Research Article

Hybrid Cloud Security Measures and Research Challenges

V.Ambica[1], Dr.A.Viji Amutha Mary[2],
venna.ambica@gmail.com,0000-0001-6262-4191
vijiamuthamary.cse@sathyabama.ac.in,0000-0002-9285-6484
[1,2]Sathyabama Institute of Science and Technology, Chennai, India

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract: Cloud Computing is a cropping technology. There are many researches going under this cloud technology. There are many challenges in terms of security for data stored in cloud. Currently there are four cloud deployment models named as public cloud, private cloud, community cloud and hybrid cloud available in the market. According to the requirements customers can avail one among the four available cloud models. This paper especially discusses the security problems and stinks occurs for hybrid cloud. This paper also analyzes various factors that effects the security of the information stored in cloud. It provides a better understanding of the cloud computing research challenges, open issues and helps to find top security threats and solutions in hybrid cloud.

Keywords: Hybrid cloud, security challenges, threats, solutions, reliability, scalability, privacy

1.Introduction

Cloud computing is an optimal way to provide computing resources on demand from software to internet storage and computational power and the preferred solutions for companies extending their infrastructure or launching new innovations. There are four types of cloud deployment models 1. Public cloud 2. Private cloud 3. Community cloud 4. Hybrid cloud.

1.1. Public cloud: The data stored in public clouds are accessible to the public which are created and stored on third party servers and service provider manages and administer pool resources. The user companies should not purchase,maintain and manage their own hardware.

Advantages:

- Low cost: The service which you use should Pay for that only. The hardware and software will be maintained by service providers.
- High Scalability: As per your company requirements you can easily extend your cloud capacity.
- High Reliability: Vast server networks to protect against failures

Disadvantages:

- Data security and privacy issues: The data is accessed by all the public and users know where their information is stored and who can access.
- Lack of tailored services: Service providers will offer only standardized services, which fail to satisfy the complex requirements of the customers.
- Lack of control: The client does not have any control on data or infrastructure and the service level policies and compliances are enforced by the service provider.

1.2.Private Cloud: There is no much difference between public and private cloud from the technical point of view, a specific company will maintain its own private cloud.

Advantages:

- High security and privacy: Only authorized persons can access the data.
- Tailored services: Companies offers customized services according the customer’s requirements.
- High scalability and Reliability: The private clouds deployed on the organization’s intranet, which guarantees the efficiency and performance of the network.
- Better control: Proper control on data and information assets.

Disadvantages:

- Cost: Initial hardware investment is very high in the case of on-premise infrastructure.
- Under-utilization: Some of the subscribed resources can be under-utilized. Optimization of all the resources is a big challenge.
- Vendor lock-in: The client organization is obligated to stay with the same service supplier as the hardware and infrastructure are outsourced by stopping the client from migrating to another vendor.

1.3.Community Cloud:

It is similar to the deployment of private cloud but the only difference is variety of companies of common histories share the facilities and other resources of one company that has the ownership of a private cloud server.

Advantages:

- Cost reduction
- High security, privacy and reliability
- Ease of exchange and collaboration of data

Disadvantages:

- Cost is high compared to public cloud
- Fixed space for data and bandwidth

1.4.Hybrid Cloud:

It combines the advantages of both public and private cloud systems, allowing the organizations to use public cloud for transfer of non-confidential data and private cloud for sensitive data. This model is gaining prominence in many businesses as it provides benefits of both clouds.

Advantages:

- Scalability
- Costefficient
- Security and flexibility

Disadvantages:

- Dependency: Depending only on single network of servers is risky in case of downtime especially for larger business with high demand for their services.
- Compliance: Make sure that all services in use are in line with company security policies to protect the data and assets against any misdemeanors.
- Network complexities: The complex system architecture of hybrid cloud will provide a facility to easily transfer data between public and private cloud networks but requires a great approach to management and maintenance.

