark (✓) denotes the presence of the respective theme/concept, and the cross mark (x) denotes its absence. Although many of the previous works proposed issues and challenges, they are not considered the same as threats and vulnerabilities, as they are different. None of the existing surveys considered the latest threats like ransomware, hardware vulnerabilities, and unprotected IoT devices.

Gonzalez *et al.* [5] presented an analysis of various security concerns related to cloud computing. Different security-related problems were identified and grouped into seven categories, namely, network security, data security, interfaces, governance, virtualization, compliance, and legal issues. There is no clear separation between threats and vulnerabilities, and the latest threats were not included. Hashizume *et al.* [6] presents an analysis of security issues in cloud computing. Different threats and vulnerabilities associated with cloud computing were identified and mapped. Different solutions or countermeasures have been explored and mapped with the associated threats and vulnerabilities. Inclusion of the latest threats was missing in this survey. Ali *et al.* [7] performed a survey on cloud computing opportunities and challenges. A taxonomy of cloud challenges was provided. The three main categories of cloud security challenges are communication security, architectural security, and contractual and legal aspects. Comprehensive state-of-the-art related solutions for cloud computing were described. This survey lacks mention of the latest threats. M. A. Khan [8] performed a survey on security issues in cloud computing. A taxonomy based on attacks was proposed. The main categories based on attacks are networks, virtual machines, storage, and applications. Threats and vulnerabilities were not mentioned, and the latest threats were not included. Different countermeasures based on attack categories were mentioned. Coppolino *et al.* [9] performed a survey of emerging threats and existing solutions related to cloud security. Cloud security issues and attack vectors were identified. Different attacks related to network, hardware, and hypervisor and existing solutions were described. The latest threats were not considered.

Ramachandra *et al.* [10] performed a survey on security in cloud computing. Implications and challenges across cloud deployment types and risks across cloud service types were mentioned. Although different vulnerabilities were mentioned, there is no clear separation between threats and vulnerabilities. There is no mapping between threats and vulnerabilities, and the latest threats like ransomware, specter and meltdown, and unprotected IoT devices were not included. A brief overview of solutions was presented but is not in a comprehensive manner. Singh *et al.* [11] performed a comprehensive survey on cloud computing security issues and challenges. Different threats based on Cloud Security Alliance (CSA) were described and mapped to cloud service models. A taxonomy of cloud security attacks and solutions was presented. Different issues related to cloud security and their solutions were described. This survey lacks mention of the latest threats. Basu *et al.* [12] performed a survey of challenges and solutions related to cloud computing security. Cloud security was evaluated based on three factors, namely, confidentiality, integrity, and availability. A taxonomy of the three factors and associated issues or requirements was provided. The latest threats related to cloud computing were not considered, and different existing solutions for threats

Table 2. Summary of related work comparison

S.No.	Ref.No.	Author(s)	Year	Extensive Survey	Taxonomy			Inclusion of latest threats like Ransomware, Spectre and Meltdown, IoT	Threat-wise state-of-the-art countermeasures
					Threats (T)	Vulnerabilities (V)	Mapping of T and V		
1	[5]	N. Gonzalez et al.	2012	✓	✓	✓	✓	x	x
2	[6]	K. Hashizume et al.	2013	✓	✓	✓	✓	x	✓
3	[7]	M. Ali et al.	2015	✓	x	x	x	x	x
4	[8]	M. A. Khan	2016	✓	x	x	x	x	x
5	[9]	L. Coppolino et al.	2016	x	x	x	x	x	x
6	[10]	G. Ramachandra et al.	2017	x	x	✓	x	x	x
7	[11]	A. Singh et al.	2017	✓	✓	x	x	x	✓
8	[12]	S. Basu et al.	2018	x	x	x	x	x	x
9	[13]	J. B. Hong et al.	2019	✓	✓	x	x	x	x
10	[14]	Kumar and Goyal	2019	✓	✓	✓	✓	x	x
11	[15]	Akshaya and Padmavathi	2019	✓	x	x	x	x	x
12	[16]	Alhenaki et al.	2019	x	✓	x	x	x	x
13	[17]	H. Tabrizchi et al.	2020	✓	✓	x	x	x	x
14	[18]	S. N. Mthunzi et al.	2020	✓	x	x	x	x	x
15	[19]	Mishra et al.	2020	x	✓	✓	x	x	x
16	[20]	Butt et al.	2020	x	✓	x	x	x	x
17	[21]	Maduji and Anu	2021	✓	✓	x	x	x	✓
18		This Paper		✓	✓	✓	✓	✓	✓

were not provided. Hong *et al.* [13] provided a comprehensive survey on attacks and threats in cloud computing. A three-way relationship between cloud threats, vulnerabilities, and attacks was established. Although this survey gives a comprehensive overview of various attacks that can be performed in a cloud, there is no mapping between the threats and the related vulnerabilities. Also, the latest threats are not considered.

Kumar and Goyal [14] presented a comprehensive review of cloud security threats, vulnerabilities, requirements, and countermeasures. The authors elaborated on twelve threats and eight vulnerability categories. They provided a mapping between the security requirements, threats, and vulnerabilities. A threat-wise mapping of countermeasures was not found, although a mapping between countermeasures and vulnerabilities was present. The latest threats were not mentioned. Akshaya and Padmavathi [15] presented a taxonomy of various kinds of attacks that can affect cloud resources. The authors provided various attacks and possible solutions at various levels of cloud computing. This work does not mention any threats, vulnerabilities, a mapping between threats and vulnerabilities, latest threats, and no threat-wise coun-

termeasures. Alhenaki *et al.* [16] presented a survey on different threats and possible attacks in a cloud computing environment. The threats are based on CSA's top threats. Attack-wise countermeasures were also presented. There was no mention of the latest threats, and vulnerabilities were also missing.

Tabrizchi and Rafsanjani [17] performed a survey on cloud computing security issues, threats, and solutions. A new classification of cloud security issues and challenges was proposed. The issues were classified into five categories, namely, security policies, user-oriented security, data storage, application, and network. Their work also proposes different threats associated with cloud computing security. There was no clear mapping between threats and vulnerabilities, and the latest threats were not included. Mthunzi *et al.* [18] provides a holistic cloud security taxonomy. Different existing cloud security taxonomies were surveyed and compared. Various taxonomies were proposed like taxonomy related to cloud players, taxonomy related to private cloud, taxonomy related to the public cloud, etc. We think that the proposed taxonomy is too complex despite being holistic. The latest threats were not available, and no existing solutions were presented. Mishra *et al.* [19] provided various threats and vulnerabilities associated with cloud web applications. The author's work is not general and is limited to only web applications. There is no mention of the latest threats in this work. Butt *et al.* [20] provided an analysis of cloud computing threats, attacks, and countermeasures that specifically used one or more machine learning algorithms. Authors had identified four attack categories, namely, network-based attacks, VM-based attacks, storage-based attacks, and application-based attacks. Threats were vaguely specified. The attack taxonomy given is not up to the mark. For example, insufficient due diligence was mentioned as an attack, but it is not. There was no mention of the latest threats. The given countermeasures are limited to machine learning ones. Maduji and Anu [21] identified several challenges related to cloud computing security and grouped them into categories, namely, network, data access, and virtualization. Based on the challenges, different countermeasures were also mentioned. There was no mention of threats, vulnerabilities, and the latest threats.

2.2 Analysis of Literature

A threat is an incident or an event that may cause loss or damage to an individual or organization, and a vulnerability is a weakness in the system that allows an attacker to exploit the threat. A general list of 17 threats in cloud computing was provided in previous work [22] and is presented in Table 3. The threats from here onwards will be referred to as T01, T02, etc. Possible vulnerabilities were also identified for each of the threats, and the information [23] is reorganized and presented in Table 4. The vulnerabilities from here onwards will be referred to as V01, V02, etc. A taxonomy of cloud computing threats and the associated vulnerabilities are shown in Figure 3.

The literature related to cloud computing security after 2014 was considered, and a total of 193 research articles were studied concerning the threats. The articles were grouped into three categories, namely model, implementation, and conceptual. The articles under the model category include an algorithm, framework, or design for addressing a threat or vulnerability. The articles under the implementation category provide a working prototype or a complete solution for addressing a threat or vulnerability. Finally, the articles under the conceptual category only describe a threat and associated factors or provide an experimental evaluation of previously existing works or discuss security-related concepts in cloud computing. The summary of the 193 articles, the category they belong to, and the threat(s) they address are presented in Table 5. The threats addressed by some of the articles are marked as unknown as it was not clear from the article what threats are being addressed. Articles that just describe the security-related concepts are marked as none in the threats addressed column. The threats are sorted based on the number of research articles addressing a particular threat, and the result is presented in Table 6. This information is also visualized through a bar graph, as shown in Figure 4. The percentage of research articles addressing a specific threat can be seen in Figure 5.

3 Solutions and Countermeasures: A State-of-the-Art

Each threat and the research articles addressing that threat, i.e., state-of-the-art solutions and countermeasures for a threat, are discussed below. The classification of all the solutions and countermeasures can be seen in Figure 6. After each category name, the number of solutions that fall into it is represented in between parentheses. The category Secure Approach/Framework/Model/Protocol includes all the solutions where the respective authors developed their algorithms or methods or a process as a countermeasure for the cloud computing threats. The majority of the solutions fall into the categories of Secure Approach/Framework/Model/Protocol, Cryptography, and Secure Authentication as can be deduced from the given figure. Threat-wise summary of the solutions is provided in the form of a table after each section given below.

Table 3. A list of threats in cloud computing

Threat No.	Threat Name	Description of the Threat
T01	Data Breaches	A data breach is the disclosure of sensitive information to unauthorized parties either intentionally or unintentionally
T02	Data Loss	Data loss is the unavailability of data due to software or hardware failure or due to natural disasters or man-made errors
T03	Malicious Insiders	A former employee, system administrator, or a business partner acting as a perpetrator in causing damage to the organisation or business
T04	Denial of Service (DoS)	An attack in which a system or service is made inaccessible to the legitimate users
T05	Vulnerable Systems and APIs	Vulnerabilities in the operating systems, APIs, or other middleware might lead to compromise of the subsystem or the entire system
T06	Weak Authentication and Identity Management	Weak key management schemes and poor access control mechanism leads to circumvention of the system security measures
T07	Account Hijacking	Stolen credentials of cloud users or operators may allow illegitimate users to use the cloud resources for nefarious purpose
T08	Shared Technology Vulnerabilities	As the cloud provides multi-tenancy, the vulnerabilities in virtual machines and hypervisor might allow the attacker to compromise all the users sharing the resources
T09	Lacking Due Diligence	A cloud consumer must periodically review the accreditations and standards followed by the cloud service provider
T10	Advanced Persistent Threats (APT)	An attack in which the perpetrator infiltrates the system and continuously monitors it for sensitive information
T11	Abuse of Cloud Services	Weakly configured cloud facilities and services can be used by malicious users to launch attacks on co-resident users
T12	A Lack of Responsibility	Cloud users are responsible for securing their application workloads in the cloud. Any negligence in doing so might lead to service unavailability or a data breach
T13	Insufficient Security Tools	Sophisticated attacks like DDoS cannot be mitigated to a full extent with the existing available open-source tools
T14	Human Error	The weakest link in security is the human element. A simple mistake by a system administrator might wreak havoc in the system
T15	Ransomware	A type of malware which compromises the availability of the system or service by encrypting the data and thereby making it unusable

Threat No.	Threat Name	Description of the Threat
T16	Spectre and Meltdown	The hardware level vulnerabilities that allows the attackers to access the co-resident users data or even compromise the hypervisor
T17	Unprotected IoT Devices	A misconfigured device might allow a perpetrator to access other devices in the network and thereby cause damage to the system by accessing sensitive information

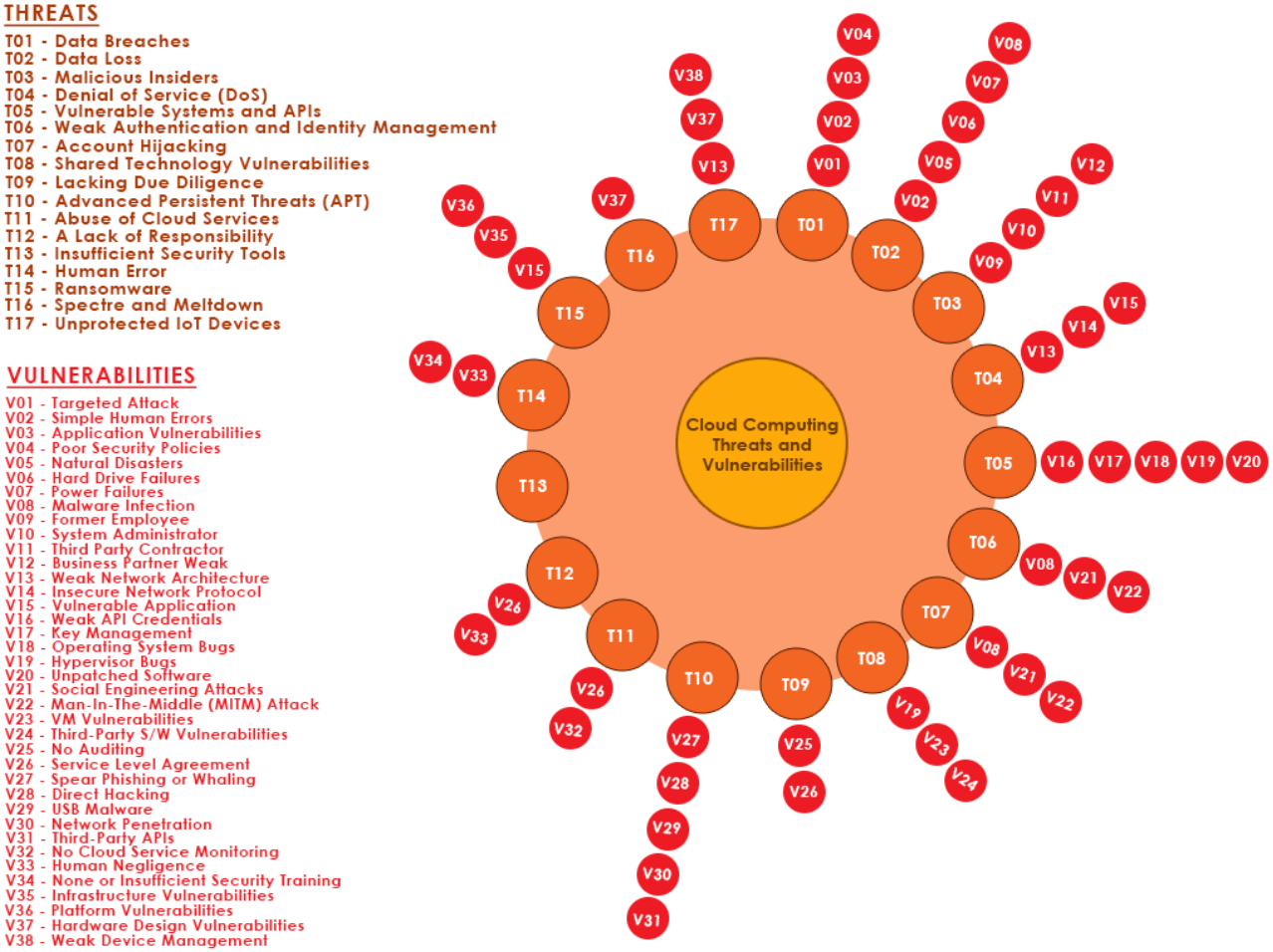

Figure 3. Taxonomy of threats and vulnerabilities in cloud computing

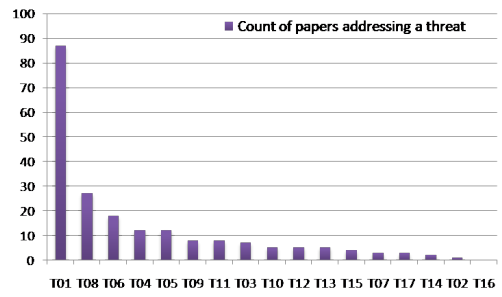

Figure 4. Bar graph visualizing the count of research papers addressing a threat

3.1 Data Breaches (T01)

A data breach is an unauthorized access to sensitive information. A great deal of research was conducted to solve this threat. Jaiman and Somani [28] proposed a model for preserving the privacy and security of data in the cloud. They proposed a secure order preserving scheme for encrypting the data inside the cloud. Their algorithm uses schemes such as shuffling, impurity insertion, and randomness in order-preserving functions. They demonstrated how their algorithm works by providing a secure sorting operation on given encrypted data. Aljafer *et al.* [29]

Table 4. A list of vulnerabilities in cloud computing

Vulnerability No.	Vulnerability Name	Related Threat(s)	Service Model(s) Susceptible to Vulnerabilities
V01	Targeted Attack	T01	SAAS, PAAS, IAAS
V02	Simple Human Errors	T01, T02	SAAS, PAAS, IAAS
V03	Application Vulnerabilities	T01	SAAS, PAAS, IAAS
V04	Poor Security Policies	T01	SAAS, PAAS, IAAS
V05	Natural Disasters	T02	IAAS
V06	Hard Drive Failures	T02	IAAS
V07	Power Failures	T02	IAAS
V08	Malware Infection	T02, T06, T07	IAAS
V09	Former Employee	T03	SAAS, PAAS, IAAS
V10	System Administrator	T03	SAAS, PAAS, IAAS
V11	Third Party Contractor	T03	SAAS, PAAS, IAAS
V12	Business Partner Weak	T03	SAAS, PAAS, IAAS
V13	Weak Network Architecture	T04, T17	SAAS, PAAS, IAAS
V14	Insecure Network Protocol	T04	SAAS, PAAS, IAAS
V15	Vulnerable Application	T04, T15	SAAS, PAAS, IAAS
V16	Weak API Credentials	T05	SAAS, PAAS, IAAS
V17	Key Management	T05	SAAS, PAAS, IAAS
V18	Operating System Bugs	T05	SAAS, PAAS, IAAS
V19	Hypervisor Bugs	T05, T08	SAAS, PAAS, IAAS
V20	Unpatched Software	T05	SAAS, PAAS, IAAS
V21	Social Engineering Attacks	T06, T07	SAAS, PAAS, IAAS
V22	Man-In-The-Middle (MITM) Attack	T06, T07	SAAS, PAAS, IAAS
V23	VM Vulnerabilities	T08	PAAS, IAAS
V24	Third-Party S/W Vulnerabilities	T08	PAAS, IAAS
V25	No Auditing	T09	SAAS
V26	Service Level Agreement	T09, T11, T12	SAAS
V27	Spear Phishing or Whaling	T10	SAAS, PAAS, IAAS
V28	Direct Hacking	T10	SAAS, PAAS, IAAS
V29	USB Malware	T10	SAAS, PAAS, IAAS
V30	Network Penetration	T10	SAAS, PAAS, IAAS
V31	Third-Party APIs	T10	SAAS, PAAS, IAAS
V32	No Cloud Service Monitoring	T11	PAAS, IAAS
V33	Human Negligence	T12, T14	SAAS, IAAS
V34	None or Insufficient Security Training	T14	SAAS, IAAS
V35	Infrastructure Vulnerabilities	T15	SAAS, IAAS
V36	Platform Vulnerabilities	T15	SAAS, IAAS
V37	Hardware Design Vulnerabilities	T16, T17	IAAS
V38	Weak Device Management	T17	SAAS, IAAS

Table 5. Summary of research articles analyzed

S.No.	Reference No.	Author(s)	Category			Threat(s) Addressed
			Model	Implementation	Conceptual	
1	[24]	M. Christodorescu *et al.*	✓	✓		T08
2	[25]	A. Bates *et al.*	✓	✓		T08
3	[26]	M. Kazim *et al.*	✓	✓		T08
4	[27]	Y. Zhang *et al.*	✓	✓		T08
5	[28]	V. Jaiman, G. Somani	✓			T01
6	[29]	H. Aljafer *et al.*			✓	T01
7	[30]	J. Szefer *et al.*	✓	✓		T03
8	[31]	W. Huang *et al.*			✓	Unknown
9	[32]	I. Papagiannis *et al.*	✓	✓		T14
10	[33]	X. Liao *et al.*	✓	✓		T11
11	[34]	M. Medhioub *et al.*			✓	T06
12	[35]	P. Anand *et al.*	✓	✓		T09,T12
13	[36]	X. Liao *et al.*	✓	✓		T11
14	[37]	U. Nagar *et al.*	✓			T01
15	[38]	Chaimae and Habiba	✓	✓		T01,T05,T06
16	[39]	K. Thimmaraju *et al.*	✓	✓		T08
17	[40]	A. Meryem *et al.*	✓	✓		T08,T10
18	[41]	D. Zissis, D. Lekkas	✓			T01
19	[42]	X. He *et al.*	✓	✓		T04,T05
20	[43]	Y. Yu *et al.*	✓	✓		T05
21	[7]	M. Ali *et al.*			✓	None
22	[44]	B. Cusack, E. Ghazizadeh	✓			T03,T05,T06
23	[45]	M. M. Potey *et al.*	✓	✓		T01
24	[46]	N. Vurukonda *et al.*			✓	T01
25	[47]	S. Iqbal *et al.*			✓	None
26	[8]	M. A. Khan *et al.*			✓	None
27	[48]	C. Saadi, H. Chaoui	✓	✓		T03,T04
28	[9]	L. Coppolino *et al.*			✓	None
29	[49]	A. Alabdulatif *et al.*	✓	✓		T01
30	[50]	L. T. Yang *et al.*	✓	✓		T01
31	[51]	K. Kritikos *et al.*	✓			T05,T08,T12
32	[11]	A. Singh, K. Chatterjee			✓	None
33	[52]	I. Indu *et al.*	✓	✓		T03,T06,T07
34	[53]	C. A. B. de Carvalho *et al.*			✓	T09
35	[54]	N. Kaaniche *et al.*			✓	T01
36	[55]	H. Cui *et al.*	✓	✓		T01
37	[56]	J. Cui *et al.*	✓	✓		T01
38	[57]	S. Challa *et al.*	✓	✓		T06,T17

39	[58]	W. Zheng *et al.*	✓	✓		T01
40	[59]	S. C. Sukumaran *et al.*	✓			T01
41	[60]	P. R. Kumar *et al.*			✓	T01
42	[61]	C. B. Tan *et al.*	✓			T01
43	[62]	A. A. Nayak *et al.*			✓	T01
44	[63]	M. Ali *et al.*	✓	✓		T01,T06
45	[64]	M. Amar *et al.*	✓			T01,T03,T04,T10,T11,T15
46	[65]	K. Fang *et al.*	✓	✓		T01,T08
47	[66]	N. Uddin *et al.*	✓	✓		T05
48	[67]	K. V Raipurkar *et al.*	✓			T01
49	[68]	H. Chen *et al.*	✓			T09
50	[69]	T. Lorünser *et al.*	✓			Unknown
51	[70]	P. Mishra *et al.*	✓	✓		T04,T08,T10,T11,T13,T15
52	[71]	D. Singh	✓			T01,T06
53	[72]	Y. Verginadis *et al.*	✓			T01
54	[73]	C. Prakash, S. Dasgupta			✓	None
55	[74]	S. Pereira *et al.*	✓	✓		T01,T06,T07
56	[75]	N. C. Paxton			✓	T01,T02,T07,T08
57	[76]	J. Lejeune *et al.*	✓	✓		T01,T06
58	[77]	A. Grover	✓			T01
59	[78]	B. Feng *et al.*	✓	✓		T01
60	[79]	B. Duncan *et al.*	✓			None
61	[80]	J. V. Chandra *et al.*	✓			T01,T10
62	[81]	V. Casola *et al.*	✓			T12
63	[82]	D. Bhamare *et al.*			✓	None
64	[83]	F. Ahamed *et al.*	✓	✓		T08
65	[84]	C. Liu *et al.*	✓	✓		T01
66	[85]	I. Nakouri *et al.*	✓	✓		T01,T06
67	[86]	H. Wei *et al.*	✓	✓		Unknown
68	[87]	S. Zhou *et al.*	✓	✓		T09
69	[88]	B. P. Gajendra *et al.*	✓	✓		T01
70	[89]	F. Gao	✓	✓		Unknown
71	[90]	S. Pisharody *et al.*	✓	✓		T01,T08
72	[91]	N. Amara *et al.*			✓	None
73	[92]	M. Kolhar *et al.*			✓	T01
74	[93]	D. C. Mumme *et al.*	✓	✓		T05,T08
75	[94]	C. Di Giulio *et al.*			✓	None
76	[95]	R. Nikam, M. Potey	✓			T01
77	[96]	X. Liu *et al.*	✓	✓		None
78	[97]	X. Gao *et al.*	✓	✓		T08
79	[98]	Y. Demchenko *et al.*	✓			Unknown
80	[99]	A. Alsirhani *et al.*	✓	✓		T01
81	[100]	V. Mahajan, S. K. Peddoju	✓	✓		T04,T10,T11,T15,T17
82	[101]	T. Orehovački *et al.*	✓			None
83	[102]	N. Paladi *et al.*	✓	✓		T01,T08

