IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-8, Aug 2019 E-ISSN: 2347-2693

A Critical Survey on: Cloud Security and privacy issues and its associated solutions

Smita Sharma[1*], R.P. Singh[2]

[1,2]Department of Computer Science& Engineering, SSSUTMS, Sehore (M.P.), India

Corresponding Author: sharmasmita34@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i8.288296 | Available online at: www.ijcseonline.org

Accepted: 14/Aug/2019, Published: 31/Aug/2019

***Abstract* -** Cloud computing is a set of web-based resources and services. Cloud services are delivered worldwide from data centers. By providing virtual resources via the internet, cloud computing facilitates its consumers. Google apps, provided by Google and Microsoft SharePoint, are a general example of cloud services. The rapid growth in the "cloud computing" field also increases serious security concerns. Security remained a constant problem for Open Systems and the Internet. Lack of security is the only obstacle to broad cloud computing adoption. The cloud computing boom has created many security challenges for consumers and service providers. This survey aims to identify the most vulnerable security threats in cloud computing, enabling both end users and vendors to understand the key security threats associated with cloud computing. Our work will enable researchers and security professionals to know about the concerns of users and vendors and critical analysis of the various proposed security models and tools. In a cloud computing environment, all data resides over a set of networked resources, enabling access to data via virtual machines. Because these data centers may be beyond the reach and control of users in any corner of the world, there are multiple security and privacy challenges that need to be understood and addressed. There are various issues that need to be addressed in a cloud computing scenario regarding security and privacy. This survey paper aims at elaborating and analyzing the numerous unresolved issues that threaten the adoption and diffusion of cloud computing.

***Keywords* -** Cloud computing, Cloud Security, DDoS attacks, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS).

I. INTRODUCTION

Cloud computing (CC) is not a particular technology, but a concept based on parallel computing, distributed computing and grid computing[17]. NIST (National Institute of Standards and Technology) defines cloud computing as follows:' Cloud computing is a model that enables omnipresent, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be quickly delivered and released with minimal management or service provider interactions[18]. This definition clearly states that CC helps minimize the expenditure of an organization on resource management and also reduces the user's software or hardware maintenance burden. Cloud computing is one of the fastest emerging computing technologies. In our daily lives, everyone uses cloud computing in one form or another without realizing it, such as Microsoft Office 365, Gmail and Drop-box etc. There are many advantages to using cloud computing such as accessibility whenever and wherever, better geographic coverage with the fastest time, less investment in infrastructure, etc., but there are also challenges to use cloud computing such as data security, lack of services and resources. Among the challenges is data security and privacy, and this paper explores the challenges of data security in cloud computing and provides methodologies for overcoming data security challenges. The main objective of this survey paper is to identify, classify, organize and quantify key security concerns and cloud - related solutions with the aim of organizing this information into useful tool for comparing, relating and classifying already identified concerns and solutions. Cloud computing is frequently compared with the following technologies, each of which shares some certain key aspects with cloud computing: grid computing is a distributed computing framework that co - ordinates interconnected resources to meet a common computing goal.

Grid Computing - Grid computing development was originally guided by computational complexity-advanced scientific software applications. Cloud computing is similar to grid computing because it also uses networked resources to ensure goals at application level. Cloud computing, however, takes one step even further by utilizing multi-level (hardware and application platform) virtualization

technologies to acknowledge resource sharing and cohesive resource sharing.

Utilities Computing - Utilities Computing is the paradigm of providing good on-demand resources and charging a fee to the customer based on use rather than a fixed amount. Cloud computing can be seen as a utility computing revelation. It adopts a pricing model based primarily on services for economical reasons. Service providers can genuinely maximize resource consumption and minimize their operating expenses with on-demand resource load balancing and utility-based cost structure.

Virtualization - Virtualization is a modern technology that abstracts physical hardware specific details and offers high-level applications with virtualized valuable resources. A virtualized server is often referred to as a virtual machine (VM). Virtualization forms the foundation of cloud computing, as it provides the capability of pooling computing resources from clusters of servers and dynamically assigning or reassigning virtual resources to applications on-demand.

Autonomic Computing: Originally coined by IBM in 2001, autonomic computing aims at building computing systems capable of self-management, i.e. reacting to internal and external observations without human intervention. The goal of autonomic computing is to overcome the management complexity of today's computer systems. Although cloud computing exhibits certain autonomic features such as automatic resource provisioning, its objective is to lower the resource cost rather than to reduce system complexity. In summary, cloud computing leverages virtualization technology to achieve the goal of providing computing resources as a utility. It shares certain aspects with grid computing and autonomic computing but differs from them in other aspects. Therefore, it offers unique benefits and imposes distinctive challenges to meet its requirements.