2.Literature review

Many researchers provided that there are many security quibbles occurs for data which is stored in cloud. According to Mahak Sharma and Rajat Sehrawat,to enhance the ability to diagnose and track diseases at any time and anywhere and to access information in a timely manner CCA(Cloud Computing Adoption) is a new e-healthcare networks worldwide are becoming the perfect solution[1]. Tatiana Ermakova,Benjamin fabian,Marta kornacka,Scott thiebes and Ali sunyaev stated that the protection of medical data from unauthorized disclosure and modification is the highest importance to patients. Patients strive for the possibility to stay anonymous and control access rights to their medical data in the system[2].Rakesh Kumar, Rinkaj Goyalcontributed towards identifying a single taxonomy to carry out the planned end-to-end mapping for protection specifications,risks,weaknesses and countermeasures and highlights security stinks in other relevant fields,such as trust-based security models,cloud enabled applications of Big Data, Internet of Things (IoT), Software Defined Network (SDN) and Network[5].Shekha Chenthara,Khandakar Ahmed,Hua Wang,Frank Whittaker highlighted that study challenges and cyber security directions to develop a robust security model for EHR(Electronic-Health Records)[4,17,18].

3.Hybrid cloud security

Hybrid cloud security is the protection of the data, applications and infrastructure associated with an IT architecture that including public and private clouds[19,20].

Hybrid cloud let companies choose where to place workloads and information on the basis of enforcement, audit, regulation or security requirements. This separate yet connected architecture is what makes it possible for organizations to operate essential private cloud workloads and less responsive public cloud workloads. It is an agreement that minimizes data disclosure and encourages business to tailor a versatile IT portfolio.

3.1.Hybrid cloud Security Components:

Physical Controls: These are for securing the actual hardware. Example includes locks, guards and security closed circuit cameras.

Technical Controls: There are precautions built for IT networks themselves, such as tools for encryption, network authentication and control. Technical safeguards are one of the best hybrid cloud protection tools.

Administrative Controls: There are initiatives that help citizens respond in ways that increase protection, such as preparation and planning for disasters. The figure 1 shows the cloud computing challenges and open issues.

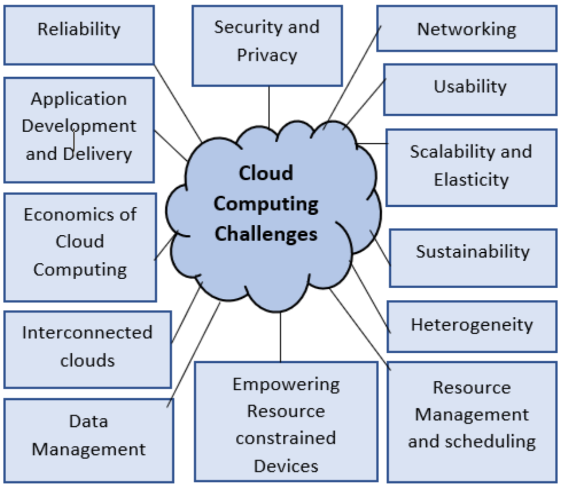

Reliability
Security and Privacy
Networking
Usability
Application Development and Delivery
Scalability and Elasticity
Cloud Computing Challenges
Economics of Cloud Computing
Sustainability
Heterogeneity
Interconnected clouds
Data Management
Empowering Resource constrained Devices
Resource Management and scheduling

Figure 1: Cloud Computing Challenges and Open Issues

3.2. Hybrid Cloud Security Challenges

3.2.1Protecting our Data: Restrict exposure to data for the organization through encryption. Thesimilar data would be in transit or at rest at various points in time requires a range of protection to minimize data disclosure during any of these states.

3.2.2. Compliance and governance: If the organizations are related to healthcare, finances or government, hybrid cloud technology may present additional considerations. The organizations need to check the distributed environments to ensure that they are compatible and must be prepared for security audits.

3.2.3. Security in the supply chain: In a dynamic ecosystem, hybrid cloud environments also contain products and applications from different vendors. The vendors will check and administrate their applications and products, how they will inspect source code and which implementation guidelines they follow, how and when vendors can provide updates and patches.

3.3. ResearchGaps:

Top security threats in Hybrid cloud

3.3.1. Lack of Encryption: Data transfer through networks is vulnerable to eaves dropping and Man-in the -Middle attacks that circumvent mutual authentication by impersonating end points.Mobility enterprise managers must encrypt communications and data to prevent security incursions.

Possible solutions:

i.By using Cryptographic protocols that includes endpoint authentication to protect from random attacks.
ii.Usage of Reliable Virtual Private Networks.
iii.By using SSL/TLS to encrypt all transmissions and to manage sever authentication and prevent interception of data.
iv.To send unencrypted traffic over a network use Secure socket shell.