84	[103]	S. Bhattacharya *et al.*			✓	T15
85	[104]	C. A. B. De Carvalho *et al.*	✓			T01
86	[105]	N. Kaaniche *et al.*	✓			T12
87	[106]	M. A. Aman and E. K. Cetinkaya	✓	✓		T01
88	[107]	C. R. Taylor, C. A. Shue	✓	✓		T12,T17
89	[108]	K. Xue *et al.*	✓	✓		T04,T11
90	[109]	J. Ning *et al.*	✓	✓		T01
91	[110]	A. Shawahna *et al.*	✓	✓		T04,T11
92	[111]	J. Yao *et al.*	✓	✓		T01
93	[112]	G. Wang *et al.*	✓	✓		T01
94	[113]	H. Abrar *et al.*	✓	✓		None
95	[114]	I. H. Abdulqadder *et al.*	✓	✓		T05
96	[115]	S. Xu *et al.*	✓	✓		T01
97	[5]	N. Gonzalez *et al.*			✓	None
98	[116]	A. Basu *et al.*	✓	✓		Unknown
99	[117]	A. TaheriMonfared *et al.*	✓	✓		T01
100	[118]	R. Schwarzkopf *et al.*	✓	✓		T08
101	[119]	R. Denz, S. Taylor			✓	T08
102	[6]	K. Hashizume *et al.*			✓	None
103	[120]	U. Habiba *et al.*			✓	T06
104	[121]	N. Fotiou *et al.*	✓			T01,T06
105	[122]	Y. Yang *et al.*	✓			T01
106	[123]	R. Rai *et al.*			✓	None
107	[124]	M. I. Salam *et al.*	✓	✓		T05
108	[125]	S. Nagaraju	✓	✓		T06
109	[126]	J. Kim *et al.*	✓	✓		T01
110	[127]	K. Fan *et al.*	✓	✓		T01
111	[128]	L. Nkenyereye *et al.*	✓	✓		T05,T11
112	[129]	S. A. El-Booz *et al.*	✓	✓		T01
113	[130]	H. Hong *et al.*	✓			T01,T03,T06
114	[131]	J. Ullrich *et al.*			✓	T05,T13
115	[132]	N. Rakotondravony *et al.*			✓	T08
116	[133]	N. Singh, A. K. Singh			✓	T01
117	[134]	A. Razaque, S. S. Rizvi	✓	✓		T03
118	[135]	L. Wang, F. Liu	✓			T08
119	[136]	A. Abusitta *et al.*	✓	✓		T04
120	[137]	L. V. Silva *et al.*	✓	✓		T01
121	[138]	Moghaddam *et al.*	✓	✓		T09, T13
122	[139]	Jin *et al.*			✓	T08
123	[140]	Halabi and Bellaiche	✓	✓		T09
124	[141]	Levitin *et al.*	✓			T01, T08
125	[142]	Amato *et al.*	✓	✓		T08
126	[143]	Jakóbik *et al.*	✓	✓		T04, T09
127	[144]	Grzonka *et al.*	✓	✓		T06
128	[145]	Liu *et al.*	✓	✓		T01

129	[146]	Celesti *et al.*	✓	✓		Unknown
130	[147]	Al-Sharhan *et al.*	✓	✓		T01
131	[148]	Patil *et al.*	✓	✓		T08
132	[149]	Casola *et al.*	✓	✓		Unknown
133	[150]	Lei *et al.*	✓	✓		Unknown
134	[151]	Thirumalai *et al.*	✓	✓		T01
135	[152]	Ali *et al.*	✓			Unknown
136	[153]	Shakil *et al.*	✓	✓		T01
137	[154]	Wei *et al.*	✓	✓		T01
138	[155]	Mthunzi *et al.*			✓	None
139	[156]	Mishra *et al.*	✓	✓		T08
140	[157]	Wazid *et al.*	✓	✓		T06
141	[158]	Sun			✓	None
142	[159]	Namasudra *et al.*	✓	✓		T01
143	[160]	Singh *et al.*	✓	✓		Unknown
144	[161]	Huang *et al.*	✓	✓		T08
145	[162]	Wang *et al.*	✓	✓		T01
146	[163]	Hyun *et al.*	✓	✓		Unknown
147	[164]	Sun *et al.*	✓	✓		T13
148	[165]	El-Latif *et al.*	✓			T01
149	[166]	Sharma *et al.*	✓	✓		T01
150	[167]	Li *et al.*	✓	✓		T09
151	[168]	Hauser *et al.*	✓	✓		T01
152	[169]	Choi and Choi	✓	✓		Unknown
153	[170]	Devi *et al.*			✓	None
154	[171]	Yang *et al.*	✓	✓		T01
155	[172]	Atlidakis *et al.*	✓	✓		T05
156	[173]	Torkura *et al.*	✓	✓		T14
157	[174]	Kumari *et al.*	✓	✓		T06
158	[175]	Liu	✓	✓		T01
159	[176]	Halabi and Bellaiche	✓	✓		T09
160	[177]	Jin *et al.*	✓	✓		T08
161	[178]	Ge *et al.*	✓	✓		T01
162	[179]	Deshpande *et al.*	✓	✓		T08
163	[180]	Sharma *et al.*	✓			T01
164	[181]	Kakkad *et al.*	✓			T01
165	[182]	Singh and Pandey			✓	None
166	[183]	Cao *et al.*	✓	✓		T01
167	[184]	Bhushan and Gupta	✓	✓		T04
168	[185]	Vijayakumar *et al.*	✓	✓		T01
169	[186]	Sajay *et al.*	✓	✓		T01
170	[187]	Shen *et al.*	✓	✓		T01
171	[188]	Praveena and Rangarajan	✓	✓		T01
172	[189]	Mouratidis *et al.*	✓	✓		T13

173	[190]	Alavizadeh *et al.*	✓	✓	Unknown
174	[191]	Joseph *et al.*	✓	✓	T01
175	[192]	Tahir *et al.*	✓	✓	T01
176	[193]	Gangireddy *et al.*	✓	✓	T01
177	[194]	Vijayakumar *et al.*	✓	✓	T01
178	[195]	Indira *et al.*	✓	✓	T01
179	[196]	Achbarou *et al.*	✓	✓	T04
180	[197]	Le and Hoang	✓		Unknown
181	[198]	Namasudra	✓	✓	T01
182	[199]	Venkatraman and Geetha	✓	✓	T01
183	[200]	Hosam and Ahmad	✓	✓	T01
184	[201]	Rios *et al.*	✓	✓	T09
185	[202]	Kiran Kumar and Shafi	✓	✓	T01
186	[203]	Orobosade *et al.*	✓	✓	T01
187	[204]	Shyla and Sujatha	✓	✓	T04, T10
188	[205]	Ogiela	✓		T01, T06
189	[206]	Seth *et al.*	✓	✓	T01
190	[207]	Tariq *et al.*	✓		None
191	[208]	Shahzadi *et al.*	✓	✓	T01
192	[209]	Akinsanya *et al.*	✓		None
193	[210]	Zhang *et al.*	✓	✓	T01

Table 6. Count of research papers addressing a threat

Threat	T01	T08	T06	T04	T05	T09	T11	T03	T10	T12	T13	T15	T07	T17	T14	T02	T16
Count	87	27	18	12	12	8	8	7	5	5	5	4	3	3	2	1	0

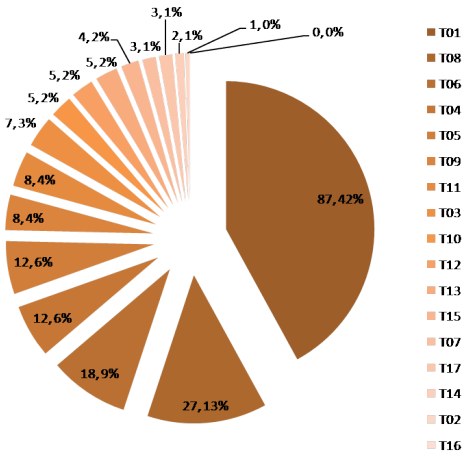

Figure 5. Percentage of Research Papers Addressing a Threat

discussed various approaches for protecting the data in a cloud environment. They provide a survey of existing solutions and discuss their advantages and shortcomings. A comparative analysis of encryption schemes like Advanced Encryption Standard (AES), Homomorphic Encryption, Attribute-Based Encryption (ABE), Proxy ReEncryption, and Hierarchical Identity Based Encryption (HIBE) was provided. Nagar *et al.* [37] proposed a new model named Collaborative Intrusion Detection Scheme (CIDS) for identifying non-detectable events like DDoS attacks. This approach places a NIDS on a virtual switch at the cloud entry point.

Individual VMs have an associated HIDS attached to them. Snort for Network Intrusion Detection System (NIDS) and the open source OSSEC for Host Intrusion Detection System (HIDS) were recommended. Chaimae and Habiba [38] presented an overview of the security issues in a cloud computing environment and proposed a new model which uses a virtual firewall and an intrusion detection and prevention system for providing security to cloud infrastructure against various attacks. The authors chose OSSEC for detecting intrusions. Various attacks like an attack against the integrity of files, attacks against websites, brute force

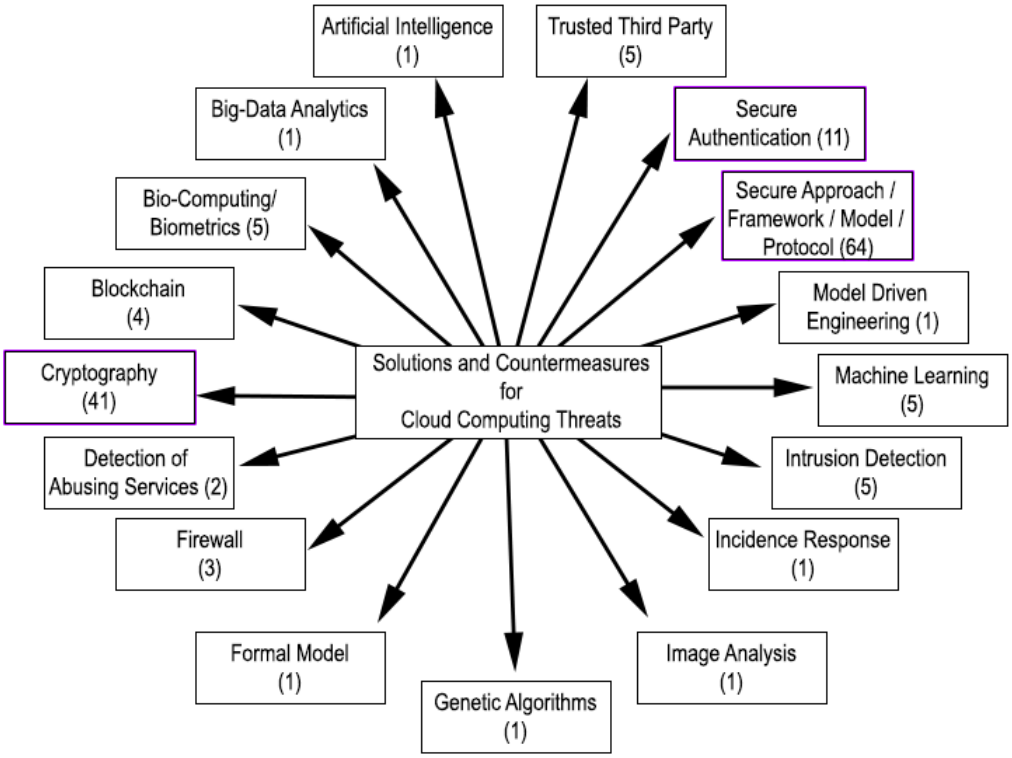

Figure 6. Classification of solutions and countermeasures for cloud computing threats

attacks, etc., were tested and detected successfully.

Zissis and Lekkas [41] described various security requirements of a cloud environment and proposed a solution that contains a trusted third party. This trusted third party preserves different security aspects of the cloud environment. The proposed solution involves Public Key Infrastructure (PKI), Single Sign On (SSO), and Lightweight Directory Access Protocol (LDAP) to preserve confidentiality, integrity, and authentication of data and communications. Potey *et al.* [45] proposed a solution for storing data securely in public clouds. They employed homomorphic encryption for encryption and decryption of data on the client-side. Data at rest in the cloud is always in an encrypted format so that third parties can't access it. The authors implemented their solution on AWS using the DynamoDB service. Vurukonda and Thirumala Rao [46] presented various issues related to data in a cloud computing environment. The issues given are data privacy and integrity, data recovery and vulnerability, improper media sanitization, and data backup. The authors also provided existing solutions for each of the mentioned data security issues. Alabdulatif *et al.* [49] proposed a novel framework for anomaly detection which is secure and privacy-preserving. The proposed solution is scalable. The framework contains trusted private servers which belong to an organization or company that collaborates with public servers in the cloud for anomaly detection. The communication between public servers and endpoints is encrypted using homomorphic encryption. Yang *et al.* [50] proposed a new algorithm for simplifying the computation of factoring large integers in the RSA algorithm. The novel algorithm is called the parallel block Wiedemann algorithm, which improves the efficiency of solving GF(2), a computation-intensive step in the General Number Field Sieve (GNFS) algorithm, which is by far considered the most efficient algorithm for factoring large numbers. Kaaniche and Laurent [54] provided a comparative analysis of various cryptographic techniques across different dimensions. Cryptographic mechanisms like ABE, proxy re-encryption, convergent encryption and homomorphic encryption were analyzed and the results were presented in a tabular format. Different remote data integrity checking mechanisms were also discussed. Cui *et al.* [55] proposed a new storage system that is attribute-based that provides secure provenance. The proposed solution guarantees the privacy of the stored data. Also, the solution provides fine-grained access control and allows dynamically adding users and revoking user access when needed. Cui *et al.* [56] developed a search protocol named Attribute-based Keyword Search with Efficient Revocation (AKSER). This can perform a search over encrypted data. The given solution can work with data produced by multiple owners and that need to be searched by several

users. AKSER achieves high efficiency in terms of user revocation.

Zheng *et al.* [58] proposed a secure and sustainable protocol for auditing cloud storage. The proposed protocol overcomes the high overhead involved in key updates at the local side by outsourcing partial key updates to a trusted Third Party Auditor (TPA). Also, the validity of the newly updated keys can be verified by the clients by using the BLS signature. Sukumaran and Mohammed [59] proposed a methodology for solving data security issues in mobile cloud computing. The methodology ensures data confidentiality and integrity by using a bio-computing solution that consists of polymerase chain reaction and primer generation. Kumar *et al.* [60] provided an overview of cloud computing and its components and described various data security issues and related challenges. Possible solutions to the security issues were also given. Tan *et al.* [61] presented a state-of-the-art of Proof of Retrievability (PoR), a scheme that ensures the integrity and availability of data stored in a cloud. Different issues and challenges regarding the implementation of PoR on cloud storage are discussed. Solutions to some of the issues were suggested. Nayak *et al.* [62] described various security-related issues of data stored in a cloud environment. They presented security issues as well as existing solutions for solving them. They also presented a model for providing secure access to data assets stored in the cloud by sending a One Time Password (OTP) for authenticating the users. Ali *et al.* [63] developed a new system for securing data in the cloud. The system was named Data Security for Cloud Environment (DaSCE) with a semi-trusted third party. This system provides key management, access control, and assured deletion of files. A working prototype was created and formally analyzed using High-Level Petri Nets (HLPN), Satisfiability Modulo Theories Library (SMT-Lib), and Z3 solver. DaSCE performance evaluation was conducted against the time taken during file upload and download. Amar *et al.* [64] proposed a mechanism that leverages big data processing on log files to detect different kinds of attacks on the resources in a cloud. Their detection mechanism is based on signature and anomaly detection techniques. MapReduce was used to process the log files, and then a frequent pattern growth approach was used to update the security rules.

Fang *et al.* [65] proposed a way to model security protocols in the cloud by using the industry-standard modeling language, UML 2.3. They also proposed a method that can automatically translate models developed using UML to pi-calculus specifications. Using ProVerif, a protocol verifier, the data secrecy and confidentiality of the security protocols were verified. The proposed approach was applied to a cloud security protocol named ConfiChair, and results were obtained. Raipurkar and Deorankar [67] proposed a model to secure customers' data in the cloud. The model uses Light Weight Directory Access Protocol (LDAP) to authenticate users, and the sensitive data is two-way encrypted. The model also provides data compression features. Singh and Verma [71] proposed a new framework to secure the data in the cloud. The proposed framework uses various servers arranged as a ring to authenticate the user to a server and vice versa by employing a station-to-station key agreement protocol. The integrity of the data is maintained using SHA-1, and confidentiality is maintained using AES. Verginadis *et al.* [72] presented a generic and formal model called Context-Aware Security Policy for ensuring the privacy and confidentiality of data in the cloud. This process guides PaaS developers through the process of persisting sensitive data in the cloud. The model enforces security-by-design and provides ontological templates for access control. Pereira *et al.* [74] presented a scheme named Storekeeper, a cloud aggregation service that allows file sharing between multiple users across multiple cloud storage platforms. This scheme preserves the confidentiality of the data that is being shared. To enable this, Storekeeper decentralizes the aggregation logic to the trusted client endpoints. Storekeeper addresses the issues of file update propagation, access control, user authentication, and key management. Paxton [75] described three security threats related to the cloud, namely data breaches, account hijacking, and multi-tenancy. Different issues and solutions related to these threats were given. Lejeune *et al.* [76] proposed two new algorithms named MIST and Malachi for protecting the user's data in the cloud by securing the authentication mechanism. The MIST algorithm allows for recovering account details effectively. Malachi algorithm provides a novel way to secure the login process of a user.

Grover and Kaur [77] proposed a new framework for securing the data before storing it in the cloud. It is a three-stage framework. In the first stage, the file to be uploaded is compressed. In the second stage, symmetric keys are generated and managed. In the third step, the file is encrypted and stored in the cloud. Feng *et al.* [78] developed a privacy-preserving protocol for auditing storage systems in the cloud. The protocol supports dynamic data operations and also provides bidirectional authentication and statistical analysis. The protocol also supports load distribution, which reduces the computational overhead by a large margin on the client-side. Error handling is also supported by the protocol. Chandra *et al.* [80] proposed a system for protection against advanced persistent

threats. The given solution used bilinear mapping and methods like reverse engineering. Also, the solution employs cryptographic concepts like Diffie-Hellman key exchange, El-Gamal encryption, and fuzzy logic. Liu *et al.* [84] proposed a Cloud Access Security Broker (CASB) based framework for data sharing and performing a search on encrypted data. Instead of delegating the search responsibility to the cloud provider, search indexes are built locally, and only identifiers of the ciphertext are pointed to in the cloud. Nakouri *et al.* [85] proposed a framework based on biometrics for securing data storage in the cloud. This framework was used to mitigate Man-in-the-Cloud (MitC) attacks. It also utilizes the concepts of chaotic maps and fuzzy extractors. This framework is implemented and was successful in distinguishing legitimate users from malicious users. Gajendra *et al.* [88] proposed a method for securing the data in transit in a cloud environment. This method depends on a trusted third party for authentication. Apart from that, Identity Based Encryption (IBE) algorithm is used for protecting the confidentiality of data.

Pisharody *et al.* [90] proposed a framework for detecting conflicts between flow rules in an SDN-based cloud environment. This framework is implemented on an OpenDaylight SDN controller. The conflict classification in traditional firewalls is extended to resolve conflicts in the SDN environment. Visualization is also provided for the administrator if any input is required. A proof-of-concept prototype is provided for demonstrating the framework's correctness, scalability, and feasibility. Kolhar *et al.* [92] performed a systematic review of different approaches to provide privacy and integrity of data in the cloud. They also analyzed different auditing solutions and described their strengths and weaknesses. Finally, they proposed possible areas to improve the auditing process. Nikam and Potey [95] proposed a solution for providing authentication and confidentiality for data stored in the cloud. This solution guarantees confidentiality by employing Ciphertext Policy-Attribute-Based Encryption (CP-ABE). Authentication is provided through two-way authentication. First, the user provides a static username and password. Second, a random token is generated using a QR code and is sent to the user as a One Time Password (OTP). By using a static password and the random token, the user is authenticated to access the data. Alsirhani *et al.* [99] proposed a scheme for ensuring the confidentiality of data stored in a cloud database. The scheme used various encryption algorithms to encrypt the database data and also fragments the data, and store it on multiple clouds, which are public clouds. Among these, one public cloud acts as a primary cloud, and the remaining clouds act as secondary nodes. This scheme was implemented and evaluated, and the results indicate that it is a secure approach with less performance overhead.

Paladi *et al.* [102] proposed a framework for securing data in IaaS clouds. The defined protocols provide data and operational security by supporting the trusted launch of VMs and by providing domain-based storage protection. Experimental results validate the proposed protocols. Trust is established by attesting to the host environment before launching the VM. Confidentiality of data in the cloud is achieved using encryption keys that are stored outside the IaaS domain. Carvalho *et al.* [104] proposed a solution that combines auditing, monitoring, and other methods to ensure the security of data stored in the cloud. Access Control Lists (ACLs) were used to provide the permissions of users and broadcast encryption. Key rotation methods were employed for reading and writing the keys. The cloud broker stores the metadata of files to allow only authorized users to access them. The cloud attestations are sent to a TPA for auditing purposes. Further, the proposed solution is evaluated using Colored Petri Nets (CPNs). M. A. Aman and E. K. Cetinkaya [106] proposed a system that secures the backup files stored in the cloud. The proposed system provides security, utility, and also performance. This scheme uses encryption intensity selection, which allows the user to select the level of encryption for encrypting their files. This scheme also provides secure deduplication and querying of encrypted data. Ning *et al.* [109] proposed a new system named CryptCloud+ with accountable authority and revocable CP-ABE features for securing cloud storage. This system also supports auditing and white-box traceability. The authors also described two misuse cases of the CP-ABE scheme, which are misuse of access credentials on the semi-trusted authority side and misuse on the cloud user side. Yao *et al.* [111] proposed a new scheme based on Searchable Symmetric Encryption (SSE) for performing searches over encrypted data stored in the cloud. This scheme uses cryptographic mechanisms like chameleon hashing and obfuscation techniques like indistinguishability obfuscation for concealing the user search patterns. This scheme generates random search tokens which cannot be traced back to the plain text query easily. This scheme's security is formally proved and was extensively experimented on.