Web Service and SOA: Web services provided services over the web using technologies like XML, Web Services Description Language (WSDL), Simple Object Access Protocol (SOAP), and Universal Description, Discovery, and Integration (UDDI). The service organization inside a cloud is managed in the form of Service Oriented Architecture (SOA) and hence we can define SOA as something that makes use of multiple services to perform a specific task.

Application Programming Interface (API): Without API's it's hard to believe the existence of cloud computing. The whole bunches of cloud services depend on API's and allow deployment and configuration through them. Based on the API category used viz. Control, Data and Application API's different functions are being controlled and services rendered to the users.

Web 2.0 and mash-up: Web 2.0 has been defined as a technology, enabling us to create web pages that don't limit a user to viewing only; in fact it allows the users to make dynamic updates as well. It enables the usage of World Wide Web technology towards a more creative and a collaborative platform. Mash-up is a web application that combines data from more than one source into a single integrated storage tool.

These were the few technological advances that led to the emergence of Cloud Computing and enabled a lot of service providers to provide the customers a hassle free world of virtualization fulfilling all their demands.

Rest of the paper is organized as follows: Section I discusses the evaluation of cloud computing and its standard definition. Section II describes the cloud computing model in detail along with its essential characteristics. Section III contains the analysis of work done in the field of security in cloud computing .Section IV describes various possible attacks in cloud computing. Section V discuss various privacy problems in cloud computing and some of the existing solutions. Section VI concludes research work with future directions .

II. CLOUD COMPUTING MODEL

The CC Business Model implies five major actors [1] in cloud computing based on their participation as shown in Fig. 1.
Cloud consumer or cloud service consumer (CSC) - This is the one who gets the service from a cloud provider and pays for the service as per the use.

Cloud provider or cloud service provider (CSP) - This is the one who provides the cloud services to the CSC. Cloud auditor- This is the one who conducts an independent assessment of cloud services, information system operations, performance and security of the cloud implementations.

Cloud broker - This is the one who interacts between CSP and CSC to make the business happen. Cloud carrier is the one who provides the connectivity and cloud services from CSP to CSC.

Table 1 clearly determines the roles of CSP (shown in boldface) and CSC in the delivery models' services. In IaaS, the CSP provides only the infrastructure like server, storage, networks and virtualization. The CSC is responsible for Application, data, runtime, middleware and operating systems. In PaaS, only the Application and Data are CSC's responsibility In SaaS, all the nine services are provided by CSP.

TABLE 1. SERVICES PROVIDED BY DELIVERY MODELS AND THE RESPONSIBILITY

Services Provided by Delivery Models	IaaS	Paas	SaaS
Application	CSC	CSC	**CSP**
Data	CSC	CSC	**CSP**
Runtime	CSC	**CSP**	**CSP**
Middleware	CSC	**CSP**	**CSP**
Operating System	CSC	**CSP**	**CSP**
Virtualization	**CSP**	**CSP**	**CSP**
Server	**CSP**	**CSP**	**CSP**
Storage	**CSP**	**CSP**	**CSP**
Networking	**CSP**	**CSP**	**CSP**

NIST based cloud computing model consists of four cloud deployment models, three service delivery models and five essential characteristics.

II.I.CLOUD SERVICE DELIVERY MODELS :
Cloud computing offers a large variety of services to its users. The users can use these services online and they have to pay for what they use. In this section we will discuss various service models of cloud.According to the different types of services offered, cloud computing can be considered to consist of three layers:

II.I.I.Software as a Service :The first and highest layer is known as: Software as a Service (SaaS). It represents the applications that are deployed/enabled over a cloud by CSPs. These are mature applications that often offer an API to allow for greater application extensibility. For instance, Google Docs can be seen as the archetypal SaaS application, it has been deployed solely within the Cloud and offers several APIs to promote use of the application. Software‘s are provided as a service to the consumers according to their requirement, enables consumers to use the services that are hosted on the cloud server.

II.I.II.Platform as a Service : The middle-ware layer is known as: Platform as a Service (PaaS). This represents a development platform that developers can utilise to write, deploy and manage applications that run on the cloud. This can include aspects such as development, administration and management tools, run-time and data management engines, and security and user management services. Clients are provided platforms access, which enables them to put their own customized software‘s and other applications on the clouds.

II.I.III.Infrastructure as a Service:The lowest layer is known as: Infrastructure as a Service (IaaS). CSP over developers, a highly scaled and elastic computing infrastructure that are used to run applications. This infrastructure can be comprised of virtualized servers, storage, databases and other items.

II.II. CLOUD DEPLOYMENT MODELS :
SaaS, PaaS and IaaS are prevalent among providers and users among the service models mentioned above.To utilize cloud computing characteristics[19][20], these services can be deployed on one or more deployment models such as public cloud, private cloud, community cloud and hybrid cloud. These deployment models are explained as follows :

II.II.I.Public Cloud :-Large industrial groups or the public have access to this type of infrastructure. These are developed and owned by the cloud services sales organization[21]. The user will have to pay for the service he uses. Public clouds can be owned and utilized by government organizations. Public clouds provide many key advantages to the service providers, including no starting investment in infrastructure and threat switch to infrastructure providers. Though, public cloud absence fine-grained control over data, network, and security and privacy settings that may harm their usefulness in many business situations.