3.3.2. InadequateSecurity Risk Assessment: Network administrators are prevented from assessing how and where an attack has occurred or whe n it happened by failing to conduct comprehensive risk profiles of an IT infrastructure and systems.
It makes potential infringements practically impossible to stop.

Possible solutions:

i.There must be robust risk management and evaluation in place - at all times.
ii.Any malicious traffic should always be scanned by IDS/IPS systems.
iii. Any malicious traffic should always be scanned by IDS/IPS systems.
iv. Log tracking and latest software updates must be activated.
v.The best way to manage network organization security using a stable SIEM system is a holistic approach. This allows all company security data to be accessed and trended easily.

3.3.3. Poor Compliance:

The Hybrid clouds need more due diligence. It must remain within compliance limits with both the providers of public cloud and private cloud services. In the hybrid model, preserving and explaining enforcement is more complex because knowledge travels back and forth.

Possible solutions:

i. It is important to coordinate the two clouds. Not only do you have to maintain compliance with your public cloud provider and private cloud, but show the compliance of the two clouds when they operate together.
ii.When processing confidential data, all clouds must comply with industry requirements for data protection.

3.3.4. Weak Security Management:

Too many company administrators run amuck because they fail to engage authentication of both their private and public cloud, identity managementand authorization procedures. Protocols for cloud protection must be integrated.

Possible solutions:

i. For both public and private clouds, replicate the controls.

ii.Synchronize security details or using a service for identity protection that works in either cloud for the systems you run.

iii.Maintain internal data storage for confidential data that is not suitable for public cloud storage.

3.3.5. Poor Data Redundancy:

A lack of redundancy puts at risk a hybrid IT cloud and the company. This is particularly true if you don't have adequately distributed redundant copies of data across all data centers. This way, spreading data mitigates the harm that happens when an interruption of one data center occurs.

Possible solutions:

i. Redundancy can be implemented by using various data centers from one cloud provider.

ii.From several providers of public clouds.

iii.Implement redundancy from a hybrid cloud

3.3.6. Failure to authenticate and identity:

When integrating public and private clouds in a hybrid setting, security management is essential. Between the cloud provider and enterprise employees, cybersecurity must be mutually shared.

Possible solutions:

i. Become diligent.

ii. Monitor and check all access permissions.

iii.Use an IP Multimedia Core Network Subsystem to synchronise data security (IMS).

3.3.7. Unprotected APIs: API endpoints, when unprotected, expose sensitive data to malicious attacks that leverage an authentication/authorization token or key to manipulate personal data and information. In enterprise mobility management and BYODtransmissions over unsecure connections, this vulnerability is of particular concern.

Possible solutions:

i. API keys must be treated the same way as code-signing and encryption keys.

ii.Third-party developers must be sure to safely manage keys.

iii.Often validate a third party to prevent a security breach before releasing API keys.

3.3.8. Denial of Service attacks: By issuing a DoS attack, attackers make a cloud or mobile enterprise unavailable. In the virtual world, network access is interrupted by an intrinsic limitation in shared resources, such as CPU, RAM, and disk space or network bandwidth.

Possible solutions:

i. Denial of Service attacks on APIs for cloud management are often caused by the company's sending bad SOAP or REST requests.

ii.By responding to the incursion and redirecting traffic to a mitigation device, flow analytics can fend off DoD attacks.

iii.Keep in mind, for the amount of traffic it collects and analyses, the flow analytics tool must be scalable. It is not as effective in battling volumetric (DDoS) attacks because it is a slower method.

3.3.9. Distributed Denial of Service (DDoS)Attacks:

These attacks on the volumetric or application layer are on the increase and more adverse than DoS. This is because they are maliciously spread and produced at a central location from different sources and created at a central location for high volume incursions. Network traffic is frequently in simulated gridlock when threats are observed and websites are rendered helpless.

Possible solutions:

i. Fending off a DDoS attack involves robust in-path deployment of a DDoS mitigation system that processes all incoming and outgoing traffic on an ongoing basis. When there aremulti-vector attacks, the device ought to be able to act immediately and scale and perform.