Wang *et al.* [112] proposed a new scheme called IDCrypt for allowing users to perform searches over encrypted data in the cloud. This scheme employs SSE, which improves the efficiency of search and security strength of searchable encryption using symmetric cryptography. Challenges for sharing the data and searching over multiple indexes securely were

also described. For addressing these issues, a token-adjustment scheme to preserve search over multiple indexes and a secure key sharing scheme employing Identity-Based Encryption (IBE) and Public Key Encryption (PKE) was proposed. Xu *et al.* [115] proposed a data-sharing scheme that is secure and which provides efficient fine-grained access control. This scheme allows dynamic user groups to share and get fine-grained access control over data by using attributes of data to enforce access policies, allowing key generation centers to update user details and offloading computation-intensive tasks to untrusted CSPs without requiring any delegation key. Taheri-Monfared and Jaatun [117] proposed a new approach for incidence response, where a component in the IaaS cloud has been compromised. NIST guidelines for incidence response were considered as an input, and new steps were added to create a new approach. This approach can provide containment, eradication, and recovery after an incident. A fake component is also introduced in the experimentation conducted using an OpenStack cloud environment. Fotiou *et al.* [121] proposed a solution for access control delegation to a trusted third party known as Access Control Provider (ACP). This solution preserves the privacy of cloud users concerning cloud providers and overcomes the complexity and lock-in weaknesses in existing access control mechanisms. This solution also offers flexibility to data owners in switching among cloud providers or using multiple clouds at the same time. Yang [122] proposed a new scheme known as Attribute-Based Searchable Encryption with Synonym Keyword search function (SK-ABSE) that allows multiple users to search over an encrypted file stored in a cloud environment. This scheme provides flexible search authorization over encrypted data, and this process preserves the privacy of users. Kim and Nepal [126] proposed a secure cloud storage system that allows multiple users to access and perform updates on encrypted data. This system allows data owners to grant flexible and fine-grained access control over the encrypted data. This system also allows efficient revocation of access to data to invalid users without actually moving the data. Their scheme utilizes Attribute-Based Encryption to support access control policies. A system administrator has the flexibility to revoke user permissions either by updating the revoked user's list or by updating an epoch counter.

Fan *et al.* [127] proposed a protocol for controlling access to data in the cloud environment. The protocol named Multi Usage Control (MUCON) uses encryption, and digital watermarking technologies to provide flexible, feature binding and offline control to the data in the cloud. El-Booz *et al.* [129] provided a secure way to access the data stored in the cloud. Their scheme strengthens the authentication of cloud users by using two techniques known as Time-Based OTP (TOTP) and Automatic Blocker Protocol (ABP) for blocking data access to TPAs who might compromise with the CSP to reveal the exposed data to the cloud users. Hong and Sun [130] proposed a new scheme named Key Policy Attribute Based Signature with Untrusted Authority and Traceability (KP-ABS-UT) to safeguard the data stored in the cloud. This scheme prevents attribute authorities from compromising the security of the cloud by forging the signatures to impersonate cloud users. In this scheme, the user's private key is composed of the user and the attribute authority, thereby preventing the attribute authority from having complete control over the user's data. Singh *et al.* [133] provided a systematic review of different methods and approaches for data privacy in the cloud. Different approaches were divided into four categories, namely, privacy by cryptography, privacy by ranking, privacy by anonymization, and privacy by probability. A taxonomy and a comparative analysis are given for different privacy-preserving approaches. Silva *et al.* [137] proposed a software architecture that provides security and preserves the privacy of users during data aggregation in IoT and cloud computing scenarios. This architecture was validated by implementing it in smart grid applications. This architecture uses an encryption technique named homomorphic encryption and hardware security extensions like Intel SGX.

Levitin *et al.* [141] proposed a model for protecting the data of cloud users from co-residence attacks performed by attackers residing on the same virtual machines. The solution proposed involves dividing the data of users into multiple blocks and replicating them on different VMs. Liu *et al.* [145] proposed a scheme for securing file sharing among a group of users in the cloud. The name of the scheme is Multi-Conditional Proxy Broadcast Re-encryption (MC-PBRE). In this scheme, the users can transfer the right to decrypt the file and also control decrypting permissions among a group of users. The proposed scheme is collusion attack resistant. Al-Sharhan *et al.* [147] proposed a new model and framework for securing the eHealth systems. The proposed model secures the health records of patients by using a Virtual Private Cloud (VPC), elastic load balancing, and a Virtual Private Network (VPN) gateway. Thirumalai *et al.* [151] proposed a scheme named Efficient Non-shareable Public Key Exponent Secure Scheme (ENPKESS), which utilizes a non-linear diophantine equation to achieve security against side-channel and timing attacks. This scheme involves three stages for encryption and two stages for decryption. Authors say that their scheme is well suited for cloud computing and IoT applica-

tions. Shakil *et al.* [153] proposed a system named BAMHealthCloud for managing healthcare data in the cloud. Their system uses behavioral biometric authentication for securing health data. Authors trained biometric signatures using the Hadoop MapReduce framework and resilient back propagation neural networks. Wei *et al.* [154] employed a distributed virtual machine agent model in the cloud, which enables tenants in the cloud to cooperate for trusted data verification. Authors integrated blockchain technology for data integrity, and for consensus, they used the virtual machine proxy model. Namasudra *et al.* [159] proposed a novel DNA encryption scheme for protecting data in the cloud computing environment. A 1024-bit secret key is generated based on different factors like the user's attributes, MAC address, ASCII value, and others. Wang *et al.* [162] proposed a new approach named Comprehensive Trustworthy Data Collection (CTDC) for sensor-cloud systems. They considered three types of trusts, namely, direct trust, indirect trust, and functional trust, for evaluating the trustworthiness of both mobile sinks and sensors. Simulations conducted by authors show that CTDC identifies malicious nodes and improves data collection performance.

El-Latif *et al.* [165] proposed a new quantum steganography protocol for securing the data transmitted to stored in the cloud. The hash function was used to authenticate the secret messages. The proposed protocol is resistant to different attacks and doesn't consume additional channels for transferring data. Sharma *et al.* [166] presented a multi-level encryption and decryption approach for securing the data in the cloud. The authors used the RSA algorithm and AES algorithm for performing multi-level encryption and decryption. Hauser *et al.* [168] developed an open-source platform called GridCloud for gathering real-time data and sharing it across jurisdictions that control the interconnected grid. The platform employs cryptographic primitives for securing data and software-mediated redundancy to overcome failures. Yang *et al.* [171] proposed a framework named AuthPrivacyChain, which provides privacy protection using blockchain. The node address in the blockchain is used as an identity, and at the same time, the access control permissions are defined. This framework prevents illegal access to resources and protects privacy. Liu [175] proposed a public-key encryption scheme that is secure against related randomness attacks. This scheme utilizes a one-way function with weak Related Key Attacks (RKA) security and obfuscation. Ge *et al.* [178] proposed a scheme with symmetric key-based verification for keyword search over dynamically encrypted cloud data. This scheme introduces a novel Accumulative Authentication Tag (AAT) based on symmetric-key cryptography. This tag is updated when dynamic operations are performed on the cloud data. For efficient data update, the authors introduced a new table called the search table. Sharma *et al.* [180] proposed a hybrid cloud framework that uses Li-Fi communication technology for IoT. The framework utilizes a local cloud for achieving more efficiency, security, reliability, and reducing delay and bandwidth cost. Kakkad *et al.* [181] proposed a model for protecting images in a cloud environment. Their model provides image authentication, which is done in two stages. First, the image is compressed using the standard discrete wavelet transform method. Second, the compressed image is encrypted using SHA and blowfish algorithms. Cao *et al.* [183] proposed a secure eHealth system for securing the EHRs in the cloud using blockchain technology. The system allows outsourcing of EHRs only by authenticated participants with the help of blockchain. The integrity of EHRs is achieved through blockchain. Vijayakumar *et al.* [185] proposed a technique that uses searchable encryption and proxy re-encryption techniques for securing patient health records in a cloud environment. Their approach allows only authorized agents to access patients' data temporarily.

Sajay *et al.* [186] proposed a hybrid approach for securing the data in the cloud. Authors combined homographic encryption and blowfish encryption algorithms for enhancing cloud security. Shen *et al.* [187] proposed a scheme for securing data in the cloud. Their scheme uses AES symmetric encryption and improved identity-based proxy re-encryption algorithms for achieving fine-grained control over the data. This scheme is applicable for heterogeneous cloud systems. Praveena and Rangarajan [188] proposed a model based on an enhanced C4.5 machine learning algorithm for securing data in the cloud. The model also uses a new deduplication algorithm and a new access control mechanism for securing the data. Joseph *et al.* [191] proposed a multimodal authentication system using fingerprint, iris, and palm traits for securing data in the cloud. The proposed system uses image processing techniques for pre-processing, feature extraction, and normalization. The extracted features are used to generate a secret key in two stages. Tahir *et al.* [192] proposed a new model named CryptoGA based on a Genetic Algorithm (GA) for dealing with data integrity and privacy issues in the cloud. GA was used to generate the keys, which are used along with a cryptographic algorithm. Gangireddy *et al.* [193] proposed a model for protecting the data in the cloud. This model uses k-medoid clustering was used for clustering the secret information. An enhanced blowfish algorithm was used for the encryption and decryption

of data. Vijayakumar and Umadevi [194] proposed a multi-level micro access algorithm for privacy preservation in the cloud. The data were indexed into multiple levels, and access to the data was restricted using a profile. The owner of the file can encrypt it using his/her key. To prevent malicious access to the data Micro Access Trust Weight (MATW) was used. Indira *et al.* [195] proposed round key and random key-based encryption mechanisms for improving security in a cloud environment. Namasudra [198] proposed a scheme for access control for securing access to the data in a cloud environment. The proposed scheme uses ABE for encrypting the data using the attributes of the users. Identity-based Timed Release Encryption (IDTRE) was used to encrypt the decryption key. Venkatraman and Geetha [199] proposed a novel algorithm named Specialized Steganographic Image Authentication (SSIA) for securing images stored in a cloud environment. The algorithm uses a combination of blowfish algorithm and genetic operators to provide two-stage encryption.

Hosam and Ahmad [200] proposed a hybrid solution for tackling the key management problem. The solution involves AES, ECC, and steganography for distributing the keys effectively in a cloud environment. Kiran Kumar and Mahammad Shafi [202] proposed a mechanism focusing on the integrity and privacy of data stored in a cloud computing environment. The proposed mechanism uses a modified RSA algorithm. Orobosade *et al.* [203] proposed a hybrid encryption algorithm for safeguarding the data in the cloud. This scheme uses AES as the first stage of encryption for securing the privacy of data before storing it in the cloud. The second stage involves ECC with AES key for achieving confidentiality of the data stored in the cloud. Ogiela [205] proposed a cognitive authentication approach that involves cognitive CAPTCHA codes for providing access to the data in the cloud. The proposed approach allows only domain experts who are trusted by solving novel cognitive CAPTCHA codes. Seth *et al.* [206] proposed a framework that involves dual encryption and data fragmentation techniques for securing cloud data. The proposed framework addresses the issues of integrity, confidentiality, and authentication. Shahzadi *et al.* [208] proposed Adaptive Neural Fuzzy Interference System (ANFIS) for resolving risks in cloud computing. It also uses Sugeno control methods for the protection of data against uncertainty from randomness. Zhang *et al.* [210] developed a Fog-based Detection System (FDS) for detecting data attacks in the sensor cloud. The authors defined three scenes based on fog computing and trust evaluation methods. The summary of solutions for T01 is given in Table 7.

3.2 Data Loss (T02)

Unavailability of the data or damage of data due to hardware or software failures or due to natural calamities like floods, typhoons, etc., or due to man-made errors is called data loss. Although the effect of the data loss threat is catastrophic, it seems that no major research was conducted after 2014 to solve this issue in cloud computing. A solution to this might be using a multi-cloud or a hybrid cloud along with replication.

3.3 Malicious Insiders (T03)

A former employee or a disgruntled employee, system administrator or business partner may disclose critical or sensitive business secrets to third-party organizations, or competitors causing loss or damage to the business. Malicious insiders are difficult to detect and handle. Szefer *et al.* [30] proposed a set of novel cyber defense strategies that mitigate physical attacks in data centers. Authors assume that the physical attackers are constrained by the data center's physical layout and other features. The proposed strategies can be activated on a physical attack. Some of them can even take effect even before the actual attack occurs. The key contributions of this paper are: 1) A defense strategy to protect against physical attacks by using VM cloning, 2) Analysis of four defense strategies for physical attacks, and 3) Standardize the ideas and concepts needed to reason about insider attacks carried out in data centers or other distributed networked systems. Cusack *et al.* [44] proposed a solution for the risk of identity theft involving single sign-on (SSO) authorization in a cloud computing environment. The solution uses federated identity management, and the solution provides a balance between the security of the service, disclosure risk, and user risk. Saadi and Chaoui [48] proposed and implemented a cloud architecture with security tools like a honeypot, honeynet, and honeyd along with Intrusion Detection System (IDS). These tools were used for behavioral analysis of traffic containing genuine and illegitimate traffic. The authors were successful in detecting some of the security attacks. Indu *et al.* [52] proposed an extension to Security Assertions Markup Language (SAML) technology to secure the communication between cloud provider, cloud server, and an identity provider. The proposed extension includes token-based authentication that is flexible and scalable. This solution provides fine-grained access to cloud web services. Amar *et al.* proposed a mechanism as described in Section 3.1. Hong and Sun proposed a new scheme as described in Section 3.1. Razaque and Rizvi [134] proposed a Privacy-Preserving Model (PPM) for auditing all the stakeholders in the cloud.

Table 7. T01 solutions summary

Author(s)	Solution Category	Summary	Limitations/Future Scope
Jaiman and Somani [28]	Cryptography	Order preserving scheme for performing operations on encrypted data stored in the cloud	Computation overhead Doesn't prevent statistical attacks Vulnerable to chosen plaintext attack
Nagar *et al.* [37]	Intrusion Detection	A framework for securing data in the cloud using Collaborative Intrusion Detection	A single point of failure due to central coordinator Not implemented and tested
Chaimae and Habiba [38]	Intrusion Detection and Firewall	An architecture for securing data in the cloud using virtual firewall and IDS/IPS	No event correlation among he HIDS components Absence of NIDS Not tested in a commercial cloud environment
Zissis and Lekkas [41]	Trusted Third Party and Cryptography	A trusted third party for securing the cloud environment Uses cryptography along with SSO and LDAP for ensuring confidentiality, integrity and authentication	Availability of the system and quality of service can be improved Trusted third party can be a single point of failure A scheme for searching over encrypted data is needed to improve the performance of the system
Potey *et al.* [45]	Cryptography	Stores data on the cloud in encrypted form using fully homomorphic encryption Uses Amazon's DynamoDB as a datastore User computations are performed on the encrypted data	Size of cipher text can be reduced for efficient data processing Efficient algorithms for searching and querying over encrypted data can be employed Not tested against security attacks
Alabdulatif *et al.* [49]	Cryptography and Machine Learning	A lightweight homomorphic encryption scheme that ensures data security and privacy Granular anomaly detection using fuzzy c-means clustering over operations on encrypted data Experimentation on Google Cloud Platform	Computation overhead can be reduced More operations can be supported by the homomorphic encryption technique The private server can be a single point of failure
Yang *et al.* [50]	Secure Approach	A novel parallel block Wiedemann algorithm for improving the computational efficiency of GNFS algorithm	Parallel performance of the block Wiedemann algorithm can be improved
Cui *et al.* [55]	Cryptography	An attribute-based cloud storage system that provides data provenance	Computational overhead can be reduced

Author(s)	Solution Category	Summary	Limitations/Future Scope
Cui *et al.* [56]	Cryptography and Trusted Third Party	An attribute-based keyword search scheme with efficient revocation A multi-certificate authority supports multiple data owners and multiple users	Dynamic searchable encryption can be explored Not tested on commercial cloud
Zheng *et al.* [58]	Secure Protocol and Trusted Third Party	A secure cloud storage auditing protocol that supports client key updates	Trusted third party can be a single point of failure Not implemented on physical H/W
Sukumaran and Mohammed [59]	Bio-computing and Cryptography	A bio-computing solution that provides data security Based on polymerase chain reaction and primer generation	No practical implementation
Nayak *et al.* [62]	Secure Model	Various schemes for securing data in the cloud Using bilinear maps for self-destructive mechanism Using OTP (One Time Password) for preventing access to the data	Although the OTP method provides security, it is not autonomous
Ali *et al.* [63]	Trusted Third Party	A semi-trusted third party scheme for that provides key management, access control, and assured file deletion	Can be extended for group data transfer and secure data forwarding
Amar *et al.* [64]	Big Data Analytics	A log file centralization approach for anomaly detection Frequent pattern growth approach which mines frequent patterns for detecting attacks	Centralized log collection and analysis can be a single point of failure Effort to reduce computational overhead can be investigated
Fang *et al.* [65]	Formal Modal	A formal analysis model which uses UML diagrams to verify the security protocols used in the cloud	Can be applied on other types of cloud-based applications
Raipurkar and Deorankar [67]	Cryptography	A secure approach using LDAP, data compression and encryption algorithms SHA-512 was used for key generation and AES was used for encryption	No practical implementation
Singh and Verma [71]	Secure Authentication and Cryptography	A secure approach for protecting the confidentiality and integrity of the data stored in cloud Uses station-to-station key agreement protocol for authentication, SHA-1 for integrity, and AES for data confidentiality	SHA-1 is not a secure algorithm Availability decreases when the ring connection for servers is disrupted

.

Author(s)	Solution Category	Summary	Limitations/Future Scope
Verginadis *et al.* [72]	Formal model	Context-aware security policy model for enhancing the confidentiality and privacy of sensitive data	Mechanisms that uses this modelling framework need to developed
Pereira *et al.* [74]	Secure Model	A privacy-preserving cloud aggregation service named Storekeeper that allows users to share files in a multi-cloud storage environment	Not tested in a commercial cloud environment
Lejeune *et al.* [76]	Secure Approach	MIST and Malachi algorithms for securing users' data by protecting their accounts The MIST algorithm is pre-defined question and answer based The Malachi algorithm involves users to enter a password and their own question and answers while logging into the account	Malachi algorithm was not yet tested and further improvements are possible
Grover and Kaur [77]	Secure Framework and Cryptography	A framework for securing the data and reducing the space occupied by the data in the cloud	The key management can be more secure Parallel encryption for larger files to improve the performance
Feng *et al.* [78]	Secure Protocol	A privacy-preserving auditing protocol that allows external auditors for auditing the client without knowledge of the actual data stored in the cloud	Need of more effective verification schemes Higher computational load for larger files at higher security level Efficiency of dynamic operations can be improved
Chandra *et al.* [80]	Cryptography	A self-destructive mechanism using bilinear mapping and reverse engineering methods to protect against advanced persistent threats Use of cryptographic concepts like Diffie-Hellman, ElGamal	Not implemented and test in a commercial cloud environment
Liu *et al.* [84]	Secure Framework	A security broker-based framework for searching over encrypted data and data sharing	Applications that need a broker has to be recognized Key management and exchange should be secure The broker can be a single point of failure
Nakouri *et al.* [85]	Biometrics	A biometric-based approach for preventing attackers from launching MitC attacks on cloud storage	Replay attacks are possible Availability of biometric H/W
Gajendra *et al.* [88]	Secure Authentication and Cryptography	A secure approach that employs IDE for encryption and MD5 algorithm for authentication	MD5 is a non-secure algorithm and is not safe

.

Author(s)	Solution Category	Summary	Limitations/Future Scope
Pisharody *et al.* [90]	Secure Framework	A secure framework named Brew, which detects conflicts in the flow rules in a SDN-based cloud environment which leads to secure implementation of policies for preventing information leakage	Performance can be improved through parallel workload sharing The flow rules can be optimized by varying the position of rules and prioritizing them Visualization module can be extended by providing support for scalability The framework can be extended to support diverse controllers
Nikam and Potey [95]	Secure Authentication and Cryptography	A secure solution using CP-ABE for confidentiality and multi-factor authentication for securing data in the cloud	Current multi-factor authentication technique uses only knowledge and possession factors Biometrics can also be included to improve the security
Alsirhani *et al.* [99]	Cryptography	A secure approach that utilizes encryption to improve database confidentiality in the cloud	Communication and processing overheads can be reduced
Paladi *et al.* [102]	Secure Framework	A framework which allows trusted launch of VMs and provides data storage security Implemented as a prototype based on the architecture of a EHR system	The trust model in the communications and data geolocation can be strengthened Not implemented and tested in a commercial cloud environment
Carvalho *et al.* [104]	Secure Framework	A solution that combines auditing, monitoring, and other methods to ensure the security of data stored in the cloud	The broker can be a single point of failure Does not address all types of security violations The storage service can be improved Vulnerable to collusion attacks
M. A. Aman and E. K. Cetinkaya [106]	Secure Framework	An approach for securing the backup files stored in the cloud Uses encryption intensity selection, which allows the user to select the level of encryption for encrypting their files	Higher processing time with systems that does not contain many duplicates Not implemented and tested in a commercial cloud environment
Ning *et al.* [109]	Cryptography	A system named CryptCloud+ with accountable authority and revocable CP-ABE features for securing cloud storage It supports auditing and white-box traceability	Black-box traceability can be used instead of white-box traceability as the former is more stronger than later Multiple authorities can be used instead of a single authority to increase the trust A secure multi-party protocol can be used for computation in the presence of multiple attackers Instead of centralized trust, it can be decentralized by including multiple authorities This system can be extended to provide partial and fully public traceability

.