II.II.II. Private Cloud:-Private clouds are intended to be used predominantly by a single organization. The organization or external providers may construct and maintain a private cloud. Private cloud advantages are apparent. First, data is considerably safer than other techniques of deployment. Typically, a private cloud is constructed at the back of the firewall, so it is safer than a public cloud. Then it advantages from SLA as well. When the company staff retrieve applications established on a private cloud, the SLA is extremely reliable irrespective of the impact of volatile internet connection because the cloud would be somewhere behind a firewall instead of a remote workstation.[21].

II.II.III.Hybrid Cloud-This cloud comprises both public and private cloud characteristics. It tries to address each approach's limits. In a hybrid cloud, small part of the service operate in private clouds, while the rest operate in public clouds. Hybrid clouds provide considerable flexibility than private and public clouds. In particular, they offers hard control and safety of application data contrast to public clouds, while promoting development and shrinking of on-demand service. To build a hybrid cloud on the down side, the best splitting between public and private cloud modules needs to be properly defined.
II.II.IV.Community cloud :- In a shared non-public cloud, a community cloud permits multiple autonomous entities to gain cost benefits. It is a element in the public cloud, deployed and developed as a community on a certain range of area. This model has huge potential for companies or organizations that are immune to the same regulatory, compliance, or legal restrictions. Community clouds are generally created where users have similar needs and provide integrated services.Cloud hosts, cloud servers, cloud storage, and a cloud data-center services are included. Several organizations share this

kind of cloud infrastructure and support a particular community with shared issues.

II.III.CHARACTERISTICS OF CLOUD COMPUTING :
Cloud computing is distinguished by its characteristics from other computing frameworks or model. These features are classified into necessary characteristics which are as follows:
II.III.I.On-demand self-service: It allows the user to provide computing capabilities unilaterally as server time and network storage. Without the need for human interaction with every ;service provider, this is feasible. Users can immediately retrieve computing resources according to their requests.

II.III.II.Broad network access : It relates to the circumstances in which users can the retrieve computing abilities over the network. Users can retrieves cloud resources via standard methods that allow them to use interdependent platforms such as mobile phones, laptops, and PCs to access cloud resources.Therefore, to retrieve cloud-based services, users do not have to be at particular locations.

II.III.III.Resource pooling: Service providers combine computing resources with each other to meet multiple different users ' computing requirements through numerous physical and virtual assets. Multiple users share the pooled resources (such as servers, storage devices, etc.). Providers choose which resources from the pool to allocate the workload of each cloud consumer to standardize service quality. Sharing inhibits cost reductions as it enables the cloud's computing hardware to serve more applications than would have been permitted with dedicated computing resources.

II.III.IV.Rapid elasticity: This relates to the fast and elasticated regulatory framework of computing abilities to scale out rapidly, and fast release to scale in rapidly. The capabilities provided to consumers are limitless and can be bought at any time in any amount.

II.III.V.Measured service: This service regulates and optimizes the use of resources instantly. It is accomplished at an appropriate level of abstraction for the CC service type. This feature allows for monitoring, manipulating and reporting the use of resources and thus allowing honest transactions of services.

III. LITERATURE REVIEW

Haider Abbas et al.[1] conducted a state of the art survey that help researchers share their research with the community an d also provides guidance on how research can benefit the cloud community. He also offered multiple data security and privacy solutions to problem.

Minhaj Ahmad Khan et al.[2] conducted a survey on cloud security issues. Security threats have been categorized and the statistical study of security issues is also recognized along with its solutions. The research's new work is to develop strong data security methods.

Bob Duncan et al.
[3] recognized the issues facing by the enterprises that are lo oking forward to achieve good security metrics.Therefore, the t hreat of weak cloud service provider and SLA can directly im pact data security through the use of audit trail.
Deepak Puthal et al.[4] examined cloud computing open difficulties. Authors discussed the architecture and facilities of cloud computing in short, then illustrating security problems in cloud computing. Authors have categorized the problems and methodology that deal with such issues at operational level, customer level, service level, application level.

Mazhar Ali et al.[5] conducted a survey of cloud computing security issues. In cloud computing, authors have also identified various security threats and weaknesses. The researcher's survey recognized various security threats and mitigating strategies

The multi-tenancy problem was clearly identified by Mohamed Al Morsey et al.[6]. Several users can share the same resource in multi tenant domain so there is a likelihood of a security threat to occur. Authors have proposed the cloud economic model to solve the issues

In this paper, Rongxing et al[7] presented a new suggestion for data forensics and post-evaluation security and authenticity in cloud computing. Their suggested secure provenance strategy is working on the bilinear coupling method and they stated it as the required fundamental building blocks of data forensics and cloud computing environment post-evaluation. They have explicitly authenticated that the suggested strategy is safe in the standard model using verified security methods.