3.3.10. Poor IP Protection:

Extra protection is necessary for intellectual property (IP). It must be in place with the strongest encryption and authentication protocols. To determine potential security risks, IP must be identified and classified. A vulnerability assessment and suitable encryption are needed.

Possible solutions:

i. In classifying IP and quantifying risk, fully automated systems are inadequate. These assignments must be performed manually. IP-related risks can be identified only once that data is classified.

ii.Know the root of your risks. Create and follow a comprehensive threat model.

iii.Create a permission matrix.

iv.Harden all elements of open source to avoid incursions.

v.Conduct comprehensive investigations to third parties.
vi.Ensure that your network infrastructure is secure.

3.3.11. Lack of Data Ownership: When handling data, cloud vendors must be thoroughly vetted for security controls. Businesses lose some power to control their own data set until cloud-deployed. To avoid surprises, enterprise managers must know what protection levels are available in the cloud.

Possible solutions:

i. Ownership of data and confidentiality must be checked. Stop sellers who do not have fair standards of ownership.

ii.Get all specified in a well-constructed Service Level Agreement (SLA) covering a hybrid IT company from the supplier. Know precisely who has access to information, what the provider does with logs/statistics of access, and the jurisdiction/geographic location of all data stored.

3.3.12. Failure to Communicate with Provider:

Without having a written estimate and service information to be conducted on your vehicle, you will not get a car fixed. Agreements at the service level (SLAs) do the same. They explain goals and tasks.

Possible solutions:

i. A customer must let the cloud provider know exactly what security specifications are expected in the case of security. It prevents surprises and catastrophes. The CSA Protection, Confidence and Assurance Registry outlines the security controls provided in the marketplace by each cloud provider. As a guide, use it.

ii.Ask thorough questions. Unless a provider of servicesgives comprehensive responses about how they identify and secure multi-tenant boundaries, guarantee FISMA, compliance with PCI and auditing, call someone else.

3.3.13. Poorly defined SLAs: Customers lose the right to monitor their own data set when transitioning to the cloud, and are compelled to count on service providers to protect data properly when in the public sector.

Possible solutions:

i. Access permissions and safeguards must be explained and security provisions in the SLA must be well defined. The same applies to the cloud service provider's standards and specifications.

ii.In the Service Level Agreement, fair service standards must be clearly detailed such that the customer has recourse if service is interrupted or data is damaged.

iii.Have it checked by an attorney before signing any agreement.

3.3.14. Data Leakage: On the part of a cloud provider, inadequate security protocols can compromise data that can be corrupted, destroyed or improperly accessed. This is particularly true in environments with worker-driven BYOD.

Possible solutions:

i. Never assume that the provider, unless it is in writing, has data leakage covered. Prevention of data loss is key. Cover the bases all. Get the fine print read.

ii.Security is the responsibility of the customer as a client of the enterprise owns consumer data.

iii.Security measures must be capable of countering malfunctions in the infrastructure, violation of confidentiality and errors in software.

3.3.15. Poorly Defined Management Strategies:

Only when everyone knows what needs to be achieved is seamless hybrid cloud management achieved. With leadership policies and procedures, jobs must be strictly defined. It is possible to hack a network without these instructions. To handle the entire infrastructure, a holistic approach has to be taken.

Possible solutions:

i.Management tools and techniques must be compatible for computing, networking and storing resources over various domains. It is a hybrid cloud administrator's task to make sure this template is in operation.

ii.Cloud management policies should define the specifics of configuration and installation rules; access control for confidential information/restricted applications; and budget management and reporting.

iii. Know just what cross-platform tools to handle a hybrid cloud can be used.

For the best protection, describe access controls, user management, and encryption strictly.

Prepare access management policies that determine how both public and private clouds access sensitive data or limited applications.

Using configuration management tools to reduce misconfiguration errors and simplify image-build processes in resource provisioning.

3.3.16.Badly Constructed Cross Platform Tools: Do you know how activities can be handled across various domains? As normal, hybrid clouds are not industry. When they do not multi-task, several administrators run amuck. In a hybrid world, poorly specified or implemented cross-platform management are major pitfalls that must be avoided.

Possible solutions:

Define whether it is necessary to run your company with specialized tools or a suite of tools. What is needed for the job to be done? Determine if you need:

i.Tools for cloud application migration for interoperability and transferring apps between private and private applications

ii.Clouds in public. Be sure to have tools for cloud monitoring that fit a virtualized environment.

iii.In order to maintain access and protection necessary for dynamic cloud provisioning and VM movement, cloud automation tools.