Author(s)	Solution Category	Summary	Limitations/Future Scope
Yao *et al.* [111]	Cryptography	A scheme based on Searchable Symmetric Encryption (SSE) for performing search over encrypted data stored in the cloud	The underlying cryptographic technique is inefficient and therefore impacts the performance of the scheme Not implemented and tested in a commercial cloud environment
Wang *et al.* [112]	Cryptography	A new scheme called IDCrypt for allowing users to perform searches over encrypted data in the cloud	As IDCrypt still faces some challenges, it can be further improved Not implemented and tested in a commercial cloud environment
Xu *et al.* [115]	Secure Model	A data-sharing scheme that is secure and provides efficient fine-grained access control	The key generation center can be secured Not implemented and tested in a commercial cloud environment
TaheriMonfared and Jaatun [117]	Incidence Response Approach	A new approach for incidence response, where a component in the IaaS cloud has been compromised NIST guidelines for incidence response were considered as an input, and new steps were added to create a new approach This approach can provide containment, eradication, and recovery after an incident	Proposed approaches need to be tested statistically and their performance overhead should be measured The proposed approaches should be implemented in a commercial cloud environment Proposed approaches need to be implemented as security services and their effectiveness from the perspective of cloud consumer and cloud environment should be measured
Fotiou *et al.* [121]	Trusted Third Party	A solution for access control delegation to a trusted third party known as ACP	The ACP need to be a trusted entity Not implemented and tested in a commercial cloud environment
Yang [122]	Cryptography	A scheme known as Attribute-Based Searchable Encryption with Synonym Keyword search function (SK-ABSE) that allows multiple users to search over an encrypted file stored in a cloud environment	The Key Distribution Center (KDC) should be a trusted entity Not implemented and tested in a commercial cloud environment
Kim and Nepal [126]	Secure Model	A secure cloud storage system that allows multiple users to access and perform updates on encrypted data	Not implemented and tested in a commercial cloud environment Centralized administrator is a single point of failure and can be decentralized
Fan *et al.* [127]	Cryptography	A protocol for controlling access to data in cloud environment Uses encryption, and digital watermarking technologies to provide flexible, feature binding and offline control to the data in the cloud	Not implemented and tested in a commercial cloud environment

Author(s)	Solution Category	Summary	Limitations/Future Scope
El-Booz *et al.* [129]	Secure Authentication	A secure way to access the data stored in the cloud This scheme strengthens the authentication of cloud users by using two techniques known as TOTP and ABP for blocking data access to TPAs	The TPA can be a single point of failure Not implemented and tested in a commercial cloud environment
Hong and Sun [130]	Cryptography	A new scheme named Key Policy Attribute Based Signature with Untrusted Authority and Traceability to safeguard the data stored in the cloud This scheme prevents attribute authorities from compromising the security of the cloud by forging the signatures to impersonate cloud users	The refreshment of user's private keys can be done Attribute revocation can be implemented Outsourcing ABS with untrusted attribute authorities can be researched further Not implemented and tested in a commercial cloud environment
Silva *et al.* [137]	Secure Framework	A software architecture that provides security and preserves the privacy of users during data aggregation in IoT and cloud computing scenarios	Intel SGX has well-known vulnerabilities. It can be replaced. Not implemented and tested in a commercial cloud environment
Levitin *et al.* [141]	Secure Model	A model for protecting the data of cloud users from co-residence attacks performed by attackers residing on the same virtual machines Involves dividing the data of users into multiple blocks and replicating them on different VMs	All the physical servers were assumed to be protected A game theoretic approach where the user predicts the attacker's behavior can be investigated Not implemented and tested in a commercial cloud environment
Liu *et al.* [145]	Secure Framework	A scheme for securing file sharing among a group of users in the cloud Users can transfer the right to decrypt the file and also control decrypting permissions among a group of users The proposed scheme is collusion attack resistant	The performance of this scheme on larger data sizes can be improved The re-encryption key size grows linearly with the number of uses Multi-conditional proxy heavy encryption can be researched further Not implemented and tested in a commercial cloud environment
Al-Sharhan *et al.* [147]	Secure Framework	A new model and framework for securing the eHealth systems The proposed model secures the health records of patients by using a Virtual Private Cloud (VPC), elastic load balancing, and a Virtual Private Network (VPN) gateway	Not evaluated against various security attacks Not implemented and tested in a commercial cloud environment
Thirumalai *et al.* [151]	Cryptography	A scheme that utilizes a non-linear diophantine equation to achieve security against side-channel and timing attacks	The central trusted party can act as a single point of failure Not implemented and tested in a commercial cloud environment

Author(s)	Solution Category	Summary	Limitations/Future Scope
Shakil *et al.* [153]	Biometrics	A system named BAMHealthCloud for managing healthcare data in the cloud Uses behavioral biometric authentication for securing health data	Not evaluated against various security attacks Not implemented and tested in a commercial cloud environment
Wei *et al.* [154]	Secure Framework and Blockchain	A distributed virtual machine agent model in the cloud, which enables tenants in the cloud to cooperate with each other for trusted data verification	Not evaluated against various security attacks Not implemented and tested in a commercial cloud environment
Namasudra *et al.* [159]	Cryptography	A novel DNA encryption scheme for protecting data in the cloud computing environment A 1024-bit secret key is generated based on different factors like user's attributes, MAC address, ASCII value, and others	Mathematical analysis of this is scheme was not done The authentication process can be further improved Not implemented and tested in a commercial cloud environment
Wang *et al.* [162]	Secure Model	A new approach named Comprehensive Trustworthy Data Collection for sensor-cloud systems	Various attacks on the sink nodes were not considered Not implemented and tested in a commercial cloud environment
El-Latif *et al.* [165]	Cryptography and Steganography	A new quantum steganography protocol for securing the data transmitted to stored in the cloud A hash function was used to authenticate the secret messages	Not implemented or simulated Only validated against a few attacks Not implemented and tested in a commercial cloud environment
Sharma *et al.* [166]	Cryptography	A multi-level encryption and decryption approach for securing the data in the cloud RSA and AES algorithms were used for performing multi-level encryption and decryption	Data security in terms of data lineage and data remanence need to be investigated Algorithms can be replaced with lightweight algorithms to improve the performance Not implemented and tested in a commercial cloud environment
Hauser *et al.* [168]	Cryptography	An open-source platform called GridCloud for gathering real-time data and sharing it across jurisdictions that control the interconnected grid	Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Yang *et al.* [171]	Secure Framework and Blockchain	A framework named AuthPrivacyChain, which provides privacy protection using blockchain	Various attacks against cloud and blockchain were not considered
Liu [175]	Cryptography	A public-key encryption scheme that is secure against related randomness attacks	Practical implementation is not available Other alternatives like IBE, ABE can be considered

Author(s)	Solution Category	Summary	Limitations/Future Scope
Ge *et al.* [178]	Cryptography	A scheme with symmetric key-based verification for keyword search over dynamically encrypted cloud data	Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Kakkad *et al.* [181]	Image Analysis and Cryptography	A model for protecting images in a cloud environment Image authentication done in two stages	Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Cao *et al.* [183]	Blockchain	A secure eHealth system for securing the EHRs in the cloud using blockchain technology Allows outsourcing of EHRs only by authenticated participants with the help of blockchain	Various attacks on the blockchain were not considered Blockchain can be tuned to improve the performance Not implemented and tested in a commercial cloud environment
Vijayakumar *et al.* [185]	Cryptography	A technique that uses searchable encryption and proxy re-encryption techniques for securing patient health records in a cloud environment	Key distribution and repudiation can be investigated Not implemented and tested in a commercial cloud environment
Sajay *et al.* [186]	Cryptography	A hybrid approach for securing the data in the cloud Combined homographic encryption and blowfish encryption algorithms for enhancing cloud security	Other alternative algorithms for encryption and decryption can be considered Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Shen *et al.* [187]	Cryptography	A scheme for securing data in the cloud Uses AES symmetric encryption and improved identity-based proxy re-encryption algorithms for achieving fine-grained control over the data	The performance of the scheme can be optimized Other alternative algorithms for encryption and decryption can be considered Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Praveena and Rangarajan [188]	Machine Learning	A model based on an enhanced C4.5 machine learning algorithm for securing data in the cloud The model also uses a new deduplication algorithm and a new access control mechanism for securing the data	Other alternative algorithms for encryption and decryption can be considered Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Joseph *et al.* [191]	Biometrics	A multimodal authentication system using fingerprint, iris, and palm traits for securing data in the cloud Uses image processing techniques for pre-processing, feature extraction, and normalization	Other alternative algorithms for encryption and decryption can be considered Not tested against various security attacks Not implemented and tested in a commercial cloud environment

Author(s)	Solution Category	Summary	Limitations/Future Scope
Tahir *et al.* [192]	Genetic Algorithms	A new model named CryptoGA based on a Genetic Algorithm (GA) for dealing with data integrity and privacy issues in the cloud GA was used to generate the keys, which are used along with a cryptographic algorithm	A two-way crossover can be implemented Other types of data like images, audio, and video can also be encrypted Memory efficiency in terms of space can be further investigated Not implemented and tested in a commercial cloud environment
Gangireddy *et al.* [193]	Machine Learning	A model for protecting the data in the cloud Uses k-medoid clustering was used for clustering the secret information An enhanced blowfish algorithm was used for encryption and decryption of data	Other alternative algorithms for encryption and decryption can be considered Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Vijayakumar and Umadevi [194]	Secure Approach	A multi-level micro access algorithm for privacy preservation in the cloud	Not tested against various security attacks
Indira *et al.* [195]	Cryptography	Round key and random key-based encryption mechanisms for improving security in a cloud environment	The performance can be further improved Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Namasudra [198]	Cryptography	A scheme for access control for securing access to the data in a cloud environment The proposed scheme uses ABE for encrypting the data using the attributes of the users	Can be integrated with other intelligent services to support IoT Not implemented and tested in a commercial cloud environment The trusted third party is a single point of failure
Venkatraman and Geetha [199]	Cryptography	A novel algorithm named Specialized Steganographic Image Authentication (SSIA) for securing images stored in a cloud environment The algorithm uses a combination of blowfish algorithm and genetic operators to provide two-stage encryption	Proxy-encryption with the highest entropy and least correlation can be used to imporve this further Not implemented and tested in a commercial cloud environment Not tested against various security attacks
Hosam and Ahmad [200]	Cryptography and Steganography	A hybrid solution for tackling the key management problem Uses AES, ECC, and steganography for distributing the keys effectively in a cloud environment	Not implemented and tested in a commercial cloud environment Not tested against various security attacks

Author(s)	Solution Category	Summary	Limitations/Future Scope
Kiran Kumar and Mahammad Shafi [202]	Cryptography	A mechanism focusing on the integrity and privacy of data stored in a cloud computing environment The proposed mechanism uses a modified RSA algorithm	Not implemented and tested in a commercial cloud environment Not tested against various security attacks
Orobosade *et al.* [203]	Cryptography	A hybrid encryption algorithm for safeguarding the data in the cloud This scheme uses AES as the first stage of encryption for securing the privacy of data before storing it on the cloud The second stage involves ECC with AES	Other alternative algorithms for encryption and decryption can be considered Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Ogiela [205]	Secure Authentication	A cognitive authentication approach in which involves cognitive CAPTCHA codes for providing access to the data in the cloud	Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Seth *et al.* [206]	Cryptography	A framework that involves dual encryption and data fragmentation techniques for securing cloud data	Different QoS metrics can be considered for analysis The proposed architecture can be integrated with tools like Megatool and NextCloud Not implemented and tested in a commercial cloud environment
Shahzadi *et al.* [208]	Secure Model	Adaptive Neural Fuzzy Interference System (ANFIS) for resolving risks in cloud computing	Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Zhang *et al.* [210]	Secure Framework	Fog-based Detection System (FDS) for detecting data attacks in the sensor cloud	Not implemented and tested in a commercial cloud environment

This model allows the Quality of Service (QoS) to be monitored and also detects malicious insiders like CSPs and TPAs. This model also allows cloud users to audit CSPs with the help of TPAs to monitor the integrity of the outsourced data. The summary of solutions for T03 is given in Table 8.

3.4 Denial of Service (T04)

In a DoS attack, the perpetrator controls an army of infected machines to send illegitimate traffic and bring down a service, thereby affecting a business or organization. DoS attack affects the availability of a system. He *et al.* [42] proposed a new type of firewall named Tree-Rule Firewall, which overcomes the limitations of traditional list-based firewalls. In this tree-rule firewall, the rules are placed in a tree-like structure and are tested in a regular network and in a cloud environment. The tree-rule firewall overcomes the rule conflicts and redundant rules posed by the traditional firewalls. Saadi and Chaoui proposed a cloud architecture that was discussed in Section 3.3. Amar *et al.* proposed a mechanism as discussed in Section 3.1. Mishra *et al.* [70] proposed a security architecture named NvCloudIDS for monitoring intrusions at virtualization and network layers. It analyses the traffic coming to or going at the network layer and predicts the behavior. It also employs VM introspection and analyzes VM traffic at the virtualization layer. This architecture was designed to improve the robustness of IDS. They validated this framework with a recent intrusion dataset, UNSW-NB. Mahajan

Table 8. T03 solutions summary

Author(s)	Solution Category	Summary	Limitations/Future Scope
Szefer *et al.* [30]	Secure Framework	A set of novel cyber defense strategies that mitigate physical attacks in data centers The proposed strategies can be activated on a physical attack Some of them can even take effect even before the actual attack occurs	Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Cusack *et al.* [44]	Secure Authentication	A solution for the risk of identity theft involving SSO authorization in a cloud computing environment The solution uses federated identity management	The trusted third parties can be a point of failure Not implemented
Saadi and Chaoui [48]	Intrusion Detection	A cloud architecture with security tools like a honeypot, honeynet, and honeyd along with Intrusion Detection System These tools were used for behavioral analysis of traffic containing genuine and illegitimate traffic	Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Indu *et al.* [52]	Secure Authentication	An extension to SAML technology to secure the communication between cloud provider, cloud server, and an identity provider The proposed extension includes token-based authentication that is flexible and scalable	The identity provider is vulnerable to attacks Not tested against various security attacks
Razaque and Rizvi [134]	Secure Model	A Privacy-Preserving Model for auditing all the stakeholders in the cloud This model allows the Quality of Service (QoS) to be monitored and also detects malicious insiders like CSPs and TPAs	The TPA can be a point of failure Not implemented and tested in a commercial cloud environment

and Peddoju [100] proposed an integrated approach that combines Network Intrusion Detection System (NIDS) and Honeypots for providing better security to the cloud. The signatures in Snort NIDS are updated by analyzing the data collected from the honeypot network and also from the dynamic malware analysis conducted in the sandboxing environment.

Xue *et al.* [108] proposed a solution to secure encrypted cloud storage against Economic Denial-of-Service (EDoS) attacks. This solution uses the CP-ABE scheme to provide security against EDoS attacks, and transparency of resource usage is guaranteed to the cloud provider and also to data owners. This solution uses a Bloom filter and also probabilistic checks to provide resource consumption accounting.

Shawahna *et al.* [110] proposed a new technique known as EDoS Attack Defense Shell (EDoS-ADS) to prevent EDoS attacks. This technique can differentiate between legitimate and malicious requests. The novel feature of this technique is that it can identify

the malicious client even though they are behind a Network Address Translation (NAT) based network. So, this technique will only block the malicious NAT users and not the entire NAT subnet or network. Abusitta *et al.* [136] proposed a new approach for detecting Denial of Service (DoS) attacks in the dynamically changing cloud environment. This model can quantify the effect of dynamic resource configurations in the cloud, which helps to filter out false negatives due to changing the resources and detect attacks more accurately. It is also able to detect flash crowds from DoS attacks by comparing VM metrics and the actual resources load. Hypervisors can also know which VMs are using more resources without any need. Jakóbik *et al.* [143] developed a model for selecting provider-level security decisions automatically in cloud computing environments. The model is based on Stackelberg games which contain two entities, namely, defender and attacker. The model has been validated on DoS attacks. Bhushan and Gupta [184] proposed a novel approach for sharing flow tables in SDN-based cloud for thwarting table overloading DDoS attacks. Their approach utilizes other idle flow tables that belong to the other OpenFlow switches. Achbarou *et al.* [196] developed a system named Distributed Intrusion Detection System (DIDS) which uses multiple reactive agents for detecting and preventing new and complex malicious attacks in a cloud environment. Shyla and Sujatha [204] proposed a novel IDS which employs Leader-based K-means clustering (LKM) and an optimal fuzzy logic system for protecting the cloud environment against various attacks. The summary of solutions for T04 is given in Table 9.

3.5 Vulnerable Systems and APIs (T05)

The presence of vulnerabilities in Application Programming Interfaces (APIs), operating systems, and other middleware components might lead to the compromise of a subsystem or the entire system. Saadi and Chaoui proposed a new model, which was discussed in Section 3.1. He *et al.* proposed a new type of firewall, which was discussed in Section 3.4. Yu *et al.* [43] described the weakness of the Remote Data Possession Checking (RDPC) protocol and demonstrated them. They also presented an improved model of the RDPC protocol and implemented it to show that the improvements are secure and practical. Cusack and Ghazizadeh proposed a solution that was discussed in Section 3.3. Kritikos *et al.* [51] proposed a model-driven approach for securing multi-cloud environments. The security aspects addressed by this approach are a) fine-grained access control over user personal data, virtual machines, and platform services and b) making the application deployments adapt to security requirements automatically. Uddin *et al.* [66] presented a single-point entry and exit API-based solution for securing file uploads in a cloud environment. Different threats related to file upload were mentioned, and different protection rules were reviewed. They provided client-side validation using scripts and also server-side validation modules for validating file uploads. Mumme *et al.* [93] proposed a system named Application Protected Execution (APEx) that provides multi-layer security by using out-of-band memory in a VM on cloud nodes. This system also provides In-VM monitoring which protects the security software execution. This system protects user space from reverse engineering and Return Oriented Programming (ROP) attacks. Code Obfuscation Engine (CObE) in the system does code stirring and uses out-of-band memory for altering the program flow and hiding the return stack.

Abdulqadder *et al.* [114] proposed a secure cloud architecture named SecSDNcloud that can resist three attack types, namely, flow table overloading, control plane saturation, and Byzantine attacks. For secure user authentication, a new digital signature generation with chaotic secure hashing is developed. For improving the quality of service, Particle Swarm Optimization (PSO) routing protocol has been enhanced. Packet analysis has been done by constructing 5-tuples. Salam *et al.* [124] proposed a model and implementation for hiding search keywords while performing a search over encrypted data stored in the cloud. This scheme allows a user to perform a search over encrypted data and retrieve the results back without compromising the user's privacy. For implementation, one of the efficient symmetric key primitives in the mobile environment was utilized. Nkenyereye *et al.* [128] proposed a secure billing protocol for vehicles that subscribe to cloud services. This protocol utilizes ABE techniques for access control over purchased services in the cloud. The privacy of the users owning the vehicles is guaranteed through pseudonym techniques. A signature scheme is utilized to provide authentication for vehicle users. The proposed protocol is efficient when compared to existing protocols using bilinear pairing operations.

Ullrich *et al.* [131] conducted a systematic study of firewalls provided by major cloud providers. For each firewall product, default configuration, configuration capabilities, filtering options, and the available documentation were studied. An extendable firewall tool for monitoring the cloud service provider's filtering behavior was also developed. The study found out that the firewalls evolved over one year, and configuration capabilities were also enhanced. Atlidakis *et al.* [172] discussed different ways an attacker can use to compromise REST APIs in a cloud environment. The authors introduced four security rules that can

Table 9. T04 solutions summary

Author(s)	Solution Category	Summary	Limitations/Future Scope
He *et al.* [42]	Firewall	A new type of firewall named Tree-Rule Firewall, which overcomes the limitations of traditional list-based firewalls The tree-rule firewall overcomes the rule conflicts and redundant rules posed by the traditional firewalls	Number of columns in the tree structure can include more than just three attributes The firewall can further be extended to support Network Address Translation Not implemented and tested in a commercial cloud environment
Mishra *et al.* [70]	Intrusion Detection	A security architecture named NvCloudIDS for monitoring intrusions at virtualization and network layers It analyses the traffic coming to or going at the network layer and predicts the behavior It also employs VM introspection and analyzes VM traffic at the virtualization layer	Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Mahajan and Peddoju [100]	Intrusion Detection	An integrated approach that combines NIDS and Honeypots for providing better security to the cloud The signatures in Snort NIDS are updated by analyzing the data collected from the honeypot network	Performance analysis was not done The network dumps collected can also be analyzed for possible attacks Other components like ACLs, firewalls and HIDS can be integrated for more comprehensive security
Xue *et al.* [108]	Cryptography	A solution to secure encrypted cloud storage against EDoS attacks Uses the CP-ABE scheme to provide security against EDoS attacks	Not tested against various security attacks
Shawahna *et al.* [110]	Secure Model	A new technique known as EDoS-ADS to prevent EDoS attacks The novel feature in this technique is that it can identify the malicious client even though they are behind a NAT based network	Not implemented and tested in a commercial cloud environment
Abusitta *et al.* [136]	Secure Model	A new approach for detecting DoS attacks in the dynamically changing cloud environment This model can quantify the effect of dynamic resource configurations in the cloud, which helps to filter out false negatives due to changing the resources and detect attacks more accurately	The centralized components affects the availability of the system Not tested against various security attacks
Jakóbik *et al.* [143]	Secure Model	A model for selecting provider-level security decisions automatically in cloud computing environments The model is based on Stackelberg games which contain two entities, namely, defender and attacker	Not implemented and tested in a commercial cloud environment

Author(s)	Solution Category	Summary	Limitations/Future Scope
Bhushan and Gupta [184]	Secure Model	A novel approach for sharing flow tables in SDN-based cloud for thwarting table overloading DDoS attacks	Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Achbarou *et al.* [196]	Intrusion Detection	A system named Distributed Intrusion Detection System which uses multiple reactive agents for detecting and preventing new and complex malicious attacks in a cloud environment	Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Shyla and Sujatha [204]	Intrusion Detection and Machine Learning	A novel IDS which employs Leader-based K-means clustering and an optimal fuzzy logic system for protecting the cloud environment against various attacks	Data is not secured Not tested against various security attacks Not implemented and tested in a commercial cloud environment

be used to represent REST API properties. The authors extended a stateful REST API fuzzer to test and detect the violation of the security rules. The summary of solutions for T05 is given in Table 10.

3.6 Weak Authentication and Identity Management (T06)

Weak key management schemes and poor access control mechanisms allow perpetrators to circumvent the system security measures of a system which may lead to taking complete control of the system. Medhioub *et al.* [34] proposed a new authentication scheme for storing data in the cloud. Further, authentication mechanisms provided by DropBox and Identity Based Cryptography (IBC) fundamentals were discussed. The authors said that username and password validation for a cloud user was not sufficient. Based on the identity of the cloud user, public keys are derived, and private keys will be derived based on a secret element that belongs to the cloud tenant's authentication domain. Saadi and Chaoui proposed a new model, which was discussed in Section 3.1. Cusack and Ghazizadeh proposed a solution that was discussed in Section 3.3. Indu *et al.* proposed an extension to Security Assertions Markup Language (SAML), which was discussed in Section 3.3. Challa *et al.* [57] created a new authentication scheme for performing authentication between a user and a cloud server and between a cloud server and a smart meter. In this scheme, both entities authenticate one another with the help of a trusted third party. A session key is created that can be used in future communication between the entities. Ali *et al.* developed a new system which was discussed in Section 3.1. Singh proposed a new framework which was discussed in Section 3.1. Pereira *et al.* presented a scheme named Storekeeper, which was discussed in Section 3.1.

Lejeune *et al.* proposed two new algorithms, which were discussed in Section 3.1. Nakouri and Kim proposed a framework based on biometrics which was discussed in Section 3.1. Habiba *et al.* [120] analyzed various cloud Identity Management Systems (IDMSs) and presented security issues in them. Various taxonomies related to IDMS features were given. These taxonomies were used to evaluate different cloud IDMSs. In the analysis done, it was revealed that none of the existing IDMS approaches provide all the features required by a cloud IDMS.

3.7 Account Hijacking (T07)

A major threat to any business or organization, whether in the cloud or on-premise, is account hijacking. Through various methods like phishing, etc., the credentials of employees and users are hijacked, and the cloud resources are used for nefarious purposes. Indu *et al.* proposed a method that was discussed in Section 3.3. Pereira *et al.* presented a scheme named Storekeeper, which was discussed in Section 3.1. Paxton *et al.* described solutions to this threat which were discussed in Section 3.1. Social engineering techniques are difficult to mitigate, and there is not much research after 2014 for mitigating account hijacking in a cloud scenario.