According to La‘Quata Sumter et al. [8] , increase in cloud computing scope has caused fear of Cyber security and the issue of security in cloud computing continues to grow. To ensure that information is safe and secure and accessible by unauthorized users, authors have suggested designing a system that will encapsulate the development and processing of information stored on the cloud. The suggested framework is based on a case study and is carried out in a relatively small cloud computing domain. According to Mladen[9] ,cloud computing is a latest field that emerged after years of research in networking and various kinds of computing. This research discusses cloud computing -related issues The research ranked security as the principle issue in cloud computing. Service providers should ensure the availability and reliability of services available to users whenever they use the internet, plus security, data protection and privacy. The main aim of this research Is to identify security and implementation problems.

In this paper, Wenchao et al.[10] took alternative views and suggested cloud security data-centric opinions. They examined the security characteristics of secure data sharing among cloud-owned applications. They suggested an advanced cloud computing security platform called Declarative Secure Distributed Systems (DS2).

In this paper, Soren et al[11] stated that cloud advantages are obscured by security and privacy difficulties, and the acceptance of cloud computing has been largely stimulated as a result of these difficulties. An strategy to evaluating security on the client side and on the server side was addressed in this paper. Rituik et al.[12] focused on the ch-allenges of job verification and cloud service users can authenticate the service provider's cost s for the services they utilize.Table II describes the problem covered and solutions provided in literature survey.

TABLE 2. REVIEW OF PROBLEMS COVERED AND SOLUTIONS PROVIDED IN LITERATURE SURVEY

Author	Context Of research	Types of Security Issues	Solution for Security Issues
Haider Abbas et al. [1]	Security & Privacy Challenges in Cloud Computing	DoS, detection of anomalies, data security, security of the network	Affinity –Based Victim Service Resizing Algorithm, Network-Based framework
Minhaj Ahmad Khan et al. [2]	Issues of Cloud Security their & comparison	Spoofing Attacks DoS,Malicious Insider	Cryptographic keys, SNORT,IDS,AES
Bob Duncan et al. [3]	Enhancing Cloud Security & Privacy through Audit Trial	Compliance with standard audit issues, company security culture	Audit Trial
Deepak Puthal et al. [4]	Analyzing of cloud computing features, issues & challenges	Data Security, Network Security, Data Segregation Data Access	Techniques for encryption and secure conven tion
Mazhar Ali et al. [5]	Opportunities and challenges in security in cloud computing	API Issues, Identity management and access control,VM Security	ACPS,SNORT IDS,Cyber Guarder, VM IPSec
Mohame d Al Morsey et al. [6]	Analysis of the Cloud Security Problem	VM Security, Hypervisor Security, Virtual Network Security, API Security	Identity & Access Management, Key Management
Rongxin g et al [7] (4cd)	Secure Provenance in Cloud Computing	Data forensics and post investigation in cloud computing	Bilinear pairing method
La'Quat a Sumter et al. [8]	Trusted Cloud Computing	Security Risk and Security assurance to cloud users	Trusted Cloud Computing Platform (TCCP)
Mladen [9]	Implementatio n and research issues in cloud computing	SSH tunnels and VLANs, verifiable integrity and complete service isolation vi a VPN	Virtual Computing Laboratory (VCL) Technology, open source
Wencha o et al. [10]	Data- centric cloud security	Secure Query Processing and Data Sharing. System Analysis and Forensics, Query Correctness Assurance	DS 2 Platform
Soren et al [11]	Security audit in public infrastructure Clouds	Reachability, Audit of Amazon Security Groups & Security Graphs.	Amazon's Elastic Compute Cloud (EC2)
Rituik et al [12]	Addressing security issues in cloud computing.	Metering problem, Proof of work, Attack scenarios & data Backups	A simulation program coded in JAVA,

IV.ATTACKS IN CLOUD SECURITY

The several security threats in cloud computing includes the following :

IV.IBUFFER OVERFLOW ATTACKS :A buffer overflow is the situation when the data sent to the buffer exceeds[22]. When a program executes, a segment of the adjacent memory location is allocated by the system to store different data types;

this memory slot is called a buffer. Buffer overflow may arise with a absence of authorization of data stored into a buffer: large amounts data overflows the buffer and modifies the adjacent memory. The data overflowing to adjacent memory makes the system more susceptible to multiple attacks as it enables intruders to deploy complex programs that cause greater harm[23].

IV.II.CLOUD AUTHENTICATI-ON ATTACKS :
Authentication is a mechanism that guarantees and indicates the correctness and validity of a user's certificate. First, the user must indicate his access rights and have the necessary property preferred for the authentication process[24].
In a cloud computing circumstances a user tries to create a connection with cloud services using his own certificates that authenticate him to utilize cloud services[25].

