Security Issues, Threats And Respective Mitigation In Cloud Computing – A Systematic Review

Mubashir Ali, Shaista Malik, Zainab Khalid, Maham Mehr Awan, Shahbaz Ahmad

Abstract: Cloud computing is one of those emerging technologies that has occupied vital importance in today's age. The proficiency of lessening expenses of computing, growing scalability and flexibility for storage related computer processes has made it to attain prime place in emerging trends. In cloud computing, entire data exist over a set of interconnected resources and is accessed through virtual machines over the network. It provides promising platform that allows efficient usage of numerous applications such as storage resources and computing infrastructure. In spite of all these benefits, there are various challenges to secure the cloud environment from vulnerabilities. Therefore, this state of the art study is conducted to highlight security related issues that arise at different levels of computations using cloud services. Moreover, taxonomy has been formulated by categorizing identified challenges in security issues and security attacks respectively. To identify the security challenges; A Systematic Literature Review (SLR) has also been conducted from the existing literature. Results show that major security issues are related to the client side, network side and at the backend. Furthermore, this study shed some light on the security issues that are encountered in cloud computing at different levels by designing architecture and offering cloud users the elucidations for safeguarding cloud data.

Index Terms: Cloud Computing, Security Issues, Threats, Challenges, Vulnerabilities, Solutions

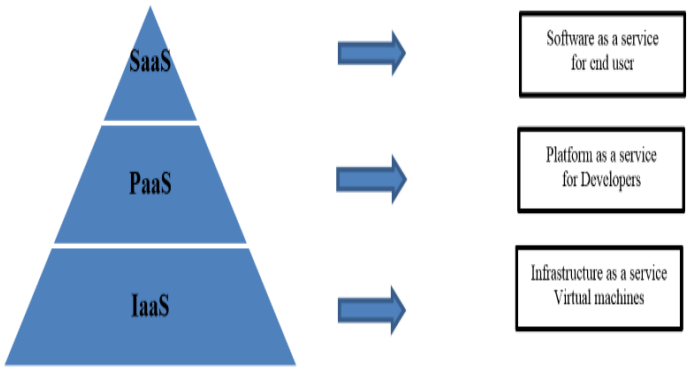
1 INTRODUCTION

Cloud based computing is one of the fundamental motives for the use of technologies of current era that based on Internet. National Institute of Standards and Technology (NIST) [1] describes that cloud computing provides on demand, convenient, ubiquitous and reliable network access to large configured shareable computing resources that can easily managed and utilized with interaction of cloud service provider and minimal effort [2]. It is state-of-the-art information system procedure that offers dynamically shared resources over the Internet and provide economic benefits [3].

Cloud computing takes motivation from "Pay As You Go (PYAG) model, the place where you pay for the services you have utilized [4]. A standout amongst these real profits of PAYG model is that we could minimize our use by providing certain assets as needed. Client might select operating system, memory, processor, networking and access control as per their need. Assets are provided on request of the client or end-user [5]. Cloud provides great assistance to individual users as well as industry and draws the attention of the researchers [6]. Services of the cloud denoted by the XaaS and X=[S, P, I] and its usage of task execution by using internet. To increase the service availability and reduce time of execution Cloud enables the resource sharing facility [7]. Cloud computing overcomes the concerns related to the lack of resources by providing various services according to the need of clients [8] at diverse level such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) as shown in figure 1. Cloud delivers different applications without installing these on the client's personal computer. It provides the developer and application designer the facility of designing applications without buying the actual server. Moreover, it offers virtual instances of the actual hardware resources. All these services of cloud come up with the potential to lessen cost and computational power [10] but are vulnerable to security threat. Data breach is one of the crucial issues in which cooperated server could significantly harm the tenant along with cloud service providers. A variety of data might be stolen such as personal data (social security numbers, personal messages, credit card information and addresses) as well as business data. In current scenario the consumer of cloud that can be the service or data owner completely rely on provider of service for security and privacy of information [11].

- *Mubashir Ali is currently associated as a Lecturer with Department of Software Engineering, Lahore Garrison University, Pakistan. His work has appeared in many leading journals and international conferences. His research interests include Internet of Things, Wireless Sensor Networks, Cloud Computing, Data Analytics and Machine Learning.*
  E-mail: dr.mubashirali1@gmail.com, mubashirali@lgu.edu.pk
- *Shaista Malik received her MSCS degree from Bahauddin Zakariya University Multan, Pakistan. Currently, he is affiliated with Department of Computer Science, Women University Multan, Pakistan. Her research interest includes Cloud Computing, Networks and Information Security*
  E-mail: shaistamalik04@gmail.com
- *Zainab Khalid received her MSCS degree from Lahore College for Women University, Pakistan. Currently, she is affiliated with Department of Software Engineering, Lahore Garrison University, Pakistan. Her research areas are Software Engineering and Cloud Computing.*
  E-mail: zainabkhalid@lgu.edu.pk
- *Maham Mehr Awan received her MSSE degree from National University of Science and Technology (NUST) Islamabad, Pakistan. Currently She is affiliated with Department of Software Engineering, Lahore Garrison University, Pakistan. Her research interest includes Risk and Quality Management.*
  E-mail: mahammehr@lgu.edu.pk
- *Shahbaz Ahmad completed his MCS from Islamia University Bahawalpur in 2013 and MSCS from National College of Business Administration & Economics, Sub Campus Bahawalpur in 2018. Currently, he is working as a researcher. His research interest includes Information Security, Network Security, Internet of things and Cloud Computing.*
  E-mail: shahbaz4426@gmail.com

Figure 1: *Cloud Services [9]*



Issues like data breach occur due to the fact that the users lose control of their data, because it is stored over cloud server [12]. Among many problems of the cloud computing are identity management of cloud user has many problems, some of them are management of cloud user, multi-tendency support and application security [13]. The main motive is to highlight these security issues that threaten the growth of cloud computing. Therefore, this study intends to propose a taxonomy of the security issues encountered by cloud environment. This taxonomy follows identification of various security issues at different levels and their possible mitigation techniques to secure the cloud applications.