3.8 Shared Technology Vulnerabilities (T08)

Cloud resources are shared among users through technologies like virtualization and hypervisors. Compromising a virtual machine or a hypervisor allows the attacker to gain control over multiple user workloads as the users are collocated on the same resources. Christodorescu *et al.* [24] proposed a solution for vir-

Table 10. T05 solutions summary

Author(s)	Solution Category	Summary	Limitations/Future Scope
Yu *et al.* [43]	Secure Model	An improved model of the RDPC protocol	Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Kritikos *et al.* [51]	Secure Approach	A model-driven approach for securing multi-cloud environments	The proposed approach needs to be validated Advanced testing need to be conducted to identify security issues The administration API can be coupled with an UI eliminating the requirement of CAMEL knowledge
Uddin *et al.* [66]	Secure Approach	A single point entry and exit API-based solution for securing file uploads in a cloud environment Different threats related to file upload were mentioned, and different protection rules were reviewed	Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Mumme *et al.* [93]	Secure Framework	A system named Application Protected Execution that provides multi-layer security by using out-of-band memory in a VM on cloud nodes Provides In-VM monitoring which protects the security software execution	Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Abdulqadder *et al.* [114]	Secure Framework	A secure cloud architecture named SecSDNcloud that can resist three attack types, namely, flow table overloading, control plane saturation, and Byzantine attacks	Can be applied to a 5G network which has higher data rate Not implemented and tested in a commercial cloud environment
Salam *et al.* [124]	Secure Model	A model and implementation for hiding search keywords while performing a search over encrypted data stored in the cloud	The execution time of the encryption module can be improved Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Nkenyereye *et al.* [128]	Cryptography	A secure billing protocol for vehicles that subscribe to cloud services This protocol utilizes ABE techniques for access control over purchased services in the cloud	The revocation process can be based on updating the access structure Not implemented and tested in a commercial cloud environment
Ullrich *et al.* [131]	Firewall	A systematic study of firewalls provided by major cloud providers An extendable firewall tool for monitoring the cloud service provider's filtering behavior was also developed	None

Author(s)	Solution Category	Summary	Limitations/Future Scope
Atlidakis *et al.* [172]	Secure Model	Extended a stateful REST API fuzzer to test and detect the violation of the security rules	Need to fuzz more services through REST APIs and check more properties to detect different kinds of bugs and security vulnerabilities Not tested against various security attacks

tual machine (VM) security using virtual machine introspection (VMI). The solution is scalable in terms of a) guest protection is centralized into a security VM, b) guest operating systems like Linux and Windows are supported, and the solution can be easily extended to other types of operating systems, c) does not assume any previous semantic knowledge of the guest, d) does not depend on the guest VM's state. The general steps in the solution are: 1) Reading the IDT from the virtual CPU registers, 2) From the available allow-lists of operating systems and in-memory code blocks, determine the guest OS running inside a VM, 3) Determine other relevant data structures related to the guest OS, 4) Continuously analyze the data structures using the white list for the guest OS for identifying whether they are modified or not. The authors also demonstrated identifying rootkits using their solution. Bates *et al.* [25] presented a technique called co-resident watermarking in which a malicious VM analyzes the traffic flow after injecting a watermark signature into the network. This attack is evaluated under a wide variety of hardware and system load configurations using both local lab environments and production cloud environments. The key contributions of this work are: 1) Virtualization side channels are investigated in physical hardware, 2) Assessing the severity of the threat through extensive evaluation, 3) Proof-of-concept by developing an accurate load measurement attack to filter out the activity of other VMs. Kazim *et al.* [26] proposed a model named Encrypted Virtual Disk Images in Cloud (EVDIC), which guarantees the confidentiality and integrity of the virtual disk images used by the VMs. They also propose a way to integrate their scheme into the popular open-source cloud platform, OpenStack. According to their model, there are three key modules: 1) Image Encryption Module (IEM), 2) Image Decryption Module (IDM), and 3) Key Management Server (KMS). The KMS is located outside the cloud. Authors assume the security of communication between the cloud and KMS will be taken care of by the underlying protocol SSL 3.0. Thimmaraju *et al.* [39] introduced a Virtual switch Attacker Model for Packet-parsing (vAMP) attack that exploits unified packet parser available in virtual switches which implement complex network protocol parsing. The authors used OpenStack to demonstrate vAMP attack illustrating how a weak attacker can compromise an entire cloud environment. Meryem *et al.* [40] proposed a new algorithm that includes map-reduce and k-means for identifying malicious user behaviors and hosts in a cloud computing environment. A centralized log is maintained, which contains all the events performed by various users on the cloud resources. To identify and predict malicious users, the authors considered cosine distances and deviation metrics.

Kritikos *et al.* proposed a model-driven approach for securing multi-cloud environments, which was discussed in Section 3.5. Fang *et al.* proposed a way to model security protocols which were discussed in Section 3.1. Mishra *et al.* proposed a security architecture named NvCloudIDS, which was discussed in Section 3.4. Ahamed *et al.* [83] proposed a technique named compartment isolation technique for securing the VM consolidation process. The proposed technique consists of two algorithms, one for selection and another for placement of VMs. The solution is scalable and also achieves energy efficiency. Pisharody *et al.* proposed a framework for detecting conflicts between flow rules in an SDN-based cloud environment which was discussed in Section 3.1. Mumme *et al.* proposed a system named Application Protected Execution (APEx) which was discussed in Section 3.5. Gao *et al.* [97] presented an approach for securing containers in the cloud. First, they described different channels through which information can be leaked in containers about the host system. Then, they described the root causes that allow perpetrators to gather information from the containers. They provided a two-stage approach that involves masking the channels and enhancing the isolation model of containers for mitigating information leakages. Paladi *et al.* proposed a framework for securing data in IaaS clouds which was discussed in Section 3.1. Schwarzkopf *et al.* [118] proposed a mechanism for improving the security of virtual machines. This approach was designed and implemented on a custom testbed. Different online penetration testing suites like OpenVAS and Nessus were used for testing the security of VMs. An update checker program was created, which identifies the software packages that are outdated irrespective of the status of the VM, whether

Table 11. T06 solutions summary

Author(s)	Solution Category	Summary	Limitations/Future Scope
Medhioub *et al.* [34]	Secure Authentication	A new authentication scheme for storing data in the cloud Based on the identity of the cloud user, public keys are derived, and private keys will be derived based on a secret element that belongs to the cloud tenant's authentication domain	To improve the performance of the system, a separate authentication server can be used Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Challa *et al.* [57]	Secure Authentication	A new authentication scheme for performing authentication between a user and a cloud server and between a cloud server and a smart meter	The trusted third party acts as a single point of failure Not implemented and tested in a commercial cloud environment
Nagaraju and Parthiban [125]	Secure Framework and Biometrics	A framework for securing the online banking process After authentication, a privacy protection gateway will obfuscate and desensitize the customer details using advanced techniques like tokenization and data anonymization	Query auditing techniques can be used for detecting and preventing data breaches An efficient autonomous algorithm can be developed for detecting sensitive fields in dynamic cloud datasets Not implemented and tested in a commercial cloud environment
Grzonka *et al.* [144]	Artificial Intelligence	A model named Multi-Agent System based Cloud Monitoring, which used Artificial Intelligence (AI) for monitoring the execution, security, and scheduling of processes in the cloud	A more effective approach for loading workers can be developed Not implemented and tested in a commercial cloud environment
Wazid *et al.* [157]	Secure Authentication	A lightweight authentication scheme for securing the data transmitted between IoT sensors and the cloud This scheme employs one-way cryptographic hash functions and bitwise XOR operations	Not implemented and tested in a commercial cloud environment
Kumari *et al.* [174]	Secure Authentication and Cryptography	An efficient authentication framework based on Elliptic Curve Cryptography (ECC) for cloud-based smart medical systems	Not implemented and tested in a commercial cloud environment

it is running or dormant on the disk. Denz and Taylor [119] presented a survey of various risks in cloud computing and different mitigation mechanisms. They proposed a way to identify zero-day threats by using an integrated approach involving malware detection, secure virtual machine managers, and cloud resilience. This approach prolongs the attacks and denies their persistence. Rakotondravony *et al.* [132] provided a classification of attacks in the IaaS cloud mainly using the Virtual Machine Introspection (VMI) mechanisms. This classification methodology considered a source, target, and direction of attacks as a cloud actor can behave as both attacker and target of an attack. A statistical analysis of the vulnerabilities based on the given classification is analyzed, and their impact on the business has been provided. Wang and Liu [135] provided a model named Trusted Measurement Model based on Dynamic policy and Privacy protection (TMMDP), which secures the cloud user's virtual machines from other tenants' virtual machines in an IaaS cloud. This model preserves the privacy of users also. This model mainly divides the modules of measurement into front-end modules and back-end modules. The front-end modules deal with measuring the security of virtual machine files, and the back-end modules deal with measuring the security of networking. Jin *et al.* [139] surveyed the security of integrating Field Programmable Gate Arrays (FPGAs) with a cloud. They identified different threats and attacks that are related to cloud FPGAs. Different countermeasures were also proposed to mitigate the attacks on cloud FPGAs. Levitin *et al.* proposed a model, which was discussed in Section 3.1. Amato *et al.* [142] proposed a solution for security analysis and modeling of cloud infrastructures by using Model Driven Engineering (MDE) techniques. They provided a formal profile of the thermal behavior of hosts and used it as a baseline for forecasting malicious actions. Patil *et al.* [148] proposed a framework named Hypervisor Level Distributed Network Security (HLDNS) which monitors the VMs on physical servers in the cloud. They defined two new fitness functions for Binary Bat Algorithm (BBA) for extracting features from cloud network traffic. The extracted features were fed to Random Forest Classifier for detecting intrusions. The alerts across all the servers are correlated to form a new attack signature. This framework was tested on the recent UNSW-NB15 and CICIDS-2017 intrusion datasets. Mishra *et al.* [156] proposed an approach named KVMInspector, which uses dynamic analysis to detect malware in the cloud. The authors used LibVMI and Nitro libraries to collect data running virtual machines. A preliminary process verification is done at the KVM layer, followed by a detailed behavioral analysis to learn about the behavior of monitored programs using machine learning techniques. Huang *et al.* [161] developed a framework named Policy-Customized Trusted Cloud Service (PC-TCS), which provides an on-demand trust management mechanism and consistent VM migrations. The framework consists of two main components, namely, Attribute-Based Signature (ABS) for achieving trusted remote attestation and an ABS and blockchain-based VM migration protocol. Jin *et al.* [177] proposed a framework named Dynamic Security Evaluation and Optimization of MTD (DSEOM), which can detect updates in container-based cloud environments, evaluate and optimize Moving Target Defense (MTD) strategies. Deshpande *et al.* [179] presented a host-based intrusion detection system for alerting cloud users by analyzing the system call traces. Their method analyses failed system call traces for early detection of intrusions. The summary of solutions for T08 is given in Table 12.

3.9 Lacking Due Diligence (T09)

A cloud consumer must periodically review the accreditations and standards followed by the cloud service provider. Anand *et al.* [35] proposed a new methodology for assessing threats in a cloud environment based on Microsoft's STRIDE-DREAD model. Threats were ranked based on their severity and the importance of the client's security requirements. After ranking the threats, a link is provided to security classification. After assessing client requirements, the risk associated with the threat category is evaluated on a scale of 0, 5, or 10 using the DREAD model. A threat assessment matrix and security index for each STRIDE model category is created using the calculated risk factor and user threat tolerance level. Finally, the security index is ranked in descending order from which the users can get an idea about the seriousness of the threats. Carvalho *et al.* [53] conducted a systematic literature review of open issues and available solutions for security in SLAs. They presented a state-of-the-art analysis of the literature. Finally, challenges in SLA security were enumerated which can be treated as future research directions. Chen *et al.* [68] presented a security framework for provenance data auditing in a cloud environment. In this framework, the data in log files is used as input for auditing the provenance data. Different audit mechanisms were compared, and their advantages and disadvantages were also listed. Zhou *et al.* [87] proposed a model for detecting breaches in the SLA. This model is based on Markov decision process theory and preserves the privacy of users. This model can also evaluate the credibility of a CSP and can monitor user privacy violations.

Moghaddam *et al.* [138] proposed a structural policy management engine for managing different policies in the cloud. It provides dedicated security levels called rings which are based on the cloud provider

Table 12. T08 solutions summary

Author(s)	Solution Category	Summary	Limitations/Future Scope
Christodorescu *et al.* [24]	Secure Framework	A solution for virtual machine security using virtual machine introspection	Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Bates *et al.* [25]	Secure Model	A technique called co-resident watermarking in which a malicious VM analyzes the traffic flow after injecting a watermark signature into the network	Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Kazim *et al.* [26]	Cryptography	A model named Encrypted Virtual Disk Images in Cloud, which guarantees the confidentiality and integrity of the virtual disk images used by the VMs	Performance analysis of the proposed approach can be done Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Meryem *et al.* [40]	Machine Learning	A new algorithm that includes map-reduce and k-means for identifying malicious user behaviors and hosts in a cloud computing environment	Not implemented Not tested against various security attacks
Ahamed *et al.* [83]	Secure Framework	A technique named compartment isolation technique for securing the VM consolidation process The proposed technique consists of two algorithms, one for selection and another for placement of VMs	The reliability of VMs can be investigated Efficient energy consumption can be investigated Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Gao *et al.* [97]	Secure Approach	An approach for securing containers in the cloud They provided a two-stage approach that involves masking the channels and enhancing the isolation model of containers for mitigating information leakages	Not implemented and tested in a commercial cloud environment
Schwarzkopf *et al.* [118]	Secure Model	A mechanism for improving the security of virtual machines Different online penetration testing suites like OpenVAS and Nessus were used for testing the security of VMs	Current approach is a basic one Support for larger number of scanners is not available Not implemented and tested in a commercial cloud environment
Denz and Taylor [119]	Secure Framework	A way to identify zero-day threats by using an integrated approach involving malware detection, secure virtual machine managers, and cloud resilience	Not implemented and tested in a commercial cloud environment
Wang and Liu [135]	Secure Model	A model named Trusted Measurement Model based on Dynamic policy and Privacy protection, which secures the cloud user's virtual machines from other tenants' virtual machines in an IaaS cloud	The trust in the system for generating policy in the security management server can be investigated Not implemented and tested in a commercial cloud environment

.

Author(s)	Solution Category	Summary	Limitations/Future Scope
Amato *et al.* [142]	Model Driven Engineering Techniques	A solution for security analysis and modeling of cloud infrastructures by using Model Driven Engineering techniques	The proposed methodology can be extended to support a more complex governor, energy manager, and more IaaS middleware Not implemented and tested in a commercial cloud environment
Patil *et al.* [148]	Secure Framework	A framework named Hypervisor Level Distributed Network Security (HLDNS) which monitors the VMs on physical servers in the cloud	The proposed framework can be extended to detect network attacks Parsing encrypted data is a major challenge The proposed framework can be integrated firewall to make it suitable for intrusion prevention System level attacks are not detectable and can be further investigated
Mishra *et al.* [156]	Secure Approach	An approach named KVMInspector, which uses dynamic analysis to detect malware in the cloud LibVMI and Nitro libraries were used to collect data running virtual machines	Does not detect network level attacks Not implemented and tested in a commercial cloud environment
Huang *et al.* [161]	Secure Framework and Blockchain	A framework named Policy-Customized Trusted Cloud Service, which provides an on-demand trust management mechanism and consistent VM migrations	Performance of ABS and blockchain in PC-TCS can be investigated Not implemented and tested in a commercial cloud environment
Deshpande *et al.* [179]	Intrusion Detection and Machine Learning	A host-based intrusion detection system for alerting cloud users by analyzing the system call traces	The detection accuracy can be improved further Does not detect network level attacks Not implemented and tested in a commercial cloud environment

capabilities and cloud consumer requirements. Cloud Security Ontology (CSON) was used to define two superclasses for providing a mapping between cloud customers' requirements and cloud providers' capabilities. Halabi and Bellaiche [140] proposed a broker-based framework for managing cloud SLAs. They developed a standard way to represent an SLA and also provided an evaluation and simulation model. Jakóbik *et al.* developed a model which was discussed in Section 3.4. Li *et al.* [167] proposed a trust assessment framework for cloud-based IoT services. The framework integrates security-based and reputation-based methods for assessing the trust in cloud services. Cloud-specific security metrics were used to evaluate the security of cloud services, and feedback ratings were used to evaluate the reputation of a cloud service which is thereby used to evaluate the trust of a cloud service. Rios *et al.* [201] proposed a framework to design, deploy and operate multi-cloud systems that include necessary privacy and security controls. This framework ensures that the deployed system adheres to General Data Protection Regulation (GDPR). This framework depends upon the risk-driven specification done with the help of SLA and continuous monitoring during the runtime. The summary of solutions for T09 is given in Table 13.

3.10 Advanced Persistent Threats (APT) (T10)

In an Advanced Persistent Threat (APT) attack, the perpetrator penetrates the target organization's or individual's network covertly and monitors the traffic for extended periods. Meryem *et al.* proposed a new algorithm as discussed in Section 3.8. Amar *et al.* pro-

Table 13. T09 solutions summary

Author(s)	Solution Category	Summary	Limitations/Future Scope
Anand *et al.* [35]	Secure Approach	A new methodology for assessing threats in a cloud environment based on Microsoft's STRIDE-DREAD model A threat assessment matrix and security index for each STRIDE model category is created using the calculated risk factor and user threat tolerance level	The security patterns related to cloud environment can be classified based on the proposed threat model Not implemented and tested in a commercial cloud environment
Chen *et al.* [68]	Secure Framework	A security framework for provenance data auditing in a cloud environment In this framework, the data in log files is used as input for auditing the provenance data	Not implemented and tested in a commercial cloud environment
Zhou *et al.* [87]	Secure Model	A model for detecting breaches in the SLA This model is based on Markov decision process theory and preserves the privacy of users	The proposed model works only when CSP offers cooperation Users' role setting also needs to be determined beforehand The modeling process can be done with a hidden Markov model
Moghaddam *et al.* [138]	Secure Framework	A structural policy management engine for managing different policies in the cloud It provides dedicated security levels called rings which are based on the cloud provider capabilities and cloud consumer requirements	Not tested against various security attacks Not implemented and tested in a commercial cloud environment
Halabi and Bellaiche [140]	Secure Framework	A broker-based framework for managing cloud SLAs	Methodologies for monitoring the proposed security SLA need to be developed The proposed security SLA and be applied to federated cloud Not implemented and tested in a commercial cloud environment
Li *et al.* [167]	Secure Framework	A trust assessment framework for cloud-based IoT services The framework integrates security-based and reputation-based methods for assessing the trust of cloud services	The centralized trust assessment can be a point of failure Not implemented and tested in a commercial cloud environment
Rios *et al.* [201]	Secure Framework	A framework to design, deploy and operate multi-cloud systems that include necessary privacy and security controls	Optimization of SLA composition and root cause analysis can be investigated The proposed solution can further be extended to support a set of privacy controls and metrics

posed a mechanism that leverages big data processing on log files which was discussed in Section 3.1. Mishra *et al.* proposed a security architecture named NvCloudIDS, which was discussed in Section 3.4. Chandra *et al.* proposed a system for protection against advanced persistent threats, which was discussed in Section 3.1. Mahajan and Peddoju proposed an integrated approach which was discussed in Section 3.4. Shyla and Sujatha proposed a novel IDS, which was discussed in Section 3.4.

3.11 Abuse of Cloud Services (T11)

Malicious users can hijack accounts of legitimate cloud users and use the cloud resources for nefarious purposes. Liao *et al.* [33] demonstrated how cloud services could be used by users for long-tail Search Engine Optimization (SEO). First, they identified 3,186 cloud directories that were hosting 318,470 doorway pages that were used for long-tail SEO. After analyzing the pages, they found out that 6 percent of the doorway pages appeared in the top 10 results displayed by the search engines. Authors were also able to determine how those doorway pages were being monetized and how the malicious users were able to counter the cloud platform's defenses. Liao *et al.* [36] performed a systematic study on cloud repositories that are used by malicious users for conducting their malicious online activities. Cloud providers often hesitate to perform a scan of their client's repositories without their permission, and this makes bad cloud repositories an emerging threat. The authors initially created a small set of seeds to identify the features of websites they serve to uniquely characterize the bad repositories. A scanner was also developed that detected over 600 bad repositories which were hosted on top cloud platforms. Amar *et al.* proposed a mechanism that leverages big data processing on log files which was discussed in Section 3.1. Mishra *et al.* proposed a security architecture named NvCloudIDS, which was discussed in Section 3.4. Mahajan *et al.* proposed an integrated approach which was discussed in Section 3.1. Xue *et al.* proposed a solution which was discussed in Section 3.4. Shawahna *et al.* proposed a new technique known as EDoS Attack Defense Shell, which was discussed in Section 3.4. Nkenyereye *et al.* proposed a secure billing protocol for vehicles that subscribe to cloud services, which was discussed in Section 3.5. The summary of solutions for T11 is given in Table 14.

3.12 Lack of Responsibility (T12)

Cloud users are responsible for securing their application workloads in the cloud. Any negligence in doing so might lead to service unavailability or a data breach. Anand *et al.* proposed a new methodology for assessing threats in a cloud environment which was discussed in Section 3.9. Kritikos *et al.* proposed a model-driven approach for securing multi-cloud environments, which was discussed in Section 3.5. Casola *et al.* [81] presented a methodology that offers security-as-a-service capabilities as a catalog. The capabilities that are to be guaranteed are specified using a Service Level Agreement (SLA). The proposed methodology is a part of a larger project named SPECS. Kaaniche *et al.* [105] proposed an SLA-based solution for providing security to cloud users. They extended the SLA language which is, rSLA. This new language is used to specify the security requirements of the cloud user. The rSLA framework is extended so that existing tools can be used to monitor the security requirements that are enforced during runtime or not. Taylor and Shue [107] proposed a system that uses cloud middleboxes to secure the connections from residential networks to malicious TLS servers. The system's name is TLSDeputy. By implementing their approach with OpenFlow, an SDN protocol, residential network communications were secured with little performance overheads. The summary of solutions for T12 is given in Table 15.

3.13 Insufficient Security Tools (T13)

There is a need to develop security tools to address various threats of cloud computing. Present tools being used in on-premise data centers are not sufficient for threat and vulnerability monitoring in the cloud. Mishra *et al.* proposed a security architecture named NvCloudIDS, which was discussed in Section 3.4. Ullrich *et al.* conducted a systematic study of firewalls which was discussed in Section 3.5. Moghaddam *et al.* proposed a structural policy management engine which was discussed in Section 3.9. Sun *et al.* [164] developed a system for monitoring the security parameters in different cloud environments. Multiple clouds can be accessed through a single API. The security system consists of different components like a scanning engine, recovery engine, evaluation model, visual display module, etc. Each resource is assigned three tuples which contain vulnerabilities, scores, and repair methods. Mouratidis *et al.* [189] proposed a novel security modeling language and analysis techniques for analyzing the security requirements of cloud computing environments. The authors proposed three analysis techniques that can take a model of a cloud computing system and add new security knowledge automatically. The summary of solutions for T13 is given in Table 16.

3.14 Human Error (T14)

The weakest link in security is humans. Perhaps the most difficult threat to monitor in the cloud is hu-

Table 14. T11 solutions summary

Author(s)	Solution Category	Summary	Limitations/Future Scope
Liao *et al.* [33]	Detection of Abusing Services	Demonstrated how cloud services could be used by users for the purpose of long-tail Search Engine Optimization	None
Liao *et al.* [36]	Detection of Abusing Services	A systematic study on cloud repositories that are used by malicious users for conducting their malicious online activities	None

Table 15. T12 solutions summary

Author(s)	Solution Category	Summary	Limitations/Future Scope
Casola *et al.* [81]	Secure Approach	A methodology that offers security-as-a-service capabilities as a catalog The capabilities that are to be guaranteed are specified using a Service Level Agreement (SLA)	Not implemented and tested in a commercial cloud environment
Kaaniche *et al.* [105]	Secure Approach	An SLA-based solution for providing security to cloud users They extended SLA language which is, rSLA for specifying the security requirements of the cloud users	Not implemented and tested in a commercial cloud environment
Taylor and Shue [107]	Secure Model	A system that uses cloud middleboxes to secure the connections from residential networks to malicious TLS servers	Not implemented and tested in a commercial cloud environment

Table 16. T13 solutions summary

Author(s)	Solution Category	Summary	Limitations/Future Scope
Sun *et al.* [164]	Secure Framework	A system for monitoring the security parameters in different cloud environments Multiple clouds can be accessed through a single API	Security of the proposed system is not evaluated
Mouratidis *et al.* [189]	Secure Framework	A novel security modeling language and analysis techniques for analyzing security requirements of cloud computing environments	None

man errors. A simple error committed by a system administrator can affect the availability of the cloud. A possible solution for reducing human errors is to adopt machine learning to observe human behavior and take actions accordingly. Papagiannis *et al.* [32] proposed a model named the text disclosure model to make users comply with the data disclosure policies of a company or organization. To track the flow of data from one cloud service to another, they introduce imprecise data flow tracking that identifies similarities between text fragments. They demonstrate the applicability of imprecise data flow tracking through a browser-based middleware, BROWSERFLOW, that alerts when they expose sensitive text to an untrusted cloud service and has a trivial performance impact on user experience. Torkura *et al.* [173] proposed Risk-driven Fault Injection (RDFI) techniques for mitigating human errors and misconfiguration errors in a cloud environment. RDFI utilizes chaos engineering principles to execute, monitor, analyze and plan security fault injection campaigns. It also employs a knowledge base that is created from the best cloud practices as a baseline. Authors developed a new tool named CloudStrike using their RDFI methods and chaos engineering algorithms. The summary of solutions for T14 is given in Table 17.