Threats and attacks on authentication in cloud environment include:
IV.I.I.Brute Force Attacks: The goal of cloud malware injection attacks is to inject malicious virtual machine (IaaS) or service execution (PaaS or SaaS) into the cloud computing system. These attacks can lead to eavesdropping by overt alteration of data, complete changes in functionality, blocking, and so on[50]. Crackers generate their malicious service implementation framework modules or virtual machines to achieve this and add connect to the cloud computing system.The crackers then trap the system to classify the target's malicious facilities or VMs as legitimate ones. The cloud computing system accordingly changes legitimate user requests to the fraud system when the attack accomplishes, permitting the execution of the opponent code[26].

IV.I.II.DOS Attacks: Denial-of-Service (DOS) is one of the cloud computing's significant security threats[162]. A DOS attack is imminent when an intruder tries to
refuse access to data and cloud computing services to authorized users[28].

IV.I.III.DDoS attacks : A DDOS attack requires using numerous manipulated systems to attack and corrupt a specific cloud to inhibit DOS attacks[29].DDoS attacks on an application layer may benefit from web application in-capabilities. They are often difficult or impossible to detect at the network layer, various security techniques will not be able to help, restricting a website operator to depend on a combination of cloud-based or proxy-based measures and best methods in application design and management of its shielding layout.

IV.I.IV.Insecure API's :Insecure Application Programming Interfaces (APIs) are one of cloud computing's key security problems. APIs are one of the main targets for cyber criminals trying to break the network of a company as they behave as a public main door for any application program and must be made available externally by default. Crackers use limited authentication, permission, and encryption. Cloud providers and software developers use APIs to enable their clients to communicate, retrieve and maintain cloud services data. APIS can be utilized in three ways. First , they can be utilized to fetch logs from applications. Secondy, they can be utilized to promote both database inclusion and storage elements. Third, they can be used to manage specific resources in the cloud. In addition, APIs are the main platforms through which websites or back-end services communicate with mobile applications. They also facilitate user authentication.

IV.I.V.Malicious Insiders : A malicious insider may be employee, consultant or business associate permitted to access network, system or information using his rights for malicious reasons. specifically, an insider's actions may be missed by network firewalls and intrusion detection systems, considering that they are permitted. Malicious insiders with significant access to cloud resources can cause significantly more harm in cloud computing than in typical single-organization information, primarily because a cloud computing attack by an insider can influence a large number of cloud consumers. Malicious insiders can have a major impact on service providers, such as retrieval of confidential data, and take control over cloud services without identification.The risk can be presented by restricting access to cloud services and information ; expanding transparency in security and management processes, including compliance detection and alerting at the time of breach[27].

IV.I.VI.SQL Injection Attacks :An attack on SQL injection arises when a mischievous user injects susceptible code into a cloud to harm cloud computing programs. Using vulnerabilities in SQL code, attackers can achieve user access to cloud information , namely extracting secret database information. An attacker may also generate a completely new malicious SQL query in an SQL injection attack to execute an unauthorized program of the database. It may harm the security and privacy of the database-dependent websites.

V.PRIVACY PROBLEMS IN CLOUD COMPUTING

Privacy is a key issue in cloud computing because the data and enterprise reasoning of a customer must be assigned to cloud servers owned and managed by cloud providers and not by the customer. The privacy threats of the data of individuals in clouds occur when sharing it with others when they are retrieved for improper use by the provider. Confidentiality concerns takes place in the provider not resolving the information leakage loopholes or exchanging information about their clients with others without the user's permission. Service terms and privacy policies enforced by service providers [30] control the risks of privacy and confidentiality.

V.I.PROBLEMS:VULNERABI-
ITIES,THREATS AND ATTACKS -
Privacy is probably one of the problems that manipulate personal information. Privacy is an individual or group's capability to selectively disclose themselves or information about themselves. Some vulnerabilities, privacy threats and attacks are as follows:-

V.I.I.Broken Authentication and Compromised Credentials : Broken authentication pertains to the condition where there is an insufficient framework for verifying user certificates. Privacy infringement for numerous cloud service users may occur when providers are unable to confirm that legitimate users have permission to access the data in the cloud. Only in uncorrupted computing systems ,authentication and access control are efficient .One of the causes of corrupted credentials is the incompetency or unavailability of security controls in cloud computing framework[31].

V.I.II Data Location Problems: Data location is among the most common safety issues encountered by an organization after cloud computing has been introduced. An organization constructs its computing framework in an in-house computing system and thus the location of the stored data and the strategies are adopted to protect the data. It is therefore hard to determine whether appropriate data protection methods have been implemented properly.