2 BACKGROUND

Cloud computing gained very popularity in current computing era. It became a social marvel ordinarily used by most of the people, which enhances the capabilities or capacity dynamically without wasting resources on training new personnel, infrastructure or licensing new software. Cloud technology has not only extended attention of the IT industry but also revolutionized the computing world as well. Rapid deployment, minimal investment and cost reduction are core factors that motivate businessmen to make use of Cloud services. So they have to concentrate on core business concerns instead of dealing with technical issues. Cost reduction is one of the major reasons for 90% organization to migrate on cloud in US and Europe [14]. Cloud technology provides professional management of network, security and economy of scale [15]. In spite of all these benefits, security is the major concern that leads to reduction in evolution of cloud computing [16]. Cloud computing transfers the valuable data, applications and their respective databases to the enormous data centres where the data management and services are doubtful. However, this innovative aspect poses various security challenges [17]. Analysts predict that in the succeeding five years, cloud computing global market will raise to $95 billion and also 12% of the global software and systems industry will shift over the cloud. By highlighting this incredible potential, IT industry or researcher must invent new techniques to ensure the privacy demands raised up by new computing innovations [18]. In recent survey of IDCI, security is pointed out as one of the major obstacle that stops 74% of IT system executives and CIO's to cloud services model adoption [19], [20]. Furthermore, Subashini and Kavitha [4] has stemmed the security issue in cloud computing systems and has provided some solutions regarding these issues. This study aims to develop an understanding about various security threats that obstruct the privacy and security of tenants. This study contributes in a way to identify various security issues and attacks reported in the existing literature. Moreover, a taxonomy has been formulated to classify different security challenges into respective dimensions. Furthermore, none of study has adopted SLR to collect the security issues before. Following research questions are designed to achieve the objectives of this research,

2.1 Research Questions

RQ1. What are the major security challenges encountered by Cloud Computing?
RQ2. What are the security hurdles encountered by cloud computing adoption?
RQ3. Which security threat mitigation techniques available to ensure the acceptable security of Cloud Computing services?
The purpose of RQ1 is to identify the security issues that arise in cloud computing when the user makes use of cloud services and of RQ2 is to identify the security attacks. The RQ3 present up to date mitigation techniques that are implemented in Cloud Computing environment to ensure the reliable and secure services. When the data is in transit state the main security risk associated with technology used to transfer the data among the networks.

3 METHODOLOGY

The identification of cloud computing security issues, threats and respective mitigation techniques in broad view of cloud services is very challenging task [21]. In this research work, Systematic Literature Review (SLR) has been conducted in order to gather the current knowledge and qualitative research method has been used in order to develop a complete understanding about cloud computing phenomenon, its pioneers, issues and attacks involved in cloud computing adoption.

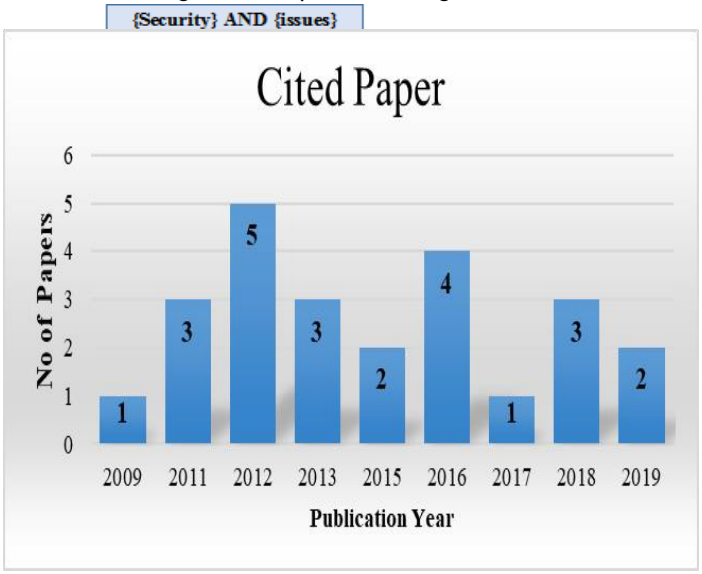
3.1 Systematic Literature Review

[22] has suggested that researchers in software engineering should implement EBSE ‘‘Evidence-based Software Engineering”. EBSE aims for evidence based technique for research practices in Software Engineering. In this perspective, evidence has been outlined as a synthesis of paramount quality scientific studies about research question or particular topic. The key scheme of synthesis is a SLR. This research has been taken as a Systematic Literature Review on the basis of novel procedures as prescribed by [23].

The major reasons that distinguish a SLR from traditional review are:

1. It states search approach which targets to identify relevant literature up to as much large extent as possible.
2. SLR reports the identified research questions by describing a review procedure.
3. SLR requires inclusive and exclusive criteria to evaluate the prime study respectively.

Figure 2: Steps for filtering studies



3.2 Search String

By following systematic research approach, required information has systematically been found in SLR using the databases Science Direct, IEEE Xplore, Springer Link and ACM as shown in Table1. Major keywords which are used to create search string includes:

- Security techniques
- Cloud computing
- Security attacks
- Cloud Security issues and challenges

Erected search string used to discover the requisite information through the SLR is

{Security} AND {issues} OR {(Challenges) OR (Attacks) OR (prevention techniques) OR (method)} of {cloud based computing}.

Source	Acronym
IEEE Software	IEEE SW
ACM	TOSEM
SpringerLink	SL
ScienceDirect	Elsevier

Table 1: *Targeted Databases*

3.3 Selection Criteria

To find out the main studies, selection criteria provides evidence related questions of research [24]. Selection of criteria for research contains exclusion and inclusion criteria for filtering and selection of research. At initial step the selection criterion conducts search on the basis of abstract and title. The selection of study process is then tracked by filtering the obtained collection of papers according to defined criteria of exclusion and inclusion that mirrors the information related to the security issues and attacks for cloud. Whole search strategy is shown in Table 2.