Table 17. T14 solutions summary

Author(s)	Solution Category	Summary	Limitations/Future Scope
Papagiannis *et al.* [32]	Secure Model	A model named the text disclosure model to make users comply with the data disclosure policies of a company or organization Applicability of imprecise data flow tracking is demonstrated through a browser-based middleware, BROWSERFLOW	Not implemented and tested in a commercial cloud environment
Torkura *et al.* [173]	Secure Framework	Risk-driven Fault Injection (RDFI) techniques for mitigating human errors and misconfiguration errors in a cloud environment RDFI utilizes chaos engineering principles to execute, monitor, analyze and plan security fault injection campaigns	A more intelligent recovery strategy can be implemented Performance can be improved and the overhead can be reduced due to network issues Performance of the attack graph can be analyzed Other cloud services can also be considered

3.15 Ransomware (T15)

Ransomware is a type of malware that affects the availability of the system or service by encrypting the data and thereby making it unusable. Amar *et al.* proposed a mechanism that leverages big data processing on log files which was discussed in Section 3.1. Mishra *et al.* proposed a security architecture named NvCloudIDS, which was discussed in Section 3.4. Mahajan and Peddoju proposed an integrated approach which was discussed in Section 3.4. Bhattacharya and Kumar [103] described cloud architecture, presenting security-related threats that can harm the cloud. Security implications due to ransomware were highlighted, and different vulnerabilities raised due to ransomware were described. Finally, a mechanism for mitigating the threats due to ransomware was proposed. The summary of solutions for T15 is given in Table 18.

3.16 Spectre and Meltdown (T16)

Spectre and Meltdown are hardware vulnerabilities observed in Intel chips that allow attackers to read sensitive data at the hardware level. Patching these vulnerabilities is difficult and affects the system's performance when patched. As these are the latest threats, no major research was carried out to mitigate them in the context of cloud computing.

3.17 Unprotected IoT Devices (T17)

IoT is a new technology that allows sensors and other devices to be deployed for collecting data regarding an object or its properties and taking necessary actions. Example applications of IoT include smart homes, smart cities, smart grids, smart healthcare, etc. One essential component of IoT is the cloud which is generally used to store and process data gathered from sensors. As sensors can be accessed by anyone and as there is less control over them, attackers can compromise them and gain access to the cloud. Challa *et al.* created a new authentication scheme for performing authentication between a user and a cloud server which was discussed in Section 3.6. Mahajan and Peddoju proposed an integrated approach which was discussed in Section 3.4. Taylor and Shue proposed a system that clouds middleboxes to secure the connections from residential networks to malicious TLS servers, which was discussed in Section 3.12.

4 Real-World Examples of Cloud Computing

In this section real-world examples are discussed for all the threats mentioned in Section 2.

4.1 Data Breaches (T01)

In March 2021, the Microsoft Threat Intelligence Center (MSTIC) [211] announced that a Chinese state-sponsored threat actor group named Hafnium infiltrated systems running Exchange Server software and exfiltrated information related to 30,000 organizations. On April 6th, 2021, Facebook announced [212] the data of 533 million Facebook users was shared online for free in a hacking forum. The breach was a

Table 18. T15 solutions summary

Author(s)	Solution Category	Summary	Limitations/Future Scope
Bhattacharya and Kumar [103]	Secure Framework	A mechanism for mitigating the threats due to ransomware was proposed	Not tested against various security attacks Not implemented and tested in a commercial cloud environment

result of misconfiguration in their contact importer. Using this vulnerability, the hackers were able to scrap the data. In May 2021, the U.S.-based Colonial Pipeline suffered a breach [213] which was suspected to be done by the Russian cybercrime group named DarkSide. The attackers stole 100GB of data and demanded a ransom of 5 million dollars.

4.2 Data Loss (T02)

The Alzheimer's Association is a charity of 2,800 employees who work to eradicate this disease. They faced a problem when one of their departing employees intentionally or unintentionally deleted all his emails [214]. The deleted emails contained critical information for the major fundraising initiative. The lost data was recovered using the Spanning Backup for Google Apps. London-based marketing agency Bartle Bogle Hegarty (BBH) faced data loss when an employee unwittingly cleaned up over 1000 folders and files. BBH was able to recover the data with the help of a backup provider but was unable to restore the folders and files metadata. In 2009, the budding social bookmarking site named Ma.gnolia suffered a severe data loss due to a complete outage [215]. All the user data got corrupted and was irretrievable. Although the site had an on-site backup, it backed up the corrupted data making it infeasible to restore it. Due to this, the site had no other option but to close.

4.3 Malicious Insiders (T03)

In 2017, an employee working at Bupa copied the information and deleted the database after acquiring access via an in-house CRM system [216]. He tried to sell the information on the Dark Web. The information contained details of about 5,47,000 customers. After an investigation, Bupa was fined a sum of 1,75,000 pounds. In July 2020, an employee working at General Electric (GE) exfiltrated over 8000 sensitive files from GE's system that contained proprietary data and trade secrets [217]. He took help from the IT administrator to access the files and emailed them to a co-conspirator. In December 2020, a San Jose resident named Sudhish Kasaba Ramesh, an ex-employee at Cisco, was found guilty by the court of installing malware that deleted over 16,000 accounts resulting in a loss of 2.4 million dollars [218].

4.4 Denial of Service (T04)

In 2018, the software developer platform GitHub suffered from a massive DDoS attack which clocked in at 1.35 Tbps and lasted for around 20 minutes [219]. Although they were prepared for such attacks, their systems were overwhelmed by this large volumetric attack which resulted in interrupted service. In 2020, Google reported a bandwidth-consuming DDoS attack from three Chinese IPs [220]. The attack lasted for six months and peaked at a rate of 2.5 Tbps. The attackers sent 167 million packets per second to 1,80,000 exposed DNS and SMPT servers which resulted in sending large responses back to Google servers. In 2014, CloudFlare, a cybersecurity provider was hit by a DDoS attack that peaked at around 400 Gbps of traffic. The attack was launched using a vulnerability in the Network Time Protocol (NTP). Although the attack was targeted toward a single CloudFlare customer, it was powerful enough to disrupt CloudFlare's services.

4.5 Vulnerable Systems and APIs (T05)

In 2020, Slickwraps, a custom skin design company was breached [221]. The hacker responsible for the breach used the company's customization tool which contained a remote code execution vulnerability to upload a file that granted access to their server. In 2020, the cosmetic giant, Estee Lauder suffered a data breach in which 440 million customer records were accessible to the public [222]. The data exposure was due to the vulnerabilities in the middleware. In 2020, Datpiff, a music distribution company faced a data breach in which the data related to 7.5 million users was sold publicly on the Internet [223]. The attacker used a vulnerability scanner to gain access to their server and get hold of the database.

4.6 Weak Authentication and Identity Management (T06)

In Jan 2022, OG, a department store suffered from a data breach where the data related to basic and gold tier customers was exposed [224]. Their database which was managed by an external third-party membership portal provider was compromised due to weak authentication. In 2020, GEDMatch, a website allowing users to know about their ancestors or relatives

by uploading their DNA suffered a data breach where the data of 1.4 million people was accessed [225]. The attack was carried out by confiscating an existing user account. In 2020, two insurance portals suffered a data breach in which the attackers accessed the member's details like names, claim information, etc. This attack was a result of credential stuffing which used the database from MyFitnessPal data breach [226].

4.7 Account Hijacking (T07)

In March 2020, Marriott found that their guest's information was accessed by a perpetrator who got hold of the account credentials of two of its employees [227]. The information that was accessed consisted of contact information, personal details, and other linked data. In April 2020, Nintendo suffered a data breach that exposed the accounts of 1,60,000 customers [228]. The hackers used the account details for making purchases and viewing other personal information. In April 2020, Zoom, the famous teleconferencing app faced a data breach where 5,00,000 accounts were being sold on the dark web [229]. The hackers used reusable passwords to hijack the accounts.

4.8 Shared Technology Vulnerabilities (T08)

In 2019, 100 million customer accounts and credit card applications of Capital One bank were breached [230]. The attack was performed by exploiting a misconfigured web application firewall which provided access to an Amazon S3 bucket. In 2020, over 39 million records that belong to View Media, an online marketing company were breached [231]. The records were residing in an Amazon S3 bucket which was not properly secured. Symantec, a well-known security provider reported that they found that attackers were using a Virtual VM to install malware on the target compromised machines [232]. The VM was running Windows 7 and it is delivered via a malicious installer.

4.9 Lacking Due Diligence (T09)

In 2020, BigFooty a popular app where Australian football fans can chat exposed their 132 GB of sensitive data to the public [233]. On being reported, AWS, their web host took the server offline. The exposure of data was due to a misconfiguration. In 2020, Russia's Sunburst cyber espionage campaign breached 100 companies including popular U.S. agencies and departments [234]. The success of these attacks was due to the weakness in the underlying cloud and local network systems. Cloud consumers should check whether the service providers are up to date with the security-related measures and certifications or not.

4.10 Advanced Persistent Threats (APT) (T10)

In 2021, Panasonic has announced that their servers faced a data breach in which the threat actors accessed their servers for months [235]. It has been said that the information of job applicants, details of business partners, and business-related information was accessed. In December 2020, nearly 18,000 public and private networks in the USA were breached [236]. The attack was conducted by placing malware into the SolarWinds software. In 2013, Target faced a data breach in which the attackers stole 41 million credit card details which resulted in 61 million dollars in cost [237]. It was a multi-stage attack that included even a custom design malware.

4.11 Abuse of Cloud Services (T11)

In 2018, Russian secret services reported that a few of the employees working in the nuclear research lab were arrested as they were suspected of using the facility's supercomputer for mining bitcoin [238]. The NCC Group and Fox-IT observed during their investigation that a threat group was using Google and Microsoft's cloud services for conducting attacks on various targets [239]. The attackers primarily gather credentials and collect data from their cloud services which is used for further infiltration into companies' systems.

4.12 Lack of Responsibility (T12)

In 2019, a staff member at Australian National University fell victim to a spear phishing campaign that resulted in a data breach [240]. The attackers stole 700 MB of data that contained the personal information of the staff and students. In March 2020, the biometric details maintained by a Brazilian company were hacked. The information included 76,000 fingerprints [241]. The company showed negligence in protecting the database with fingerprints on the cloud which resulted in the breach. In October 2019, LifeLabs, a Canadian medical testing company suffered a data breach that allowed the attackers to access records of 15 million Canadians making it the largest data breach in Canadian history [242]. The data that was breached was unsecured and unencrypted and the security personnel was not properly trained.

4.13 Insufficient Security Tools (T13)

There are no specific reported events for this threat to the best of my knowledge as it is more generic. All the security tools like firewalls, IDS/IPS, network monitoring software, antivirus software, etc. must be extended so that they can be used effectively to detect

and prevent attacks geared towards the cloud.

4.14 Human Error (T14)

In December 2019, a researcher from Comparitech found out that details of 250 million Microsoft customers were available for public access [243]. This could have left the customers open to phishing attacks. Microsoft secured the data within 24 hrs after being notified about the breach. In mid-2019, an employee in the HR department accidentally sent an email to the team of senior executives which contained the medical and personal information of 24 NHS employees [244]. Although the employee apologized later, this could have resulted in medical identity theft and even physical harm to the patients. The details of the NHS coronavirus contact-tracing app were leaked when the documents stored in Google Drive were left open for access to anyone who has the link [245]. This was a mistake from the person who set the wrong access permissions to the documents.

4.15 Ransomware (T15)

In March 2020, ExecuPharm, a pharmaceutical research company was hit by a ransomware attack in which the CLOP ransomware group encrypted the data on the servers and demanded a ransom in order to decrypt it [246]. The attackers got access to the servers via a phishing campaign targeted at the company employees. In April 2020, Cognizant was hit by a ransomware attack in which the attackers installed malware on the company servers, encrypted the data and demanded a ransom for restoring it [247]. The company had reportedly paid a sum of 50 to 50 million dollars as a ransom. In 2021, Memorial Health System faced a ransomware attack where the information of 2,00,000 was accessed by the attacker [248]. The data on their servers was encrypted. With the help of the FBI, they were able to unlock the servers.

4.16 Spectre and Meltdown (T16)

TheVerge reported that the hardware vulnerabilities named Meltdown and Spectre will affect every processor that was made in the last 20 years [249]. Proof-of-Concept exploits are already available for Meltdown. A lot of big tech companies said that they already patched their systems. No one knows whether it is true or not. There is always a possibility of using the existing vulnerabilities to create or develop new attack vectors.

4.17 Unprotected IoT Devices (T17)

In September 2016, a security expert's blog was taken down with the help of a DDoS attack that sent 620 Gbps traffic [250]. The source of the attack was the Mirai botnet which consisted of about 6,00,000 compromised IoT devices like routers, IP cameras, etc. In October 2016, one of the largest DNS providers, Dyn was hit by a massive DDoS attack using the Mirai botnet [251]. The attack rate was 1.5 Tbps which was huge. This caused major disruptions in the service and took down major websites like GitHub, Rediff, Paypal, etc. In 2016, at least five Russian banks suffered a DDoS attack that came from a botnet involving 24,000 computers and IoT devices that were located across 30 countries. This is said to be the first DDoS attack to be carried out against Russian banks at such a scale.

5 Conclusions

Cloud computing is the next big thing for small to large businesses and organizations. Irrespective of its advantages and characteristics, security remains a major concern among businesses to adopt cloud computing. A vast amount of research has been carried out on cloud computing security until now. Yet, there is no major contribution in identifying the threats and vulnerabilities in cloud computing by considering the latest threats like ransomware, hardware vulnerabilities, and IoT devices. Also, there is no comprehensive state-of-the-art of countermeasures and solutions for mitigating the threats and vulnerabilities in recent years. Therefore the goal of this research is to study the recent literature and analyze the research contributions based on different threats in cloud computing. Based on the analysis done, major contributions in the recent literature were towards solving the problems related to data security followed by methods for mitigating the threats related to shared technologies like virtualization and hypervisors. In recent years new threats like ransomware, Spectre and Meltdown, and unprotected IoT devices came to light. The research literature related to these new threats is not significant, and more amount of research should be concerned with reducing the effect of these new threats. A taxonomy of threats and related vulnerabilities is given, which can be used by cloud stakeholders to strengthen the cloud defenses and also can serve as a base for discussions regarding cloud threats and vulnerabilities. State-of-the-art countermeasures and solutions are provided for each cloud computing threat by considering research literature after 2014, although very few articles of significant importance before 2014 were also included. Data breaches and shared technology solutions are far greater when compared to other threats. More solutions should be proposed or developed to address the latest threats in cloud computing.

Limitations of this Research

The author has taken proper care in including almost all the relevant papers from major repositories and even those indexed by Google Scholar. Though most of the relevant papers have been included, the author cannot guarantee that all the relevant papers were considered while conducting this research. Articles from repositories like IACR (International Association for Cryptologic Research), arXiv, etc., were not included. Also, while the manuscript is peer-reviewed and published, some relevant papers might be published.

Declarations

Acknowledgements

I would like to thank my parents for their support and I am much thankful to reviewers and journal authorities.

Funding

This research didn't receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

[1] P M Mell and T Grance. The NIST definition of cloud computing. Technical report, National Institute of Standards and Technology, Gaithersburg, MD, 2011.

[2] Oracle. ORACLE AND KPMG CLOUD THREAT REPORT 2019 Defining Edge Intelligence: Closing Visibility Gaps with a Layered Defense Strategy Read Full Report. Technical report, 2019.

[3] Netskope. 2019 Cloud Security Report, 2019.

[4] Issa Khalil, Abdallah Khreishah, and Muhammad Azeem. Cloud Computing Security: A Survey. *Computers*, 3(1):1–35, feb 2014.

[5] Nelson Gonzalez, Charles Miers, Fernando Redígolo, Marcos Simplício, Tereza Carvalho, Mats Näslund, and Makan Pourzandi. A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing*, 1(1):1–18, jul 2012.

[6] Keiko Hashizume, David G. Rosado, Eduardo Fernández-Medina, and Eduardo B. Fernandez. An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4(1):1–13, feb 2013.

[7] Mazhar Ali, Samee U. Khan, and Athanasios V. Vasilakos. Security in cloud computing: Opportunities and challenges. *Information Sciences*, 305:357–383, jun 2015.

[8] Minhaj Ahmad Khan. A survey of security issues for cloud computing, aug 2016.

[9] Luigi Coppolino, Salvatore D'Antonio, Giovanni Mazzeo, and Luigi Romano. Cloud security: Emerging threats and current solutions. *Computers and Electrical Engineering*, 59:126–140, apr 2017.

[10] Gururaj Ramachandra, Mohsin Iftikhar, and Farrukh Aslam Khan. A Comprehensive Survey on Security in Cloud Computing. In *Procedia Computer Science*, volume 110, pages 465–472. Elsevier B.V., jan 2017.

[11] Ashish Singh and Kakali Chatterjee. Cloud security issues and challenges: A survey, feb 2017.

[12] Srijita Basu, Arjun Bardhan, Koyal Gupta, Payel Saha, Mahasweta Pal, Manjima Bose, Kaushik Basu, Saunak Chaudhury, and Pritika Sarkar. Cloud computing security challenges & solutions-A survey. In *2018 IEEE 8th Annual Computing and Communication Workshop and Conference, CCWC 2018*, volume 2018-Janua, pages 347–356. Institute of Electrical and Electronics Engineers Inc., feb 2018.

[13] Jin B. Hong, Armstrong Nhlabatsi, Dong Seong Kim, Alaa Hussein, Noora Fetais, and Khaled M. Khan. Systematic identification of threats in the cloud: A Survey. *Computer Networks*, 150:46–69, feb 2019.

[14] Rakesh Kumar and Rinkaj Goyal. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review*, 33:1–48, 2019.

[15] M. Swathy Akshaya and G. Padmavathi. *Taxonomy of Security Attacks and Risk Assessment of Cloud Computing*, volume 750. Springer Singapore, 2019.

[16] Lubna Alhenaki, Alaa Alwatban, Bashaer Alamri, and Noof Alarifi. A Survey on the Security of Cloud Computing. *2nd International Conference on Computer Applications and Information Security, ICCAIS 2019*, pages 1–7, 2019.

[17] Hamed Tabrizchi and Marjan Kuchaki Rafsanjani. A survey on security challenges in cloud computing: issues, threats, and solutions. *Journal of Supercomputing*, 76(12):9493–9532, dec 2020.

[18] Siyakha N. Mthunzi, Elhadj Benkhelifa, Tomasz Bosakowski, Chirine Ghedira Guegan, and Mahmoud Barhamgi. Cloud computing security taxonomy: From an atomistic to a holistic view. *Future Generation Computer Systems*, 107:620–644, jun 2020.

[19] Shailendra Mishra, Sunil Kumar Sharma, and Majed A. Alowaidi. Analysis of security issues

of cloud-based web applications, 2020.

[20] Umer Ahmed Butt, Muhammad Mehmood, Syed Bilal Hussain Shah, Rashid Amin, M. Waqas Shaukat, Syed Mohsan Raza, Doug Young Suh, and Md Jalil Piran. A review of machine learning algorithms for cloud computing security. *Electronics (Switzerland)*, 9(9):1–25, 2020.

[21] Nnamdi Chuka-Maduji and Vaibhav Anu. Cloud Computing Security Challenges and Related Defensive Measures: A Survey and Taxonomy. *SN Computer Science*, 2(4), 2021.

[22] P.S. Suryateja. Threats and Vulnerabilities of Cloud Computing A Review. *International Journal of Computer Sciences and Engineering*, 6(3):297–302, mar 2018.

[23] P.S. Suryateja. Cloud Service Models Threats and Vulnerabilities: A Review. *International Journal on Future Revolution in Computer Science & Communication Engineering*, 4(4):563–567, 2018.

[24] Mihai Christodorescu, Reiner Sailer, Douglas Lee Schales, Daniele Sgandurra, and Diego Zamboni. Cloud security is not (just) virtualization security. *Proceedings of the 2009 ACM workshop on Cloud computing security - CCSW '09*, page 97, 2009.

[25] Adam Bates, Benjamin Mood, Joe Pletcher, Hannah Pruse, Masoud Valafar, and Kevin Butler. Detecting co-residency with active traffic analysis techniques. In *Proceedings of the ACM Conference on Computer and Communications Security*, pages 1–12, New York, New York, USA, 2012. ACM Press.

[26] Muhammad Kazim, Rahat Masood, and Muhammad Awais Shibli. Securing the virtual machine images in Cloud computing. In *SIN 2013 - Proceedings of the 6th International Conference on Security of Information and Networks*, pages 425–428, New York, New York, USA, 2013. ACM Press.

[27] Yinqian Zhang, Ari Juels, Michael K. Reiter, and Thomas Ristenpart. Cross-tenant side-channel attacks in PaaS clouds. In *Proceedings of the ACM Conference on Computer and Communications Security*, pages 990–1003, New York, NY, USA, nov 2014. Association for Computing Machinery.

[28] Vikas Jaiman and Gaurav Somani. An order preserving encryption scheme for cloud computing. In *ACM International Conference Proceeding Series*, volume 2014-September, pages 211–216, New York, New York, USA, sep 2014. Association for Computing Machinery.

[29] Hussain Aljafer, Zaki Malik, Mohammed Alodib, and Abdelmounaam Rezgui. An experimental evaluation of data confidentiality measures on the cloud. In *MEDES 2014 - 6th International Conference on Management of Emergent Digital EcoSystems, Proceedings*, pages 117–124, New York, New York, USA, sep 2014. Association for Computing Machinery, Inc.

[30] Jakub Szefer, Pramod Jamkhedkar, Diego Perez-Botero, and Ruby B. Lee. Cyber defenses for physical attacks and insider threats in cloud computing. In *ASIA CCS 2014 - Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security*, pages 519–524, New York, NY, USA, jun 2014. Association for Computing Machinery, Inc.

[31] Wei Huang, Afshar Ganjali, Beom Heyn Kim, Sukwon Oh, and David Lie. The State of Public Infrastructure-as-a-Service Cloud Security. *ACM Computing Surveys*, 47(4):1–31, 2015.

[32] Ioannis Papagiannis, Pijika Watcharapichat, Divya Muthukumaran, and Peter Pietzuch. BrowserFlow: Imprecise data flow tracking to prevent accidental data disclosure. In *Proceedings of the 17th International Middleware Conference, Middleware 2016*, pages 1–13, New York, NY, USA, nov 2016. Association for Computing Machinery, Inc.

[33] Xiaojing Liao, Chang Liu, Damon McCoy, Elaine Shi, Shuang Hao, and Raheem Beyah. Characterizing long-Tail SEO spam on cloud web hosting services. In *25th International World Wide Web Conference, WWW 2016*, pages 321–332, Republic and Canton of Geneva, Switzerland, apr 2016. International World Wide Web Conferences Steering Committee.

[34] Manel Medhioub, Mohamed Hamdi, and Tai-Hoon Kim. A New Authentication Scheme for Cloud-based Storage Applications. *Proceedings of the 9th International Conference on Security of Information and Networks - SIN '16*, pages 57–60, 2016.

[35] Priya Anand, Jungwoo Ryoo, Hyoungshick Kim, and Eunhyun Kim. Threat Assessment in the Cloud Environment – A Quantitative Approach for Security Pattern Selection. *Imcom '16*, page 8, 2016.

[36] Xiaojing Liao, Sumayah Alrwais, Kan Yuan, Luyi Xing, Xiaofeng Wang, Shuang Hao, and Raheem Beyah. Lurking malice in the cloud: Understanding and detecting cloud repository as a malicious service. In *Proceedings of the ACM Conference on Computer and Communications Security*, volume 24-28-October-2016, pages 1541–1552, New York, NY, USA, oct 2016. Association for Computing Machinery.