V.I.III. Problems Related to Data Ownership and Content Disclosure: Another key issue of cloud computing privacy is the issue of data ownership. As users stored their data on a cloud s, data privacy might be lost. Furthermore, the users are at possibility of losing the creator of ownership.

V.I.IV. Service level agreements for cloud security: In many instances, cloud computing constitutes automation of computation and storage to an external service provider. Such automation has been controlled by Service Level Agreements (SLAs), which determine minimum performance levels that can be expected by the customer. Traditionally, however, security characteristics such as privacy and confidentiality have not been addressed by SLAs. It is normal to expect in a cloud computing consumer market that not every providers will be prone to provide their consumers with the same level of privacy. In addition, a cloud provider may provide services with variable security measures based on how much the customer is ready to pay for a service. Bernsmed et al.[32] highlighted how a cloud SLA would be expanded to cover security key elements, enabling multiple service providers with a specified level of security to formulate cloud services. Typically, Security SLAs will adopt a workflow where they are first published by a provider, and when a user desires to make use of cloud service, they will negotiate a particular SLA that the provider will undertake to and provide the service.

V.I.V. Ensuring Security Against Various Types Of Attacks : Several cloud service providers develop different methods to protect the cloud against various security attacks such as: SQL injection, Cross Site Scripting (XSS) attacks, DoS and DDoS attacks, Google Hacking and Forced Hacking. Some standard methods for identifying the above-stated attacks are as follows: avoid using interactively created SQL in the code, discover the meta-structures used within the code, verify all parameters listed by the user, restrict and prevent useless data and characters. For an adaptive cost performance ratio, a standard security platform requires to be developed. Symantec Message Labs Web Security cloud is using a similar method that disables internet security risks and penetrates the data before they enter the network. It offers protection even in extremely divergent environments with its adaptable technological innovation and insures protection against new and rapidly moving threats to malware. A Google hacking database recognizes different types of information such as: login passwords, pages comprising logon portals, information about session usage, etc. It is possible to utilize numerous software alternatives such as the Web Vulnerability Scanner to identify the probability of a Google hack. The user must insure that only those data that will not have negatively impact on him should be shared with Google in order to avoid Google hacking. This would inhibit any sharing of confidential information that could lead to challenging conditions. In the case of IP spoofing, an attacker attempts to spoof users from trusted sources that the packets arrives. The attacker thus takes possession of the data or system of the client indicating himself to be the trusted party. Using encryption methods and executing key exchange-based user authentication, spoofing attacks can be detected.

TableIII provides comparative analysis for strengths and limitations of various existing security schemes.

TABLE 3. COMPARATIVE ANALYSIS FOR STRENGTHS AND LIMITATIONS OF SOME OF THE EXISTING SECURITY SCHEMES

Existing Security Schemes	Suggested Approach	Strengths	Limitations
Data Storage security [14]	Uses homomorphic token with distributed erasure - coded data verification to assure security of data storage and location of the attacked server.	Effective against attacks of data modification and server complicity and also byzantine failures.	Security was viewed in dynamic data storage. But, there are still threats to be identified with fine - grained data error location.
User identity security in cloud computing	Utilizes effective bundles scheme, comparing predicates to encrypted data and multi - party computing.	Requires no trusted third party (TTP) for user identity verification or approval. Therefore, the identity of the user is not revealed.	The host of the demanded service may not implement an active bundle . The identity continue to be hidden and the user is not permitted to his requests.
Trusted model for interoperability and security in cross cloud [15]	For providers and users, separate areas, each area is provided with a unique trust agent. Various methods of trust for cloud service providers and users.	Helps consumers to avoid destructive suppliers. Helps cloud service providers to prevent malicious users from cooperating / serving.	In a relatively small environment, this system can manage only a restricted number of security attacks
Virtualized defense and	Uses a hierarchical structure of DHT -	Comprehensive utilization of	The proposed method is in its