Electronic Databases:	Science Direct IEEE Xplore Springer Link ACM Digital Library Web of Knowledge Emerald
Publication Types	Journal Publications Conference papers Book Chapters
Publication Period:	Since 2009 to 2019
Inclusion Criteria	I1: Criteria which cover security issues when data is at transit and when data is at rest state in Cloud. I2: Studies which match with abstract are included. I3: Studies published between the years 2009 to Jan 2019 are included. I4: Criteria that enact the attacks prevention methods which are presently being deployed in Cloud environment. I5: Security challenges and anticipations in Cloud Computing.
Exclusion Criteria	E1: Studies including repetitive security issues and attacks in Cloud Computing. E2: Studies that have been conducted before 2009 are excluded. E3: Studies with mismatched abstract are excluded. E4: Studies in languages other than English.

Table 2: *Search Strategy*

3.4 Search Process

Secondary data sources have been used for this research. Secondary data source means published informatory articles, research papers, survey papers mainly in scientific and technical journals. These articles / papers are published between 2009 and 2019 as shown in Fig. 2. Both institutional and public databases are explored to search interrelated papers. Online databases have taken as start point and then moved to IEEE, Springer, ACM and Science Direct services. In the end search has been implemented on general Google search engine to complete the search procedure. The keyword “Cloud Computing” is utilized because involved target is understanding cloud computing only. This study is exclusively concerned with papers that are about cloud computing by businesses acceptance. Significant usage of vital factor was done that recollected the accessed papers and concluded with 21 papers in total. Preferred papers are in between the year 2011 and 2019 as shown in Fig. 3. Most of the papers were retrieved from professional journals and only few from academic databases. Majority of selected papers comprised of security issues, attacks and personal sentiments of professionals belonging to providers and clients. Most of papers trying to providing visions and state the portent on how cloud computing to be adopted and what precautionary techniques to take on, and circumstances of cloud adoption and attack prevention. Be capable to view phenomenon from diverse approaches is a chief factor in conducting a qualitative research that aimed to development of theory [25]. Selected studies those are strongly related with the topic are illustrated in Table.

Figure 3: *Number of selected papers with their publication year*

Serial #	Reference	Type
1	[7]	J
2	[11]	J
3	[26]	J
4	[15]	J
5	[13]	C
6	[27]	C
7	[28]	B
8	[29]	J
9	[30]	J
10	[31]	J
11	[32]	J
12	[33]	J
13	[34]	J
14	[35]	J
15	[14]	J
16	[36]	J
17	[37]	C
18	[16]	J
19	[38]	J
20	[19]	J
21	[4]	C
22	[39]	J

Table 3: *Selected Studies*

4 PROPOSED TAXONOMY OF CLOUD COMPUTING

A taxonomy of the cloud security has been proposed following SLR. It comprises of two major categories which include security issues and security attacks as mentioned in Fig. 4. Security issues have been further divided into ten different aspects. These aspects include embedded security issues, application security issues, web application issues, trust issue [40] and so on. Furthermore, security attacks have been identified which occur in cloud computing due to these security issues. Different prevention techniques have been explored in order to secure the services of cloud. These attacks have four major directions i.e. basic level, virtual machine, application level and network level attacks [38]. These are further categorized into subcategories for more understanding. Below mentioned factors are the challenges identified for cloud computing environment. Cloud computing in the market truly depends on the assurance of minimum security problems to customers.

4.1 SECURITY ISSUES

In present days one of the key concern is Security in environment of cloud computing. Identified security issues and attacks require elaboration and deep discussion.

A. Embedded Security Issues

The embedded systems based on recent technology which is not fully explored yet. The innovations of embedded systems are due to the up gradation of working tools with these systems. These have to face several challenges caused by their distinctive features. Virtualization is the main reason that caused the embedded security issues [38]. These include VM isolation, Programmability, VM Monitoring, Electronic access control and SNMP (simple network management protocol) Server.