[37] Upasana Nagar, Xiangjian He, Priyadarsi Nanda, and Zhiyuan Tan. A Framework for

Data Security in Cloud using Collaborative Intrusion Detection Scheme. In *ACM International Conference Proceeding Series*, pages 188–193, New York, NY, USA, oct 2017. Association for Computing Machinery.

[38] Saadi Chaimae and Chaoui Habiba. A new approach to mitigate security threats in cloud environment. In *ACM International Conference Proceeding Series*, pages 1–7, New York, NY, USA, mar 2017. Association for Computing Machinery.

[39] Kashyap Thimmaraju, Bhargava Shastry, Tobias Fiebig, Felicitas Hetzelt, Jean Pierre Seifert, Anja Feldmann, and Stefan Schmid. Taking control of cloud systems via the unified packet parser. In *CCSW 2017 - Proceedings of the 2017 Cloud Computing Security Workshop, co-located with CCS 2017*, pages 11–15, New York, NY, USA, nov 2017. Association for Computing Machinery, Inc.

[40] Amar Meryem, Douzi Samira, and El Ouahidi Bouabid. Enhancing cloud security using advanced MapReduce k-means on log files. In *ACM International Conference Proceeding Series*, pages 63–67, New York, New York, USA, jan 2018. Association for Computing Machinery.

[41] Dimitrios Zissis and Dimitrios Lekkas. Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3):583–592, mar 2012.

[42] Xiangjian He, Thawatchai Chomsiri, Priyadarsi Nanda, and Zhiyuan Tan. Improving cloud network security using the Tree-Rule firewall. *Future Generation Computer Systems*, 30(1):116–126, jan 2014.

[43] Yong Yu, Yafang Zhang, Jianbing Ni, Man Ho Au, Lanxiang Chen, and Hongyu Liu. Remote data possession checking with enhanced security for cloud storage. *Future Generation Computer Systems*, 52:77–85, jul 2015.

[44] Brian Cusack and Eghbal Ghazizadeh. Evaluating single sign-on security failure in cloud services. *Business Horizons*, 59(6):605–614, nov 2016.

[45] Manish M. Potey, C. A. Dhote, and Deepak H. Sharma. Homomorphic Encryption for Security of Cloud Data. In *Procedia Computer Science*, volume 79, pages 175–181. Elsevier B.V., jan 2016.

[46] Naresh Vurukonda and B. Thirumala Rao. A Study on Data Storage Security Issues in Cloud Computing. In *Procedia Computer Science*, volume 92, pages 128–135. Elsevier B.V., jan 2016.

[47] Salman Iqbal, Miss Laiha Mat Kiah, Babak Dhaghighi, Muzammil Hussain, Suleman Khan, Muhammad Khurram Khan, and Kim Kwang Raymond Choo. On cloud security attacks: A taxonomy and intrusion detection and prevention as a service, oct 2016.

[48] Chaimae Saadi and Habiba Chaoui. Cloud Computing Security Using IDS-AM-Clust, Honeyd, Honeywall and Honeycomb. In *Procedia Computer Science*, volume 85, pages 433–442. Elsevier B.V., jan 2016.

[49] Abdulatif Alabdulatif, Heshan Kumarage, Ibrahim Khalil, and Xun Yi. Privacy-preserving anomaly detection in cloud with lightweight homomorphic encryption. *Journal of Computer and System Sciences*, 90:28–45, dec 2017.

[50] Laurence T. Yang, Gaoyuan Huang, Jun Feng, and Li Xu. Parallel GNFS algorithm integrated with parallel block Wiedemann algorithm for RSA security in cloud computing. *Information Sciences*, 387:254–265, may 2017.

[51] Kyriakos Kritikos, Tom Kirkham, Bartosz Kryza, and Philippe Massonet. Towards a security-enhanced PaaS platform for multi-cloud applications. *Future Generation Computer Systems*, 67:206–226, feb 2017.

[52] I. Indu, P. M. Rubesh Anand, and Vidhyacharan Bhaskar. Encrypted token based authentication with adapted SAML technology for cloud web services, dec 2017.

[53] Carlos André Batista de Carvalho, Rossana Maria de Castro Andrade, Miguel Franklin de Castro, Emanuel Ferreira Coutinho, and Nazim Agoulmine. State of the art and challenges of security SLA for cloud computing. *Computers and Electrical Engineering*, 59:141–152, apr 2017.

[54] Nesrine Kaaniche and Maryline Laurent. Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms, oct 2017.

[55] Hui Cui, Robert H. Deng, and Yingjiu Li. Attribute-based cloud storage with secure provenance over encrypted data. *Future Generation Computer Systems*, 79:461–472, feb 2018.

[56] Jie Cui, Han Zhou, Hong Zhong, and Yan Xu. AKSER: Attribute-based keyword search with efficient revocation in cloud computing. *Information Sciences*, 423:343–352, jan 2018.

[57] Sravani Challa, Ashok Kumar Das, Prosanta Gope, Neeraj Kumar, Fan Wu, and Athanasios V. Vasilakos. Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems. *Future Generation Computer Systems*, 108:1267–1286, jul 2020.

[58] Wenying Zheng, Dengzhi Liu, Xiong Li, and

Arun Kumar Sangaiah. Secure sustainable storage auditing protocol (SSSAP) with efficient key updates for cloud computing. *Sustainable Computing: Informatics and Systems*, 28:100237, dec 2020.

[59] Sreeja Cherillath Sukumaran and Misbahuddin Mohammed. PCR and Bio-signature for data confidentiality and integrity in mobile cloud computing. *Journal of King Saud University - Computer and Information Sciences*, mar 2018.

[60] P. Ravi Kumar, P. Herbert Raj, and P. Jelciana. Exploring Data Security Issues and Solutions in Cloud Computing. In *Procedia Computer Science*, volume 125, pages 691–697. Elsevier B.V., jan 2018.

[61] Choon Beng Tan, Mohd Hanafi Ahmad Hijazi, Yuto Lim, and Abdullah Gani. A survey on Proof of Retrievability for cloud data integrity and availability: Cloud storage state-of-the-art, issues, solutions and future trends, may 2018.

[62] Akshay A. Nayak, N. K. Sridhar, G. R. Poornima, and Shivashankar. Security issues in cloud computing and its counter measure. In *RTEICT 2017 - 2nd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, Proceedings*, volume 2018-January, pages 35–41. Institute of Electrical and Electronics Engineers Inc., jul 2017.

[63] Mazhar Ali, Saif U. R. Malik, and Samee U. Khan. DaSCE: Data Security for Cloud Environment with Semi-Trusted Third Party. *IEEE Transactions on Cloud Computing*, 5(4):642–655, jun 2015.

[64] Meryem Amar, Mouad Lemoudden, and Bouabid EL Ouahidi. Log file's centralization to improve cloud security. In *Proceedings of 2016 International Conference on Cloud Computing Technologies and Applications, CloudTech 2016*, pages 178–183. Institute of Electrical and Electronics Engineers Inc., feb 2017.

[65] Kunding Fang, Xiaohong Li, Jianye Hao, and Zhiyong Feng. Formal Modeling and Verification of Security Protocols on Cloud Computing Systems Based on UML 2.3. In *2016 IEEE Trustcom/BigDataSE/ISPA*, 2016.

[66] Nasir Uddin and Mohammad Jabr. File upload security and validation in context of software as a service cloud model. In *2016 6th International Conference on IT Convergence and Security, ICITCS 2016*. Institute of Electrical and Electronics Engineers Inc., nov 2016.

[67] Kunal V. Raipurkar and Anil V. Deorankar. Improve data security in cloud environment by using LDAP and two way encryption algorithm. In *2016 Symposium on Colossal Data Analysis and Networking, CDAN 2016*. Institute of Electrical and Electronics Engineers Inc., sep 2016.

[68] Haoyu Chen, Shanshan Tu, Chunye Zhao, and Yongfeng Huang. Provenance cloud security auditing system based on log analysis. In *Proceedings of 2016 IEEE International Conference of Online Analysis and Computing Science, ICOACS 2016*, pages 155–159. Institute of Electrical and Electronics Engineers Inc., sep 2016.

[69] Thomas Lorünser, Daniel Slamanig, Thomas Länger, and Henrich C. Pöhls. PRISMACLOUD tools: A cryptographic toolbox for increasing security in cloud services. In *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016*, pages 733–741. Institute of Electrical and Electronics Engineers Inc., dec 2016.

[70] Preeti Mishra, Emmanuel S. Pilli, Vijay Varadharajant, and Udaya Tupakula. NvCloudIDS: A security architecture to detect intrusions at network and virtualization layer in cloud environment. In *2016 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2016*, pages 56–62. Institute of Electrical and Electronics Engineers Inc., nov 2016.

[71] Deepak Singh and Harsh K. Verma. A new framework for cloud storage confidentiality to ensure information security. In *2016 Symposium on Colossal Data Analysis and Networking, CDAN 2016*. Institute of Electrical and Electronics Engineers Inc., sep 2016.

[72] Yiannis Verginadis, Ioannis Patiniotakis, Gregoris Mentzas, Simeon Veloudis, and Iraklis Paraskakis. Data Distribution and Encryption Modelling for PaaS-enabled Cloud Security. *2016 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, pages 497–502, 2016.

[73] Chandan Prakash and Surajit Dasgupta. Cloud computing security analysis: Challenges and possible solutions. In *International Conference on Electrical, Electronics, and Optimization Techniques, ICEEOT 2016*, pages 54–57. Institute of Electrical and Electronics Engineers Inc., nov 2016.

[74] Sancha Pereira, Andre Alves, Nuno Santos, and Ricardo Chaves. Storekeeper: A Security-Enhanced Cloud Storage Aggregation Service. In *Proceedings of the IEEE Symposium on Reliable Distributed Systems*, pages 111–120. IEEE Computer Society, dec 2016.

[75] Napoleon C. Paxton. Cloud security: A review of current issues and proposed solutions. In *Proceedings - 2016 IEEE 2nd International Conference on Collaboration and Internet Computing,*

IEEE CIC 2016, pages 452–455. Institute of Electrical and Electronics Engineers Inc., jan 2017.

[76] Justin Lejeune, Cara Tunstall, Kuo Pao Yang, and Ihssan Alkadi. An algorithmic approach to improving cloud security: The MIST and Malachi algorithms. In *IEEE Aerospace Conference Proceedings*, volume 2016-June. IEEE Computer Society, jun 2016.

[77] Ankit Grover and Banpreet Kaur. A framework for cloud data security. In *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016*, pages 1199–1203. Institute of Electrical and Electronics Engineers Inc., jan 2017.

[78] Bin Feng, Xinzhu Ma, Cheng Guo, Hui Shi, Zhangjie Fu, and Tie Qiu. An Efficient Protocol with Bidirectional Verification for Storage Security in Cloud Computing. *IEEE Access*, 4:7899–7911, 2016.

[79] Bob Duncan, Alfred Bratterud, and Andreas Happe. Enhancing cloud security and privacy: Time for a new approach? In *2016 6th International Conference on Innovative Computing Technology, INTECH 2016*, pages 110–115. Institute of Electrical and Electronics Engineers Inc., feb 2017.

[80] J. Vijaya Chandra, Narasimham Challa, and Sai Kiran Pasupuleti. Advanced persistent threat defense system using self-destructive mechanism for cloud security. In *Proceedings of 2nd IEEE International Conference on Engineering and Technology, ICETECH 2016*, pages 7–11. Institute of Electrical and Electronics Engineers Inc., sep 2016.

[81] Valentina Casola, Alessandra De Benedictis, Madalina Erascu, Massimiliano Rak, and Umberto Villano. A Security SLA-driven Methodology to Set-Up Security Capabilities on Top of Cloud Services. In *Proceedings - 2016 10th International Conference on Complex, Intelligent, and Software Intensive Systems, CISIS 2016*, pages 549–554. Institute of Electrical and Electronics Engineers Inc., dec 2016.

[82] Deval Bhamare, Tara Salman, Mohammed Samaka, Aiman Erbad, and Raj Jain. Feasibility of Supervised Machine Learning for Cloud Security. In *ICISS 2016 - 2016 International Conference on Information Science and Security*. Institute of Electrical and Electronics Engineers Inc., mar 2017.

[83] Farhad Ahamed, Seyed Shahrestani, and Bahman Javadi. Security Aware and Energy-Efficient Virtual Machine Consolidation in Cloud Computing Systems. In *2016 IEEE Trustcom/BigDataSE/ISPA*, pages 1516–1523. IEEE, aug 2016.

[84] Chuanyi Liu, Guofeng Wang, Peiyi Han, Hezhong Pan, and Binxing Fang. A Cloud Access Security Broker based approach for encrypted data search and sharing. In *2017 International Conference on Computing, Networking and Communications, ICNC 2017*, pages 422–426. Institute of Electrical and Electronics Engineers Inc., mar 2017.

[85] Ihsen Nakouri, Mohamed Hamdi, and Tai Hoon Kim. A new biometric-based security framework for cloud storage. In *2017 13th International Wireless Communications and Mobile Computing Conference, IWCMC 2017*, pages 390–395. Institute of Electrical and Electronics Engineers Inc., jul 2017.

[86] Hang Wei, Guan Yu Hu, Xiaoxia Han, Peili Qiao, Zhiguo Zhou, Zhi Chao Feng, and Xiao Jing Yin. A New BRB Model for Cloud Security-State Prediction Based on the Large-Scale Monitoring Data. *IEEE Access*, 6:11907–11920, dec 2017.

[87] Shengli Zhou, Lifa Wu, and Canghong Jin. A privacy-based SLA violation detection model for the security of cloud computing. *China Communications*, 14(9):155–165, sep 2017.

[88] Bhale Pradeepkumar Gajendra, Vinay Kumar Singh, and More Sujeet. Achieving cloud security using third party auditor, MD5 and identity-based encryption. In *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016*, pages 1304–1309. Institute of Electrical and Electronics Engineers Inc., jan 2017.

[89] Feng Gao. Application of Generalized Regression Neural Network in Cloud Security Intrusion Detection. In *Proceedings - 2017 International Conference on Robots and Intelligent System, ICRIS 2017*, pages 54–57. Institute of Electrical and Electronics Engineers Inc., nov 2017.

[90] Sandeep Pisharody, Janakarajan Natarajan, Ankur Chowdhary, Abdullah Alshalan, and DIjiang Huang. Brew: A Security Policy Analysis Framework for Distributed SDN-Based Cloud Environments. *IEEE Transactions on Dependable and Secure Computing*, 16(6):1011–1025, nov 2019.

[91] Naseer Amara, Huang Zhiqui, and Awais Ali. Cloud Computing Security Threats and Attacks with Their Mitigation Techniques. In *Proceedings - 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2017*, volume 2018-January, pages 244–251. Institute of Electrical and Electronics Engineers Inc., jul 2017.

[92] Manjur Kolhar, Mosleh M. Abu-Alhaj, and Saied M. Abd El-Atty. Cloud data auditing techniques with a focus on privacy and security. *IEEE Security and Privacy*, 15(1):42–51, jan 2017.

[93] Dean C. Mumme, Brooke Wallace, and Robert McGraw. Cloud Security via Virtualized Out-of-Band Execution and Obfuscation. In *IEEE International Conference on Cloud Computing, CLOUD*, volume 2017-June, pages 286–293. IEEE Computer Society, sep 2017.

[94] Carlo Di Giulio, Read Sprabery, Charles Kamhoua, Kevin Kwiat, Roy H. Campbell, and Masooda N. Bashir. Cloud Standards in Comparison: Are New Security Frameworks Improving Cloud Security? In *IEEE International Conference on Cloud Computing, CLOUD*, volume 2017-June, pages 50–57. IEEE Computer Society, sep 2017.

[95] Rushikesh Nikam and Manish Potey. Cloud storage security using Multi-Factor Authentication. In *2016 International Conference on Recent Advances and Innovations in Engineering, ICRAIE 2016*. Institute of Electrical and Electronics Engineers Inc., 2016.

[96] Xiaochen Liu, Chunhe Xia, Tianbo Wang, and Li Zhong. CloudSec: A Novel Approach to Verifying Security Conformance at the Bottom of the Cloud. In *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, pages 569–576. Institute of Electrical and Electronics Engineers Inc., sep 2017.

[97] Xing Gao, Zhongshu Gu, Mehmet Kayaalp, Dimitrios Pendarakis, and Haining Wang. ContainerLeaks: Emerging Security Threats of Information Leakages in Container Clouds. In *Proceedings - 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2017*, pages 237–248. Institute of Electrical and Electronics Engineers Inc., aug 2017.

[98] Yuri Demchenko, Fatih Turkmen, Mathias Slawik, and Cees De Laat. Defining Intercloud Security Framework and Architecture Components for Multi-cloud Data Intensive Applications. In *Proceedings - 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, CCGRID 2017*, pages 945–952. Institute of Electrical and Electronics Engineers Inc., jul 2017.

[99] Amjad Alsirhani, Peter Bodorik, and Srinivas Sampalli. Improving Database Security in Cloud Computing by Fragmentation of Data. In *2017 International Conference on Computer and Applications, ICCA 2017*, pages 43–49. Institute of Electrical and Electronics Engineers Inc., oct 2017.

[100] Varan Mahajan and Sateesh K. Peddoju. Integration of network intrusion detection systems and honeypot networks for cloud security. In *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2017*, volume 2017-January, pages 829–834. Institute of Electrical and Electronics Engineers Inc., dec 2017.

[101] Tihomir Orehovački, Darko Etinger, and Snježana Babić. Perceived security and privacy of cloud computing applications used in educational ecosystem. In *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2017 - Proceedings*, pages 717–722. Institute of Electrical and Electronics Engineers Inc., jul 2017.

[102] Nicolae Paladi, Christian Gehrmann, and Antonis Michalas. Providing User Security Guarantees in Public Infrastructure Clouds. *IEEE Transactions on Cloud Computing*, 5(3):405–419, jul 2017.

[103] S. Bhattacharya and C. R.S. Kumar. Ransomware: The CryptoVirus subverting cloud security. In *2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies, ICAMMAET 2017*, volume 2017-Janua, pages 1–6. Institute of Electrical and Electronics Engineers Inc., dec 2017.

[104] Carlos Andre Batista De Carvalho, Miguel Franklin De Castro, and Rossana Maria De Castro Andrade. Secure cloud storage service for detection of security violations. In *Proceedings - 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, CCGRID 2017*, pages 715–718. Institute of Electrical and Electronics Engineers Inc., jul 2017.

[105] Nesrine Kaaniche, Mohamed Mohamed, Maryline Laurent, and Heiko Ludwig. Security SLA Based Monitoring in Clouds. In *Proceedings - 2017 IEEE 1st International Conference on Edge Computing, EDGE 2017*, pages 90–97. Institute of Electrical and Electronics Engineers Inc., sep 2017.

[106] Mortada A. Aman and Egemen K. Cetinkaya. Towards Cloud Security Improvement with Encryption Intensity Selection. In *DRCN 2017 - Design of Reliable Communication Networks; 13th International Conference*, 2017.

[107] Curtis R. Taylor and Craig A. Shue. Validating security protocols with cloud-based middleboxes. In *2016 IEEE Conference on Communications and Network Security, CNS 2016*, pages 261–269. Institute of Electrical and Electronics

Engineers Inc., feb 2017.

[108] Kaiping Xue, Weikeng Chen, Wei Li, Jianan Hong, and Peilin Hong. Combining Data Owner-Side and Cloud-Side Access Control for Encrypted Cloud Storage. *IEEE Transactions on Information Forensics and Security*, 13(8):2062–2074, aug 2018.

[109] Jianting Ning, Zhenfu Cao, Xiaolei Dong, Kaitai Liang, Lifei Wei, and Kim Kwang Raymond Choo. CryptCloud: Secure and Expressive Data Access Control for Cloud Storage. *IEEE Transactions on Services Computing*, 14(1):111–124, jan 2021.

[110] Ahmad Shawahna, Marwan Abu-Amara, Ashraf S.H. Mahmoud, and Yahya Osais. EDoS-ADS: An Enhanced Mitigation Technique against Economic Denial of Sustainability (EDoS) Attacks. *IEEE Transactions on Cloud Computing*, 8(3):790–804, jul 2020.

[111] Jing Yao, Yifeng Zheng, Cong Wang, and Xiaolin Gui. Enabling Search over Encrypted Cloud Data with Concealed Search Pattern. *IEEE Access*, 6:11112–11122, feb 2018.

[112] Guofeng Wang, Chuanyi Liu, Yingfei Dong, Peiyi Han, Hezhong Pan, and Binxing Fang. IDCrypt: A Multi-User Searchable Symmetric Encryption Scheme for Cloud Applications. *IEEE Access*, 6:2908–2921, dec 2017.

[113] Hina Abrar, Syed Jawad Hussain, Junaid Chaudhry, Kashif Saleem, Mehmet A. Orgun, Jalal Al-Muhtadi, and Craig Valli. Risk Analysis of Cloud Sourcing in Healthcare and Public Health Industry. *IEEE Access*, 6:19140–19150, feb 2018.

[114] Ihsan H. Abdulqadder, Deqing Zou, Israa T. Aziz, Bin Yuan, and Weiming Li. SecSDN-Cloud: Defeating Vulnerable Attacks Through Secure Software-Defined Networks. *IEEE Access*, 6:8292–8301, jan 2018.

[115] Shengmin Xu, Guomin Yang, Yi Mu, and Robert H. Deng. Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups in the Cloud. *IEEE Transactions on Information Forensics and Security*, 13(8):2101–2113, aug 2018.

[116] Anirban Basu, Jaideep Vaidya, Hiroaki Kikuchi, Theo Dimitrakos, and Srijith K. Nair. Privacy preserving collaborative filtering for SaaS enabling PaaS clouds. *Journal of Cloud Computing*, 1(1):1–14, jul 2012.

[117] Aryan TaheriMonfared and Martin Gilje Jaatun. Handling compromised components in an IaaS cloud installation. *Journal of Cloud Computing: Advances, Systems and Applications*, 1(1):16, aug 2012.

[118] Roland Schwarzkopf, Matthias Schmidt, Christian Strack, Simon Martin, and Bernd Freisleben. Increasing virtual machine security in cloud environments. *Journal of Cloud Computing*, 1(1):1–12, jul 2012.

[119] Robert Denz and Stephen Taylor. A survey on securing the virtual cloud. *Journal of Cloud Computing*, 2(1):17, nov 2013.

[120] Umme Habiba, Rahat Masood, Muhammad Awais Shibli, and Muaz A. Niazi. Cloud identity management security issues & solutions: a taxonomy. *Complex Adaptive Systems Modeling*, 2(1):5, dec 2014.

[121] Nikos Fotiou, Apostolis Machas, George C. Polyzos, and George Xylomenos. Access control as a service for the Cloud. *Journal of Internet Services and Applications*, 6(1):11, dec 2015.

[122] Yang Yang. Attribute-based data retrieval with semantic keyword search for e-health cloud. *Journal of Cloud Computing*, 4(1):1–6, dec 2015.

[123] Rashmi Rai, Gadadhar Sahoo, and Shabana Mehfuz. Exploring the factors influencing the cloud computing adoption: a systematic study on cloud migration. *SpringerPlus*, 4(1):1–12, dec 2015.

[124] Md Iftekhar Salam, Wei Chuen Yau, Ji Jian Chin, Swee Huay Heng, Huo Chong Ling, Raphael C.W. Phan, Geong Sen Poh, Syh Yuan Tan, and Wun She Yap. Implementation of searchable symmetric encryption for privacy-preserving keyword search on cloud storage. *Human-centric Computing and Information Sciences*, 5(1):1–16, dec 2015.

[125] Sabout Nagaraju and Latha Parthiban. Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway. *Journal of Cloud Computing*, 4(1):1–23, dec 2015.

[126] Jongkil Kim and Surya Nepal. A Cryptographically Enforced Access Control with a Flexible User Revocation on Untrusted Cloud Storage. *Data Science and Engineering*, 1(3):149–160, sep 2016.