Reputation based trust Management	based interface networks, with each layer performing specific functions.	virtualization for cloud security	development stage and additional simulations are required to validate performance.
Safe, virtual network in Cloud environment[15]	It has been proposed that cloud providers abstract the underlying internal structure of their cloud services and placement measures and also emphasis on side - channel hazards to minimize the risk of disclose of information .	Insures the verification of the opponent or the opposing party and enables us find a distant place from their target for an opposing party and thus guarantees a safer framework for the other VMs.	If the opponent learns the other VM's location, it may attempt to attack them. This can damage the other intermediate VMs.
Border Gateway Protocol (BGP) [16]	A excellent architecture of BGP (PGBGP) has been recommended to verify the instances where an Autonomous System may erroneously reveal itself as the destination for all data being transported over that network.	Verifies autonomous systems (ASs) and plays detection of anomalies using a response system to assure that the data is not transferred to the incorrect AS.	Susceptible to attacks such as Denial of Service(DoS). This method only concentrate on the messages of routing control, but does not authenticate the path preceded by real traffic.
Client based Privacy Manager	Minimizes the threat of data leakage and loss of confidential data using strategies of obfuscation and de-obfuscation. The key concept is to save private data in the cloud in encrypted form..	It protects data privacy by configuring end - user service issues.	The fair coordination of service providers and vendors does not necessitate the addition of extra privacy policies.
Anonymity based methods	They support data anonymization of the algorithm before they were collected in the cloud. Whenever cloud service provider needs data that it uses domain expertise, anonymous data must be evaluated in order to obtain the necessary knowledge.	It is transparent and versatile and it is distinct from conventional cryptography.	It is restricted for number of offered services
Fully Homomorphic encryption	Current mechanism of encryption to protect data privacy has been modified, This encryption technique makes it possible to calculate the encrypted data that is preserved in the cloud.	Effective privacy support tool	Cannot use practically.
Privacy Persevering Repository	Built a database repository where information exchange services can update data and limit access by restricting data usage allocation.	Ensures data confidentiality and high reliability. Still not safe to meet all security challenges.	Perhaps not provide protection against all security attacks
Fog Computing	Techniques are used to audit the access rights by observing patterns of data retrieval	Provides protection from information misuse	Do not solve all the problems

VI. CONCLUSION AND FUTURE WORK

This paper provides an insight into various threats to the security and privacy of user-confidential data in the cloud environment. Researchers have suggested various methods to address issues using different methods that help to reduce the issue of data security and cloud privacy. We mentioned the benefits and weaknesses of current methods to fix security and privacy issues in their entirety. From the view-point of the user, cloud computing is going through serious security risks, it might be concluded that lack of security measures is the only remarkable drawback of cloud computing. Both service providers and customers need to work in collaboration to assure security and privacy of cloud and its data. For stronger cloud security, mutual trust between cloud service providers and consumers is essential. We have recognized in this paper, that security is the biggest obstacle in broad cloud computing acceptance. Cloud service users are afraid of loss of data and privacy. Researchers and IT security professionals need to come one step forward and need to take advanced steps to provide users with security and privacy.

REFERENCES

[1] H. Abbas, O. Maennel, S. Assar, "Security and privacy issues in cloud computing", Institut Mines-Télécom and Springer-Verlag France 2017.
[2] M. H. Khan, "A Survey of Security Issues For Cloud Computing", Journal of Network and Computer Applications, ELSEVIER 2016.
[3] B. Duncan, M. Whittington, "Enhancing Cloud Security and Privacy: The Power and the Weakness of the Audit Trail", CLOUD COMPUTING 2016 : The Seventh International Conference on Cloud Computing, GRIDs, and Virtualization.
[4] D. Puthal, B. P. S. Sahoo, S. Mishra, S. Swain, "Cloud Computing Features, Issues and Challenges: A Big Picture", 2015 International Conference on Computational Intelligence & Networks (CINE 2015)
[5] M. Ali, S U. Khan, A V. Vasilakos, "Security in cloud computing: Opportunities and challenges", Information Sciences 305 (2015) pp 357–383 ELSEVIER.
[6] M.Al Morsy, Z.Grundy, Ingo Müller, "An Analysis of the Cloud Computing Security Problem", 17th Asia-Pacific Software Engineering Conference (APSEC 2010) Cloud Workshop, Sydney, Australia, 30 November-03 December 2010.
[7] Rongxing et al, ―Secure Provenance: The Essential Bread and Butter of Data Forensics in Cloud Computing‖, ASIACCS'10, Beijing, China..
[8] R. La'Quata Sumter, ―Cloud Computing: Security Risk Classification‖, ACMSE 2010, Oxford, USA
[9]Mladen A. Vouch, ―Cloud Computing Issues, Research and Implementations‖, Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246