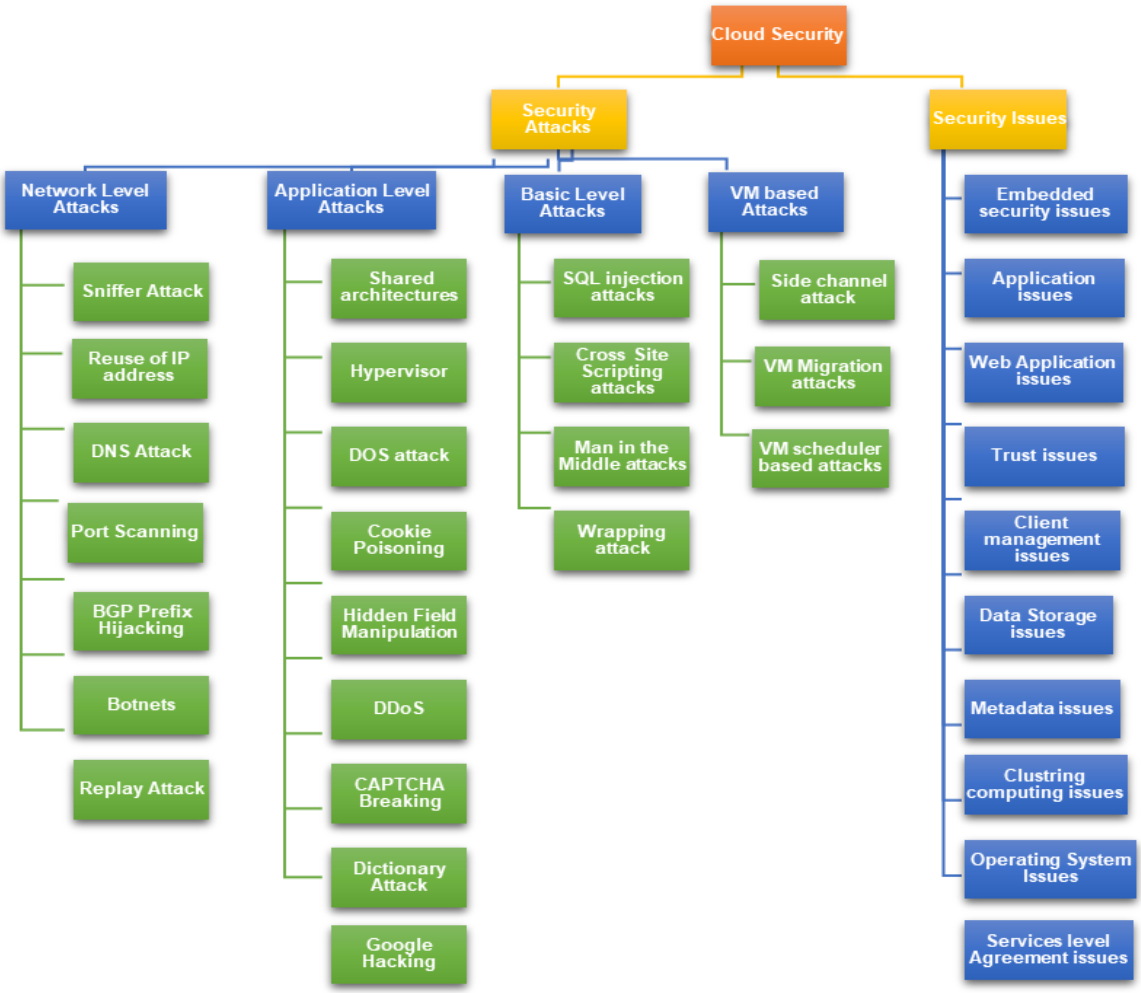
B. Application Issues

The security of application software is one of the most susceptible zone in cloud. Most applications have different types of platforms and frameworks like parallel applications, front end and backend applications. Also a software application may have millions of lines of programming code [41]. Beside these, software can be written in different languages and by different programmers. These factors lead to variety of vulnerabilities. Different application issues are regarding platform selection, user front end design, user back end, license, framework, service availability, and parallel nature of applications which concern with the security of cloud.

C. Trust Issues

Trust is measured as the experience of the customer or user that contributes for making trust worthy decisions. Furthermore, storage, stakeholders, computational algorithm access and virtualization also relates to trust. Trust evaluation is multiphase that depends upon the multidimensional factors [27]. The most relevant security, trust and privacy issue has been surveyed and analyzed in [42]. TCP concepts presented by next frontier in security transparency, aims to make sure the integrity and confidentiality of data taken by provider of service. Trust issues include human factors, forensic values, Reputation, Governance, Trusted third party (TTP) and Lack of consumer trust. On the basis of cloud service provisioning three key aspects can be can be concluded as the requirements of trust. These are operational performance of the system, Quality of Service and privacy and security of cloud computing. The trust requirements with sub-factors are given in Table 4.

Figure 5: *Taxonomy of Cloud Security*



Operational Performance	Quality of Service	Privacy and Security
Continuity	Availability	Auditability
Scalability	Usability	Controllability
Adaptability	Consistency	Openness and transparency
Flexibility	Reliability	Accountability
Resilience	Quick Response	Auditability

Table 4: *Key Requirements for Trust [40]*

D. Web Application Issues

These are similar to the security issues of internet services that contains various problems like port scanning, IP spoofing, injection flaws of social engineering and may more. According to [35], many technologies influenced by cloud computing like virtualization and web2.0 which inherit the security issues. Also vulnerabilities in this type of system are identified. In SaaS application it creates many faults by which attacker gains control on slave computers to run the malicious activities [43]. These issues are related to web server and technology, Proxy server [39], Protocol and standard.

E. Client Management Issues

Efficient management of clients according to secure utilization of resources is one of the key concern to ensure the privacy of cloud computing. It is similar like to protect the president over road and president in house. Similarly, data over cloud verses data in client private system [26]. Client management issues includes client experience, privacy, authentication, and client identity and management issues [44].

F. Metadata Issues

Security professional knows that metadata contains sensitive and confidential information. Inadvertent leakage of sensitive detail available in Metadata causes the various risk for organization. The attacker might extract the security information of metadata about implementation and faulty accounting. The attacker can alter Web Service Description language in metadata spoofing attack [5]. Metadata issues are protection of data location, separation, maintenance and sanitization.

G. Data Storage Issues

In cloud based computing storage of data is most crucial components. Internet devices and different online applications are growing rapidly as the part of distributed computing, data security and its storage become complicated. The security issues regarding cloud storage include location of data warehouses, data leakage and loss, sanitization, unreliable data, anonymity, availability, integrity management, cryptography, metadata location protection and maintenance

[31].

H. Operating System Issues

Cloud computing utilize many types of servers in diverse network, different operating system and multiple VM which arises different challenges for cloud security. A lot of security attacks are being deployed on IOS, BSD, Windows and Linux. OS attacks such as the overflow attack on stack and GNU Bash caused the serious issues due to the remotely code execution. Prominent OS issues include GNU Bash Common Vulnerability and stack buffer overflow issues with high risk and serious threat [6].

I. Distributed Computing Issues

Distributed computing, like Cluster, utilizes many computers, virtual machines, servers that are connected tightly or loosely to work together and viewed as single system. In single cluster by increasing the nodes brings many challenges for the administrator of the system, that give rise to different clustering issues of security in virtual, physical, hierarchal and multi clusters.

J. Service Level Agreement (SLA) Issues

SLA is the process of performance measurement, setting benchmark for service goals and expectations of customers. Some questions that are arising in it are could security be effectively explained in context of SLA. Security issues of management of service level includes incorrect installation of OS and unintentionally turning off the security events auditing by the administrator while critical vendor monitoring [6].

5 SECURITY ATTACKS

Attack in cloud computing is a malicious action which aims to adversely affect the resources of Cloud. Security issues also discussed and studied by many researchers [45] and have given the detailed description on secure cloud infrastructure. The basic security attacks defined in taxonomy are discussed in this section with their available mitigation techniques.

5.1 NETWORK LEVEL ATTACKS

The machines active inside a cloud platform are connected to the outside platform of cloud by network. Over the network the intruder might attack on system that might weaken the services of cloud working and possibly put privacy of data at hazard. Network level attacks are explained below,

A. Sniffer Attack

Data packets passing over the network can be captured by the intruders by using the different applications. The data transmitted in non-encrypted format can be read. There is a risk to capture or trace the vital information flowing through the network. Sniffing detection platform developed on the basis of RTT (round trip time) and ARP (address resolution protocol) that is used to discover a sniffing structure running on the network [46].