[127] Kefeng Fan, Xiangzhen Yao, Xiaohe Fan, Yong Wang, and Mingjie Chen. A new usage control protocol for data protection of cloud environment. *Eurasip Journal on Information Security*, 2016(1):7, dec 2016.

[128] Lewis Nkenyereye, Youngho Park, and Kyung Hyune Rhee. A secure billing protocol over attribute-based encryption in vehicular cloud computing. *Eurasip Journal on Wireless Communications and Networking*, 2016(1):196, dec 2016.

[129] Sheren A. El-Booz, Gamal Attiya, and Nawal El-Fishawy. A secure cloud storage system

combining time-based one-time password and automatic blocker protocol. *Eurasip Journal on Information Security*, 2016(1):13, dec 2016.

[130] Hanshu Hong and Zhixin Sun. An efficient and traceable KP-ABS scheme with untrusted attribute authority in cloud computing. *Journal of Cloud Computing*, 5(1):2, dec 2016.

[131] Johanna Ullrich, Jordan Cropper, Peter Frühwirt, and Edgar Weippl. The role and security of firewalls in cyber-physical cloud computing. *Eurasip Journal on Information Security*, 2016(1):18, dec 2016.

[132] Noëlle Rakotondravony, Benjamin Taubmann, Waseem Mandarawi, Eva Weishäupl, Peng Xu, Bojan Kolosnjaji, Mykolai Protsenko, Hermann de Meer, and Hans P. Reiser. Classifying malware attacks in IaaS cloud environments. *Journal of Cloud Computing*, 6(1):26, dec 2017.

[133] Niharika Singh and Ashutosh Kumar Singh. Data Privacy Protection Mechanisms in Cloud, mar 2018.

[134] Abdul Razaque and Syed S. Rizvi. Privacy preserving model: a new scheme for auditing cloud stakeholders. *Journal of Cloud Computing*, 6(1):7, dec 2017.

[135] Liangming Wang and Fagui Liu. A trusted measurement model based on dynamic policy and privacy protection in IaaS security domain. *Eurasip Journal on Information Security*, 2018(1):1–8, dec 2018.

[136] Adel Abusitta, Martine Bellaiche, and Michel Dagenais. An SVM-based framework for detecting DoS attacks in virtualized clouds under changing environment. *Journal of Cloud Computing*, 7(1):9, dec 2018.

[137] Leandro V. Silva, Pedro Barbosa, Rodolfo Marinho, and Andrey Brito. Security and privacy aware data aggregation on cloud computing. *Journal of Internet Services and Applications*, 9(1):6, dec 2018.

[138] Faraz Fatemi Moghaddam, Philipp Wieder, Süleyman Berk Çemberci, and Ramin Yahyapour. Cloud security distributary set (CSDS): A policy-based framework to define multi-level security structure in clouds. *ACM International Conference Proceeding Series*, Part F1481:74–79, 2019.

[139] Chenglu Jin, Vasudev Gohil, Ramesh Karri, and Jeyavijayan Rajendran. Security of Cloud FPGAs: A Survey. 0(0), 2020.

[140] Talal Halabi and Martine Bellaiche. A broker-based framework for standardization and management of Cloud Security-SLAs. *Computers and Security*, 75:59–71, 2018.

[141] Gregory Levitin, Liudong Xing, and Yuanshun Dai. Co-residence based data vulnerability vs. security in cloud computing system with random server assignment. *European Journal of Operational Research*, 267(2):676–686, 2018.

[142] Flora Amato, Francesco Moscato, Vincenzo Moscato, and Francesco Colace. Improving security in cloud by formal modeling of IaaS resources. *Future Generation Computer Systems*, 87:754–764, 2018.

[143] Agnieszka Jakóbik, Francesco Palmieri, and Joanna Kołodziej. Stackelberg games for modeling defense scenarios against cloud security threats. *Journal of Network and Computer Applications*, 110:99–107, 2018.

[144] Daniel Grzonka, Agnieszka Jakóbik, Joanna Kołodziej, and Sabri Pllana. Using a multi-agent system and artificial intelligence for monitoring and improving the cloud performance and security. *Future Generation Computer Systems*, 86:1106–1117, 2018.

[145] Yepeng Liu, Yongjun Ren, Chunpeng Ge, Jinyue Xia, and Qirun Wang. A CCA-secure multi-conditional proxy broadcast re-encryption scheme for cloud storage system. *Journal of Information Security and Applications*, 47:125–131, 2019.

[146] Antonio Celesti, Maria Fazio, Antonino Galletta, Lorenzo Carnevale, Jiafu Wan, and Massimo Villari. An approach for the secure management of hybrid cloud–edge environments. *Future Generation Computer Systems*, 90:1–19, 2019.

[147] Salah Al-Sharhan, Esraa Omran, and Kamran Lari. An integrated holistic model for an eHealth system: A national implementation approach and a new cloud-based security model. *International Journal of Information Management*, 47(July 2017):121–130, 2019.

[148] Rajendra Patil, Harsha Dudeja, and Chirag Modi. Designing an efficient security framework for detecting intrusions in virtual network of cloud computing. *Computers and Security*, 85:402–422, 2019.

[149] Valentina Casola, Alessandra De Benedictis, Massimiliano Rak, and Umberto Villano. A novel Security-by-Design methodology: Modeling and assessing security by SLAs with a quantitative approach. *Journal of Systems and Software*, 163(May):0–56, 2020.

[150] Chao Lei, Hongjun Dai, Zhilou Yu, and Rui Li. A service recommendation algorithm with the transfer learning based matrix factorization to improve cloud security. *Information Sciences*, 513(xxxx):98–111, 2020.

[151] Chandrasegar Thirumalai, Senthilkumar Mohan, and Gautam Srivastava. An efficient public key secure scheme for cloud and IoT security.

Computer Communications, 150:634–643, 2020.

[152] Omar Ali, Anup Shrestha, Akemi Chatfield, and Peter Murray. Assessing information security risks in the cloud: A case study of Australian local government authorities. *Government Information Quarterly*, 37(1):101419, 2020.

[153] Kashish A. Shakil, Farhana J. Zareen, Mansaf Alam, and Suraiya Jabin. BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud. *Journal of King Saud University - Computer and Information Sciences*, 32(1):57–64, 2020.

[154] Peng Cheng Wei, Dahu Wang, Yu Zhao, Sumarga Kumar Sah Tyagi, and Neeraj Kumar. Blockchain data-based cloud data integrity protection mechanism. *Future Generation Computer Systems*, 102:902–911, 2020.

[155] Siyakha N. Mthunzi, Elhadj Benkhelifa, Tomasz Bosakowski, Chirine Ghedira Guegan, and Mahmoud Barhamgi. Cloud computing security taxonomy: From an atomistic to a holistic view. *Future Generation Computer Systems*, 107:620–644, 2020.

[156] Preeti Mishra, Ishita Verma, and Saurabh Gupta. KVMInspector: KVM Based introspection approach to detect malware in cloud environment. *Journal of Information Security and Applications*, 51:102460, 2020.

[157] Mohammad Wazid, Ashok Kumar Das, Vivekananda Bhat K, and Athanasios V. Vasilakos. LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment. *Journal of Network and Computer Applications*, 150:102496, 2020.

[158] Pan Jun Sun. Security and privacy protection in cloud computing: Discussions and challenges. *Journal of Network and Computer Applications*, 160:102642, 2020.

[159] Suyel Namasudra, Debashree Devi, Seifedine Kadry, Revathi Sundarasekar, and A. Shanthini. Towards DNA based data security in the cloud computing environment. *Computer Communications*, 151(December 2019):539–547, 2020.

[160] Parminder Singh, Avinash Kaur, Pooja Gupta, Sukhpal Singh Gill, and Kiran Jyoti. RHAS: robust hybrid auto-scaling for web applications in cloud computing. *Cluster Computing*, 24(2):717–737, 2021.

[161] Chenlin Huang, Wei Chen, Lu Yuan, Yan Ding, Songlei Jian, Yusong Tan, Hua Chen, and Dan Chen. Toward security as a service: A trusted cloud service architecture with policy customization. *Journal of Parallel and Distributed Computing*, 149:76–88, 2021.

[162] Tian Wang, Yang Li, Weiwei Fang, Wenzheng Xu, Junbin Liang, Yewang Chen, and Xuxun Liu. A Comprehensive Trustworthy Data Collection Approach in Sensor-Cloud System. *IEEE Transactions on Big Data*, 7790(c):1–1, 2018.

[163] Sangwon Hyun, Jinyong Kim, Hyoungshick Kim, Jaehoon Jeong, Susan Hares, Linda Dunbar, and Adrian Farrel. Interface to Network Security Functions for Cloud-Based Security Services. *IEEE Communications Magazine*, 56(1):171–178, 2018.

[164] Aobing Sun, Guohong Gao, Tongkai Ji, and Xuping Tu. One Quantifiable Security Evaluation Model for Cloud Computing Platform. *Proceedings - 2018 6th International Conference on Advanced Cloud and Big Data, CBD 2018*, pages 197–201, 2018.

[165] Ahmed A.Abd El-Latif, Bassem Abd-El-Atty, M. Shamim Hossain, Samir Elmougy, and Ahmed Ghoneim. Secure quantum steganography protocol for fog cloud internet of things. *IEEE Access*, 6(c):10332–10340, 2018.

[166] Yoshita Sharma, Himanshu Gupta, and Sunil Kumar Khatri. A Security Model for the Enhancement of Data Privacy in Cloud Computing. *Proceedings - 2019 Amity International Conference on Artificial Intelligence, AICAI 2019*, pages 898–902, 2019.

[167] Xiang Li, Qixu Wang, Xiao Lan, Xingshu Chen, Ning Zhang, and Dajiang Chen. Enhancing cloud-based IoT security through trustworthy cloud service: An integration of security and reputation approach. *IEEE Access*, 7(c):9368–9383, 2019.

[168] Carl Hauser, Eugene Litvinov, Xiaochuan Luo, Qiang Zhang, Dave Anderson, Theo Gkountouvas, Ming Meng, Ken Birman, and Anjan Bose. Gridcloud: Infrastructure for cloud-based wide area monitoring of bulk electric power grids. *IEEE Transactions on Smart Grid*, 10(2):2170–2179, 2019.

[169] Chang Choi and Junho Choi. Ontology-Based Security Context Reasoning for Power IoT-Cloud Security Service. *IEEE Access*, 7:110510–110517, 2019.

[170] B. Thirumaleshwari Devi, S. Shitharth, and M. A. Jabbar. An Appraisal over Intrusion Detection Systems in Cloud Computing Security Attacks. *2nd International Conference on Innovative Mechanisms for Industry Applications, ICIMIA 2020 - Conference Proceedings*, (Icimia):722–727, 2020.

[171] Caixia Yang, Liang Tan, Na Shi, Bolei Xu, Yang Cao, and Keping Yu. AuthPrivacyChain: A Blockchain-Based Access Control Framework with Privacy Protection in Cloud. *IEEE Access*, 8:70604–70615, 2020.

[172] Vaggelis Atlidakis, Patrice Godefroid, and Marina Polishchuk. Checking Security Properties of Cloud Service REST APIs. *Proceedings - 2020 IEEE 13th International Conference on Software Testing, Verification and Validation, ICST 2020*, pages 387–397, 2020.

[173] Kennedy A. Torkura, Muhammad I.H. Sukmana, Feng Cheng, and Christoph Meinel. CloudStrike: Chaos Engineering for Security and Resiliency in Cloud Infrastructure. *IEEE Access*, 8:123044–123060, 2020.

[174] Adesh Kumari, Vinod Kumar, M. Yahya Abbasi, Saru Kumari, Pradeep Chaudhary, and Chien Ming Chen. CSEF: Cloud-Based Secure and Efficient Framework for Smart Medical System Using ECC. *IEEE Access*, 8:107838–107852, 2020.

[175] Pengtao Liu. Public-key encryption secure against related randomness attacks for improved end-to-end security of cloud/Edge computing. *IEEE Access*, 8:16750–16759, 2020.

[176] Talal Halabi and Martine Bellaiche. Towards Security-Based Formation of Cloud Federations: A Game Theoretical Approach. *IEEE Transactions on Cloud Computing*, 8(3):928–942, 2020.

[177] Hai Jin, Zhi Li, Deqing Zou, and Bin Yuan. DSEOM: A Framework for Dynamic Security Evaluation and Optimization of MTD in Container-Based Cloud. *IEEE Transactions on Dependable and Secure Computing*, 18(3):1125–1136, 2021.

[178] Xinrui Ge, Jia Yu, Hanlin Zhang, Chengyu Hu, Zengpeng Li, Zhan Qin, and Rong Hao. Towards Achieving Keyword Search over Dynamic Encrypted Cloud Data with Symmetric-Key Based Verification. *IEEE Transactions on Dependable and Secure Computing*, 18(1):490–504, 2021.

[179] Prachi Deshpande, S. C. Sharma, S. K. Peddoju, and S. Junaid. HIDS: A host based intrusion detection system for cloud computing environment. *International Journal of Systems Assurance Engineering and Management*, 9(3):567–576, 2018.

[180] Pradip Kumar Sharma, Jung Hyun Ryu, Kyung Yeob Park, Jin Ho Park, and Jong Hyuk Park. Li-Fi based on security cloud framework for future IT environment, 2018.

[181] Vishruti Kakkad, Meshwa Patel, and Manan Shah. Biometric authentication and image encryption for image security in cloud framework. *Multiscale and Multidisciplinary Modeling, Experiments and Design*, 2(4):233–248, 2019.

[182] Vaishali Singh and S. K. Pandey. *Cloud Security Ontology (CSO)*. Springer International Publishing, 2019.

[183] Sheng Cao, Gexiang Zhang, Pengfei Liu, Xiaosong Zhang, and Ferrante Neri. Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. *Information Sciences*, 485:427–440, 2019.

[184] Kriti Bhushan and B. B. Gupta. Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment. *Journal of Ambient Intelligence and Humanized Computing*, 10(5):1985–1997, 2019.

[185] V. Vijayakumar, M. K. Priyan, G. Ushadevi, R. Varatharajan, Gunasekaran Manogaran, and Prathamesh Vijay Tarare. E-Health Cloud Security Using Timing Enabled Proxy Re-Encryption. *Mobile Networks and Applications*, 24(3):1034–1045, 2019.

[186] K. R. Sajay, Suvanam Sasidhar Babu, and Yellepeddi Vijayalakshmi. Enhancing the security of cloud data using hybrid encryption algorithm. *Journal of Ambient Intelligence and Humanized Computing*, (2018), 2019.

[187] Jinan Shen, Xuejian Deng, and Zhenwu Xu. Multi-security-level cloud storage system based on improved proxy re-encryption. *Eurasip Journal on Wireless Communications and Networking*, 2019(1), 2019.

[188] D. Praveena and P. Rangarajan. A machine learning application for reducing the security risks in hybrid cloud networks. *Multimedia Tools and Applications*, 79(7-8):5161–5173, 2020.

[189] Haralambos Mouratidis, Shaun Shei, and Aidan Delaney. A security requirements modelling language for cloud computing environments. *Software and Systems Modeling*, 19(2):271–295, 2020.

[190] Hooman Alavizadeh, Hootan Alavizadeh, Dong Seong Kim, Julian Jang-Jaccard, and Masood Niazi Torshiz. *An Automated Security Analysis Framework and Implementation for MTD Techniques on Cloud*, volume 11975 LNCS. Springer International Publishing, 2020.

[191] Teena Joseph, S. A. Kalaiselvan, S. U. Aswathy, R. Radhakrishnan, and A. R. Shamna. A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment. *Journal of Ambient Intelligence and Humanized Computing*, 12(6):6141–6149, 2021.

[192] Muhammad Tahir, Muhammad Sardaraz, Zahid Mehmood, and Shakoor Muhammad. CryptoGA: a cryptosystem based on genetic algorithm for cloud data security. *Cluster Computing*, 24(2):739–752, 2021.

[193] Venkata Koti Reddy Gangireddy, Srihari Kan-

nan, and Karthik Subburathinam. Implementation of enhanced blowfish algorithm in cloud environment. *Journal of Ambient Intelligence and Humanized Computing*, 12(3):3999–4005, 2021.

[194] V. Vijayakumar and K. Umadevi. Protecting user profile based on attribute-based encryption using multilevel access security by restricting unauthorization in the cloud environment, 2021.

[195] N. Indira, S. Rukmani Devi, and A. V. Kalpana. R2R-CSES: proactive security data process using random round crypto security encryption standard in cloud environment, 2021.

[196] Omar Achbarou, My Ahmed El Kiram, Outmane Bourkoukou, and Salim Elbouanani. A New Distributed Intrusion Detection System Based on Multi-Agent System for Cloud Environment. *International Journal of Communication Networks and Information Security (IJCNIS)*, 10(3):2018, 2018.

[197] Ngoc T. Le and Doan B. Hoang. A Threat Computation Model using a Markov Chain and Common Vulnerability Scoring System and its Application to Cloud Security. *Journal of Telecommunications and the Digital Economy*, 7(1):37–56, 2019.

[198] Suyel Namasudra. An improved attribute-based encryption technique towards the data security in cloud computing, 2019.

[199] K. Venkatraman and K. Geetha. Dynamic virtual cluster cloud security using hybrid steganographic image authentication algorithm. *Automatika*, 60(3):314–321, 2019.

[200] Osama Hosam and Muhammad Hammad Ahmad. Hybrid design for cloud data security using combination of AES, ECC and LSB steganography. *International Journal of Computational Science and Engineering*, 19(2):153–161, 2019.

[201] Erkuden Rios, Eider Iturbe, Xabier Larrucea, Massimiliano Rak, Wissam Mallouli, Jacek Dominiak, Victor Muntés, Peter Matthews, and Luis Gonzalez. Service level agreement-based GDPR compliance and security assurance in (multi)Cloud-based systems. *IET Software*, 13(3):213–222, 2019.

[202] Y. Kiran Kumar and R. Mahammad Shafi. An efficient and secure data storage in cloud computing using modified RSA public key cryptosystem. *International Journal of Electrical and Computer Engineering*, 10(1):530–537, 2020.

[203] Alabi Orobosade, Thompson Aderonke, Alese Boniface, and Arome J. Cloud Application Security using Hybrid Encryption. *Communications on Applied Electronics*, 7(33):25–31, 2020.

[204] S. Immaculate Shyla and S. S. Sujatha. Cloud Security: LKM and Optimal Fuzzy System for Intrusion Detection in Cloud Environment. *Journal of Intelligent Systems*, 29(1):1626–1642, 2020.

[205] Urszula Ogiela. Cognitive cryptography for data security in cloud computing. *Concurrency and Computation: Practice and Experience*, 32(18):1–4, 2020.

[206] Bijeta Seth, Surjeet Dalal, Vivek Jaglan, Dac Nhuong Le, Senthilkumar Mohan, and Gautam Srivastava. Integrating encryption techniques for secure data storage in the cloud. *Transactions on Emerging Telecommunications Technologies*, (January):1–24, 2020.

[207] Muhammad Imran Tariq, Shakeel Ahmed, Nisar Ahmed Memon, Shahzadi Tayyaba, Muhammad Waseem Ashraf, Mohsin Nazir, Akhtar Hussain, Valentina Emilia Balas, and Marius M. Balas. Prioritization of information security controls through fuzzy AHP for cloud computing networks and wireless sensor networks. *Sensors (Switzerland)*, 20(5):1–36, 2020.

[208] Shumaila Shahzadi, Bushra Khaliq, Muhammad Rizwan, and Fahad Ahmad. Security of Cloud Computing Using Adaptive Neural Fuzzy Inference System. *Security and Communication Networks*, 2020, 2020.

[209] Opeoluwa Ore Akinsanya, Maria Papadaki, and Lingfen Sun. Towards a maturity model for health-care cloud security (M2HCS). *Information and Computer Security*, 28(3):321–345, 2020.

[210] Guangxue Zhang, Tian Wang, Guojun Wang, Anfeng Liu, and Weijia Jia. Detection of hidden data attacks combined fog computing and trust evaluation method in sensor-cloud system. *Concurrency Computation*, 33(7):1, 2021.

[211] New nation-state cyberattacks - Microsoft On the Issues.

[212] The Facts on News Reports About Facebook Data — Meta.

[213] Colonial Pipeline Cyber Attack: Hackers Used Compromised Password - Bloomberg.

[214] 4 real-life examples of SaaS data loss... — Spanning.

[215] Gnolia - Wikipedia.

[216] Bupa fined £175,000 after employee stole 500,000 customer records and tried to sell them online.

[217] Trade Secret Theft — FBI.

[218] San Jose Man Sentenced To Two Years Imprisonment For Damaging Cisco's Network — USAO-NDCA — Department of Justice.

[219] A 1.3-Tbs DDoS Hit GitHub, the Largest Yet Recorded — WIRED.

[220] How we're tackling evolving online threats.
[221] Slickwraps apologizes to customers after comically bad data breach - The Verge.
[222] Estée Lauder Exposes 440M Records, with Email Addresses, Network Info — Threatpost.
[223] Have I Been Pwned warns of DatPiff data breach impacting millions.
[224] OG department store customers' personal details leaked in data breach, Singapore News - AsiaOne.
[225] Why a Data Breach at a Genealogy Site Has Privacy Experts Worried - The New York Times.
[226] Security Experts Weigh In On Massive Data Breach Of 150 Million MyFitnessPal Accounts.
[227] Marriott International Notifies Guests of Property System Incident — Marriott News Center.
[228] The Disney+ Credential Stuffing Attack Could Happen to You.
[229] 500K Zoom Accounts Discovered for Sale on the Dark Web.
[230] Capital One data breach: A hacker gained access to 100 million credit card applications and accounts - CNN.
[231] Online marketing company exposes 38+ million US citizen records.
[232] Virtual machines hide ransomware until the encryption process is done - Help Net Security.
[233] Australian sports fan portal leaks 132GB of private data.
[234] Russia's Hacking Success Shows How Vulnerable the Cloud Is to Cyberattacks.
[235] Hackers Raided Panasonic Server for Months, Stealing Personal Data of Job Seekers.
[236] How the US government hack happened, explained by an expert - Vox.
[237] Target's Data Breach: The Commercialization of APT — SecurityWeek.Com.
[238] Russian Nuke Scientists, Ukrainian Professor Arrested for Bitcoin Mining.
[239] Abusing cloud services to fly under the radar – NCC Group Research.
[240] Inside a massive cyber hack that risks compromising leaders across the globe - ABC News (Australian Broadcasting Corporation).
[241] Brazil: Millions of Records Leaked, Including Biometric Data.
[242] Lifelabs Data Breach, the Largest Ever in Canada, May Cost the Company Over $1 Billion in Class-Action Lawsuit - CPO Magazine.
[243] Microsoft Security Shocker As 250 Million Customer Records Exposed Online.
[244] NHS data breach exposes 24 staff data in Scotland — News — GRC World Forums.
[245] Secret NHS files reveal plans for coronavirus contact tracing app — WIRED UK.
[246] Hackers publish ExecuPharm internal data after ransomware attack — TechCrunch.
[247] IT giant Cognizant confirms data breach after ransomware attack.
[248] Memorial Health System alerts patients to possible data breach — News, Sports, Jobs - News and Sentinel.
[249] The CPU catastrophe will hit hardest in the cloud - The Verge.
[250] KrebsOnSecurity Hit With Record DDoS – Krebs on Security.
[251] DDoS attack on Dyn - Wikipedia.

Suryateja S. Pericherla is an Associate Professor working in the Department of CSE at Vishnu Institute of Technology, India. He has more than 10 years of teaching experience and is an individual researcher whose research interests are Cloud Computing, the Internet of Things, Computer Security, Network Security, and Blockchain. He is a member of professional societies like IEEE, ACM, CSI and ISCA. He published several research papers which are indexed by SCIE, WoS, Scopus, Springer and others.