[10]Wenchaoet al, ―Towards a Data-centric View of Cloud Security‖, CloudDB 2010, Toronto, Canada
[11] Soren Bleikertz et al, ―Security Audits of Multi-tier Virtual Infrastructures in Public Infrastructure Clouds‖, CCSW 2010, Chicago, USA.
[12] Wayne A. Jansen, ―Cloud Hooks: Security and Privacy Issues in Cloud Computing , 44th Hawaii International Conference on System Sciesnces 2011.
[13] Dan Lin & Anna Squicciarini, ―Data Protection Models for Service Provisioning in the Cloud , SACMAT‘10, 2010, Pittsburgh, Pennsylvania, USA
[14]. Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing,"
17th International workshop on Quality of Service, USA, pp.1-9, July 13-15, 2009, ISBN: 978-1-4244-3875-4
[15].Shantanu Pal, Sunirmal Khatua, Nabendu Chaki, Sugata Sanyal, "A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security," Annals of Faculty Engineering Hunedoara International Journal of Engineering (Archived copy), scheduled for publication in vol. 10, issue 1, January 2012. ISSN: 1584-2665.
[16]Josh Karlin, Stephanie Forrest, Jennifer Rexford, "Autonomous Security for Autonomous Systems," Proc. Of Complex Computer and Communication Networks; vol. 52, issue. 15, pp. 2908- 2923, Elsevier, NY, USA, 2008.
[17] I Foster, Yong Zhao, I Raicu, and S Lu. Cloud computing and grid computing 360-degree compared. In Grid Computing Environments Workshop, 2008. GCE '08,
[18] Peter Mell and Tim Grance. The NIST definition of cloud computing. National Institute of Standards and Technology, 53(6):50, 2009. 7, 9
[19] William; Athley Ambrose. Cloud Computing : Security Risks, SLA, and Trust. 2010. With Cloud Computing becoming a popular term on the Information Technology (IT) market, security and accountability has become important issues to highlight.
[20] S. Ramgovind, Mariki M. Elo_, and E. Smith. "The management of security in cloud computing " Information Security for South Africa (ISSA), 2010
[21]Parkhill D (1966) The challenge of the computer utility. Addison-Wesley, Reading
[22] D. Naccache *et al.*, "Buffer Overflow Attacks," *Encyclopedia of Cryptography and Security*, Boston, MA: Springer US, 2011, pp. 174–177.
[23] K.S. Kumar and N.R. Kisore, "Protection against Buffer Overflow Attacks through Runtime Memory Layout Randomization," in *Intl Conf. on Information Technology*, 2014, pp. 184–189.
[24] C.P. Pfleeger and S.L. Pfleeger, "Security in computing," Prentice Hall, 2006.
[25] C. Cowan *et al.*, "StackGuard: Automatic Adaptive Detection and Prevention of Buffer-Overflow Attacks, " *7th USENIX Security Symp.*, San Antonio, Texas, Jan. 1998.
[26] S.K. Das, K. Kant, and N. Zhang, "Handbook on securing cyber-physical critical infrastructure," Morgan Kaufmann, 2012.
[27] A. Chonka, Y. Xiang, W. Zhou, and A. Bonti, "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks," *J. Netw. Comput. Appl.*, vol. 34 (4), July 2011, pp. 1097–1107.
[28] A. Mitrokotsa and C. Douligeris, "Detecting denial of service attacks using emergent self-organizing maps," 5th *IEEE Intl. Sym. on Signal Processing and Information Technology*, 2005, pp. 375–380.
[29] P.L.S. Kumari and A. Damodaram, "An Alternative Methodology for Authentication and Confidentiality Based on Zero Knowledge Protocols Using Diffie-Hellman Key Exchange," *Intl. Conf. on Information Technology*, 2014, pp. 368–373.
[30] Z. Wang, K. Sun, S. Jajodia, and J. Jing, "Proof of Isolation for Cloud Storage," *Secure Cloud Computing*, Springer, New York, 2014, pp. 95–121. [31] L. Rodero-Merino, L. Vaquero, E. Caron, F. Desprez, and A. Muresan, "Building Safe PaaS Clouds: a Survey on Security in Multitenant Software Platforms," *Computers and Security*, vol. 31 (1), Feb. 2012.
[32]R.L. Krutz and R.D. Vines, "*Cloud security : a comprehensive guide to secure cloud computing*,"Wiley, 2010.

Authors Profile

Smita Sharma has completed her B.Tech and M.Tech in Computer Science & Engineering from Rajiv Gandhi Technical University , Bhopal (M.P.) . She is currently a PH.D scholar in the Department of Computer Science and engineering in SSSUTMS . Her interests of research are cloud security , artificial intelligence and image processing. She has published more than 10 research papers in reputed international journals and conferences related to these research areas. She has about six years of teaching experience. She is a member of ACM . She is currently working as an Assistant Professor in Computer Science & Engineering department in University of Information Technology, Rajiv Gandhi Technical University , Bhopal (M.P.).

Dr. R.P. Singh is former Director and Prof. Electronics and Communication at Maulana Azad National Institute of Technology, (MANIT) Bhopal. Dr. Singh Graduated and Post Graduated in Electronic Engineering from Institute of Technology (now IIT), B.H.U. Varanasi in 1971 and 1973, respectively. He did his Ph.D. from Barakatullah University Bhopal in 1991. He has 39 years of teaching, research, and administrative experience in Maulana Azad College of Technology (MACT)/MANIT out of which 22 years as Professor. He was Head of the Department at of Electronics, and Computer Science and Engineering Department at MANIT Bhopal .He has worked as Professor In-charge Academic and Chairman Admission Committee Dean (Academic) & Dean (R/D) at MACT /MANIT, Bhopal. He has published 125 papers in National / International reputed and indexed Journals including SCI. He was Chairman of Computer Society of India. Bhopal. He has been Consulting Editor of Journal of Institution of Engineers and reviewer in many International/National Journals.