B. Reusing IP Addresses Attack

IP address can be reused and reassigned by other users on the network. The address of a user still remains in the cache of DNS even after his use [12]. If this address is used by another user due to re-assignment or hacking, it violates the original user's privacy. In this way other users can access the data of original user. In order to prevent this attack old ARP addresses are cleared from cache.

C. DNS Attack

DNS translates the Domain name address into IP address. There are chances to route the user to some other malicious cloud as an alternative of originally asked. As a result, path becomes rerouted through some malicious connection between sender and receiver. Such selected route may cause security problems. To reduce the effects of DNS attacks Domain Name System Security Extensions (DNSSEC) is used.

D. Scanning of Port

On server side port might be explored for status checking of services that are running on target machine. The network on which the target machine resides is required to be accessed for port scanning. Port scanning is used to expose target machine vulnerabilities that result in the denial-of-service attacks [47]. Firewall and intrusion prevention system (IPS) are used to avoid this attack. Firewall actively detect and control the effected and exposed ports [48]. The IPS detect port and shut these down before these are able to gain a full map of network.

E. BGP Prefix Hijacking

A network type attack in which wrong IP address is assigned to Autonomous system. As a result, malicious insiders acquire entrance to the undetectable IP address. A defective AS broadcasts incorrectly about the related IPs. In this case authenticated traffic routed to unauthenticated IP address. Hence data reaches to some other unintended destination. Distributed anomaly detection system provides analogous security and has a more acceptable adoption path to cryptographic methods. A related security system has been described in [49].

F. Botnets

Botnets are defined as an interconnected malware of affected computer network without knowledge of user as planned by cybercriminals. Botnets are the infected computers (bots) collection of that are remotely controlled by a bot-master (machine that control the bot network) by the Command and Control channel (C&C) [50]. These are usually send spam emails, transmit viruses and engage in other actions of cybercrime. For avoidance of botnet attack, bot-master is identified by filtering packets and tracking the communication [51], [52].

G. Replay Attack

In this attack a legal transmission of data is fraudulently delayed or repeated. The attacker saves and diverts old messages and in future sends this message to one of participants to gain access. The attacker gains access to unauthorized resources by sending messages to old tenant. Session tokens, timestamps, deny concurrent logins and limiting the session time have been used to prevent this attack [30].

Levels of Cloud	Attack	Mitigation Technique
Network Level Attack	Sniffer Attack	Sniffing Detection Platform based on RTT and ARP.
	Reusing IP Addresses	Old ARP Addresses Cleared from Cache

	DNS Attack	Domain Name System Security Extensions
	Scanning of Port	Firewall and Intrusion Prevention System
	BGP Prefix Hijacking	Distributed anomaly detection system
	Botnets	Packet Filtration
	Replay Attack	Session Tokens, Timestamps, Deny Concurrent Logins
Application Level Attack	Shared Architectures	Assessment of Application's Binary Code
	Hypervisor Concerned Attacks	Progressive Cloud Defence System and by Guest Virtual Machine Monitoring
	Denial of service Attack	Intrusion Detection System
	Cookie Poisoning	Applying an Encryption Scheme on Cookies and Performing regular Cookie Clean up
	Manipulation of Hidden Field	Deploying Proper Security Checks
	Distributed Denial of Service Attacks	Intrusion Detection System
	CAPTCHA Breaking	Safe Design of CAPTCHA Framework on the basis of many Moving Objects Recognition with Complicated Background
	Dictionary Attack	OTP and Strong Encryption Techniques
	Google Hacking	Web Vulnerability Scanner
VM based Attack	Side Channel Attack	Strong Cryptographic Algorithms
	VM Migration Attack	Proper Suspension of Actions and Effective Formation of Security Strategies
	VM Scheduler Based Attacks	Improved Varieties of Scheduler
Basic Level Attack	SQL Injection Attack	Proxy Based Framework
	Cross Site Scripting Attack	Blueprint Based Method Reduces the Dependence on Web Browsers by Identifying Networks Untrusted Contents
	Man in the Middle Attack	Cain, Dsniff, Ettercap, Airjack and Wsniff
	Wrapping Attack	Proper Signature Technique and Configuration of SSL

Table 5: *Addressing security attacks of cloud computing*

5.2 APPLICATION LEVEL ATTACKS

The tremendous advantages of cloud computing encourage organizations to move and develop applications to cloud. The advantages include increase of efficiency, reduction of cost etc. But security issues obstruct the success of this adoption. Thus proper security methodology for cloud is necessary to be devised. The applications that are running on the cloud computing vulnerable to several attacks through injecting malicious code to trace path of execution to exploit important information.

A. Shared Architecture

Cloud has shared architecture and multi-tenant environment. Victim's application execution path can be traced when the architecture is shared. The shared environment includes various unique issues includes authorization, access control and authentication. In multitenant environment resource accounting, rapid elasticity and Isolation are major challenges [53]. Its vulnerabilities further can be used to hijack account and discover victim's events. In shared architecture data leakage chance can be detected by the assessment of application's binary code [54].

B. Hypervisor Oriented Attacks

Hypervisor permits distinct hardware host the configuration of multiple virtual machines multiple virtual machines to configure on a distinct hardware host. Malicious code is run by the guest system In this guest system attempts to configure malicious code to take full control and block the services of host system [55]. Progressive cloud defense system can be developed by inter-communication among various components and

monitoring the events of the guest Virtual Machines [56].

C. Denial of Service Attack

Service providing sever is flooded with enormous requests and service becomes unavailable to authorized user. The most popular encounter technique is Intrusion Detection System [57]. Preventive tools are Firewalls and Switches.

D. Cookie Poisoning

Unauthorized person can change or modify the contents of cookies by an unauthorized access to application. Cookies comprise identity related authorizations of user. Once these are accessed, to impersonate an authorized user, their content scan be copied. Applying an encryption scheme on cookies and performing regular cookie clean up can avert this attack [58].

E. Manipulation of Hidden Field

Some fields are hidden in webpages which are used by developer. In HTML forms, hidden fields carry significant information such as user ID and price etc. The attacker can save the index page to change the values of these fields and then post on web page [36]. This attack can be avoided by system by deploying proper security checks.

F. Distributed DOS Attacks

The attack is transmitted from diverse dynamic networks which have previously interacted such as the Denial of service attack. The attacker takes control of stream of information by using some data that was previously exchanged between computers of network. In this way the attacker gets control on the public use information amount and its type [59]. Use of IDS is to defend the cloud from DDOS attacks [60].

G. CAPTCHA Breaking

CAPTCHA was designed for the over-exploitation and spam prevention of the resources of network [61]. CAPTCHA might be breached by spammer, with use of the audio system and by text to speech transformation software to setback the CAPTCHA test. As a result, an unauthenticated user gets access to an account. As a preventive measure safe design of CAPTCHA framework has been presented on the basis of many moving objects recognition with complicated background.

H. Dictionary Attack

All possible word combination used by attacker in dictionary attack, to decrypt the data successfully exchanged within a network. As a result, attacker gains unauthorized access to data flowing in the network. It can be eluded by using an OTP (The One-Time Password) as explained in [62]. Strong encryption algorithms are used in order to prevent these type of attacks.

I. Google Hacking

Google search engine is used by the hackers for the discovery of the sensitive data and use this data for the user account hacking. After gathering the all required information, hacking of the concerned system is performed by the hacker. Software solution used to prevent such as Web Vulnerability (WV) Scanner is used to avoid any sensitive material distribution.

5.3 Virtual Machine Based Attacks

Such attacks cause vulnerabilities in the VM to affect. This interferes services and data protection of cloud. Various VM reason several risks presence hosted on a system. Furthermore, multiple virtual machine managing stages might be used to endorse huge amount attacks of cloud.

A. Side Channel Attacks

The information concerning the cryptographic keys, use of resource and other important information are collected from the target machine that resides onto the identical physical machine on which the VM of attacker resides [63]. Strong cryptographic algorithms and authentications are used to lessen these attacks [64].

B. VM Migration Attacks

VMs along with data can easily be migrated from its original location to another location due to the high mobility and elasticity features of the cloud. In this situation the user always unaware about the location of the data and it is very difficult to copy or to make clone of data [11]. Sensitive data movement in form of metadata causes the sensitive information loss and risk of errors. Proper suspension of actions and effective formation of security strategies might render the migration of VM to become more protected [65].

C. VM Scheduler Based Attacks

Some weaknesses in the scheduler might result in stealing of resource or theft-of-service [66]. VM can be programmed to run afterward exact time however remembering the credit balance of the time slice of VM execution. Improved varieties of scheduler [67] might augment hypervisors security while keeping objectivity and competence. Implementation of firewall, segmenting network logically, encryption of data transmission and monitoring of network can be used to prevent attacks [31].

5.4 Basic Level Attacks

This is the fourth category of attacks in taxonomy. There are three main attacks, as described below, which can threaten the user while entering into cloud.

A. SQL Injection Attack

Into the SQL code the vulnerable code is injected for gaining the unauthorized control to database [68] to dynamically detect and extracts user. Proxy based framework used for the SQL injection attacks prevention [69].

B. Cross Site Scripting Attack

Malicious scripts can be inoculated into code of web pages. User accidentally clicks these affected risky links. As a result, interfering third party acquires control of user's personal information and hack the accounts. A blueprint based method has been proposed that reduces the dependence on web browsers by identifying untrusted contents on networks [20].

C. Man in the Middle Attack

In this attack unauthorized person attempts to intrude on-going discussion among the client and server to inject wrong information. Attacker gains control onto both client and sender data and their communication. This attack could only occur when the attacker can imitate each endpoint of their agreement as predicted from the authentic end. All protocols which include some method of authentication at endpoints are specifically used to prevent these attacks [70]. For instance, authentication sent to either of two parties using a certificate of mutually trusted authority. Various encryption techniques as the Cain, Dsniff, Ettercap, Airjack and Wsniff used for attack prevention [29].

WRAPPING ATTACK

Replicating body of the SOAP (Simple Object Access Protocol) header wrapping attacks are launched where authentication information of tenants is kept. It allows attacker to run malicious code and intrude Cloud services. The use of proper signature technique and configuration of SSL help to prevent this attack.

CONCLUSION

Cloud computing security threats require detailed exploration with respect to their relevance and prospective impact to real world scenarios of cloud. As derived results from SLR, first better opinion for improving security of Cloud Computing comprises by strengthen the security abilities of frameworks of both web services and web browsers. Hence, as part of current work, foundations for the security of Cloud Computing can be harden that rested by the specifications, underlying protocols and tools employed in cloud scenario. IT industry is revolutionized by the publicity of cloud paradigm. It provides numerous benefits for organizations and companies. Still the cloud is vulnerable to security even it provides various advantages. Hence security is a top priority challenge of the cloud adoption. The vendors and customers are aware about security issues and attacks. This research has carried to bring forth to light various issues, attacks and security challenges that hamper cloud computing adoption. Security challenges and issues rise from the unique Cloud characteristics such as security issues such as virtualization, resource pooling and sharing. Various cloud security issues and attacks are analyzed according to provider security concern. In addition, management teams planned for cloud technology for the improvement of performance, security, quality and innovation of provided services to users and tenants. Consequently, the analysis of existing literature schemes also analyzed to counter the issues in efficient and cost saving way. Security issues and attacks are also presented in hierarchal manner. Cloud service system in three levels and the important consideration of security are discussed in three levels. On the basis of above findings, mitigation techniques can be explored. Later it is possible in future to develop a state of the art prevention technique to mitigate majority of security issues and attacks in one go.

ACKNOWLEDGMENT

We would like to thank journal editor, area editor and anonymous reviewers for their valuable comments and suggestions to help and improve our research paper.

CONFLICT OF INTEREST

On behalf of all authors, the corresponding author states that there is no conflict of interest.

REFERENCES

[1] P. Mell and T. Grance, “The NIST definition of cloud computing,” 2011.

[2] D. Nister and H. Stewenius, “Scalable recognition with a vocabulary tree,” in Computer vision and pattern recognition, 2006 IEEE computer society conference on, 2006, vol. 2, pp. 2161–2168.

[3] W. Kim, “Cloud computing architecture,” Int. J. Web Grid Serv., vol. 9, no. 3, pp. 287–303, 2013.

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

[5] C.-Y. Ku and Y.-S. Chiu, “A Novel Infrastructure for Data Sanitization in Cloud Computing (Research Paper),” in Diversity, Technology, and Innovation for Operational Competitiveness: Proceedings of the 2013 International Conference on Technology Innovation and Industrial Management, 2013, p. S3_25-28.

[6] N. Fotiou, A. Machas, G. C. Polyzos, and G. Xylomenos, “Access control as a service for the Cloud,” J. Internet Serv. Appl., vol. 6, no. 1, pp. 1–15, 2015.

[7] S. S. Gill et al., “Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges,” Internet of Things, p. 100118, 2019.

[8] R. Buyya, J. Broberg, and A. M. Goscinski, Cloud computing: Principles and paradigms, vol. 87. John Wiley & Sons, 2010.

[9] D. Villegas et al., “Cloud federation in a layered service model,” J. Comput. Syst. Sci., vol. 78, no. 5, pp. 1330–1344, 2012.

[10] D. Bermbach, “Quality of Cloud Services: Expect the Unexpected,” IEEE Internet Comput., vol. 21, no. 1, pp. 68–72, 2017.

[11] S. Basu et al., “Cloud computing security challenges & solutions-a survey,” in 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), 2018, pp. 347–356.

[12] T. Mather, S. Kumaraswamy, and S. Latif, Cloud security and privacy: an enterprise perspective on risks and compliance. “ O’Reilly Media, Inc.,” 2009.

[13] K. Karthiban and S. Smys, “Privacy preserving approaches in cloud computing,” in 2018 2nd International Conference on Inventive Systems and Control (ICISC), 2018, pp. 462–467.

[14] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, “A survey on security issues and solutions at different layers of Cloud computing,” J. Supercomput., vol. 63, no. 2, pp. 561–592, 2013.

[15] J. Qaddour, “Security Threat and Challenges Analysis of Cloud Computing with Some Solutions.”

[16] H. Tianfield, “Security issues in cloud computing,” in Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on, 2012, pp. 1082–1089.

[17] H. Lo, R. Wang, J. P. Garbani, E. Daley, R. Iqbal, and C. Green, “Forrester report,” State Enterp. Softw., vol. 2009, 2009.

[18] P. BNA, “Privacy & security law report,” 2009.

[19] J. A. Bowen, “Cloud computing: Issues in data privacy/security and commercial considerations,” Comput. INTERNET LAWYER, vol. 28, no. 8, pp. 1–8, 2011.

[20] M. Ter Louw and V. N. Venkatakrishnan, “Blueprint: Robust prevention of cross-site scripting attacks for existing browsers,” in Security and Privacy, 2009 30th IEEE Symposium on, 2009, pp. 331–346.

[21] V. S. K. Maddineni and S. Ragi, “Security Techniques for protecting data in Cloud Computing.” 2012.

[22] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, “Systematic literature reviews in software engineering–a systematic literature review,” Inf. Softw. Technol., vol. 51, no. 1, pp. 7–15, 2009.

[23] B. A. Kitchenham, T. Dyba, and M. Jorgensen, “Evidence-based software engineering,” in Proceedings of the 26th international conference on software engineering, 2004, pp. 273–281.

[24] V. Ramesh, R. L. Glass, and I. Vessey, “Research in computer science: an empirical study,” J. Syst. Softw., vol. 70, no. 1, pp. 165–176, 2004.

[25] A. Strauss and J. Corbin, Basics of qualitative research, vol. 15. Newbury Park, CA: Sage, 1990.
[26] M. A. Khan, "A survey of security issues for cloud computing," J. Netw. Comput. Appl., vol. 71, pp. 11–29, 2016.
[27] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, 2012, vol. 1, pp. 647–651.
[28] S. Singh, Y.-S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," J. Netw. Comput. Appl., vol. 75, pp. 200–222, 2016.
[29] S. N. Kumar and A. Vajpayee, "A Survey on Secure Cloud: Security and Privacy in Cloud Computing," Am. J. Syst. Softw., vol. 4, no. 1, pp. 14–26, 2016.
[30] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Futur. Gener. Comput. Syst., vol. 82, pp. 395–411, May 2018.
[31] N. H. Hussein, A. Khalid, and K. Khanfar, "A Survey of Cryptography Cloud Storage Techniques," Int. J. Comput. Sci. Mob. Comput. pg, pp. 186–191, 2016.
[32] M. Ali, S. U. Khan, and A. V Vasilakos, "Security in cloud computing: Opportunities and challenges," Inf. Sci. (Ny)., vol. 305, pp. 357–383, 2015.
[33] Y. Liu, Y. Sun, J. Ryoo, S. Rizvi, and A. V Vasilakos, "A survey of security and privacy challenges in cloud computing: solutions and future directions," J. Comput. Sci. Eng., vol. 9, no. 3, pp. 119–133, 2015.
[34] R. Charanya, M. Aramudhan, K. Mohan, and S. Nithya, "Levels of security issues in cloud computing," Int. J. Eng. Technol., vol. 5, no. 2, pp. 1912–1920, 2013.
[35] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," J. Internet Serv. Appl., vol. 4, no. 1, p. 5, 2013.
[36] R. Bhadauria and S. Sanyal, "Survey on security issues in cloud computing and associated mitigation techniques," arXiv Prepr. arXiv1204.0764, 2012.
[37] M. Z. Meetei and A. Goel, "Security issues in cloud computing," in Biomedical Engineering and Informatics (BMEI), 2012 5th International Conference on, 2012, pp. 1321–1325.
[38] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Futur. Gener. Comput. Syst., vol. 28, no. 3, pp. 583–592, 2012.
[39] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "On technical security issues in cloud computing," in Cloud Computing, 2009. CLOUD'09. IEEE International Conference on, 2009, pp. 109–116.
[40] W.-J. Fan, S.-L. Yang, H. Perros, and J. Pei, "A multi-dimensional trust-aware cloud service selection mechanism based on evidential reasoning approach," Int. J. Autom. Comput., vol. 12, no. 2, pp. 208–219, 2015.
[41] M. Ouedraogo, S. Mignon, H. Cholez, S. Furnell, and E. Dubois, "Security transparency: the next frontier for security research in the cloud," J. Cloud Comput., vol. 4, no. 1, p. 12, 2015.
[42] P. Saripalli and B. Walters, "Quirc: A quantitative impact and risk assessment framework for cloud security," in Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, 2010, pp. 280–288.
[43] W. A. Jansen, "Cloud hooks: Security and privacy issues in cloud computing," in System Sciences (HICSS), 2011 44th Hawaii International Conference on, 2011, pp. 1–10.
[44] D. Attas and O. Batrafi, "Efficient integrity checking technique for securing client data in cloud computing," IJECS, vol. 8282, no. 6105, p. 11, 2011.
[45] F. Lombardi and R. Di Pietro, "Secure virtualization for cloud computing," J. Netw. Comput. Appl., vol. 34, no. 4, pp. 1113–1122, 2011.
[46] X. Chen, S. Chen, X. Zeng, X. Zheng, Y. Zhang, and C. Rong, "Framework for context-aware computation offloading in mobile cloud computing," J. Cloud Comput., vol. 6, no. 1, p. 1, 2017.
[47] D. Riquet, G. Grimaud, and M. Hauspie, "Large-scale coordinated attacks: Impact on the cloud security," in Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on, 2012, pp. 558–563.
[48] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (idps)," NIST Spec. Publ., vol. 800, no. 2007, p. 94, 2007.
[49] J. Karlin, S. Forrest, and J. Rexford, "Autonomous security for autonomous systems," Comput. Networks, vol. 52, no. 15, pp. 2908–2923, 2008.
[50] F. V. Alejandre, N. C. Cortés, and E. A. Anaya, "Feature selection to detect botnets using machine learning algorithms," in Electronics, Communications and Computers (CONIELECOMP), 2017 International Conference on, 2017, pp. 1–7.
[51] W. Lin and D. Lee, "Traceback Attacks in Cloud--Pebbletrace Botnet," in Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on, 2012, pp. 417–426.
[52] K. Kourai, T. Azumi, and S. Chiba, "A self-protection mechanism against stepping-stone attacks for IaaS clouds," in Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing (UIC/ATC), 2012 9th International Conference on, 2012, pp. 539–546.
[53] Y. Chen, X. Li, and F. Chen, "Overview and analysis of cloud computing research and application," in E-Business and E-Government (ICEE), 2011 International Conference on, 2011, pp. 1–4.
[54] G. Doychev, B. Köpf, L. Mauborgne, and J. Reineke, "Cacheaudit: A tool for the static analysis of cache side channels," ACM Trans. Inf. Syst. Secur., vol. 18, no. 1, p. 4, 2015.
[55] S. Luo, Z. Lin, X. Chen, Z. Yang, and J. Chen, "Virtualization security for cloud computing service," in Cloud and Service Computing (CSC), 2011 International Conference on, 2011, pp. 174–179.
[56] H. Wu, Y. Ding, C. Winer, and L. Yao, "Network security for virtual machine in cloud computing," in Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on, 2010, pp. 18–21.
[57] K. Vieira, A. Schulter, C. Westphall, and C. Westphall, "Intrusion detection techniques in grid and cloud computing environment," IT Prof. IEEE Comput. Soc., vol. 12, no. 4, pp. 38–43, 2010.

[58] D. Gollmann, “Securing web applications,” Inf. Secur. Tech. Rep., vol. 13, no. 1, pp. 1–9, 2008.
[59] R. Lua and K. C. Yow, “Mitigating ddos attacks with transparent and intelligent fast-flux swarm network,” IEEE Netw., vol. 25, no. 4, 2011.
[60] A. Bakshi and Y. B. Dujodwala, “Securing cloud from ddos attacks using intrusion detection system in virtual machine,” in Communication Software and Networks, 2010. ICCSN’10. Second International Conference on, 2010, pp. 260–264.
[61] S. Sridhar and S. Smys, “A Survey on Cloud Security Issues and Challenges with Possible Measures,” in International Conference on Inventive Research in Engineering and Technology, 2016, vol. 4.
[62] S. S. Jadhav, P. K. Hagwane, P. C. Labhade, and K. S. Nalawde, “Data Confidentiality in Cloud Computing Using Android Application,” Imp. J. Interdiscip. Res., vol. 2, no. 6, 2016.
[63] D. Pratiba, G. Shobha, S. Tandon, and S. B. Srushti, “Cache based Side Channel Attack on AES in Cloud Computing Environment,” Int. J. Comput. Appl., vol. 119, no. 13, 2015.
[64] M. Godfrey and M. Zulkernine, “A server-side solution to cache-based side-channel attacks in the cloud,” in Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on, 2013, pp. 163–170.
[65] G. Xiaopeng, W. Sumei, and C. Xianqin, “VNSS: a Network Security sandbox for virtual Computing environment,” in Information Computing and Telecommunications (YC-ICT), 2010 IEEE Youth Conference on, 2010, pp. 395–398.
[66] F. Zhou, M. Goel, P. Desnoyers, and R. Sundaram, “Scheduler vulnerabilities and coordinated attacks in cloud computing,” J. Comput. Secur., vol. 21, no. 4, pp. 533–559, 2013.
[67] N. Gruschka and M. Jensen, “Attack surfaces: A taxonomy for attacks on cloud services,” in Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, 2010, pp. 276–279.
[68] J. Clarke-Salt, SQL injection attacks and defense. Elsevier, 2009.
[69] A. Liu, Y. Yuan, D. Wijesekera, and A. Stavrou, “SQLProb: a proxy-based architecture towards preventing SQL injection attacks,” in Proceedings of the 2009 ACM symposium on Applied Computing, 2009, pp. 2054–2061.
[70] F. Callegati, W. Cerroni, and M. Ramilli, “Man-in-the-Middle Attack to the HTTPS Protocol,” IEEE Secur. Priv., vol. 7, no. 1, pp. 78–81, 2009.