3.3.17.Disgruntled or Malicious Employees: The most malicious attacks can be right under our noses sometimes. Not all staff and insiders are reliable. Customers or confidential data can be used by certain insiders to interrupt business activities.

Possible solutions:

i. Managers of the Content Protection Policy (CSP) must provide robust security controls that can track the activities of employee networks to prevent this kind of malicious fallout.

ii.Establish an insider threat program with tactics clearly identified.

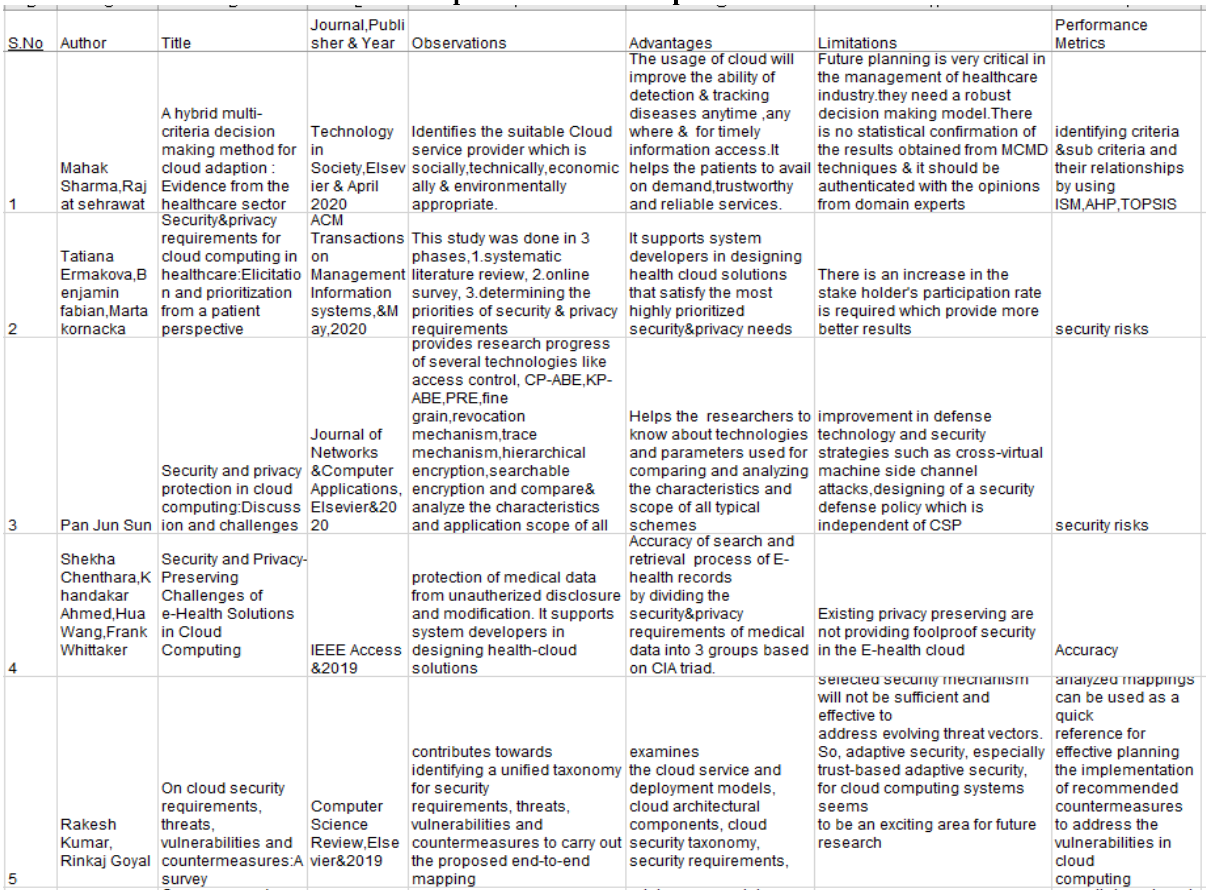
iii.Never trust - Always search. Stop any unauthorized attempt at entry.

iv.Implement a strict protection policy for passwords.

v.Limit access to the vital assets of the organisation.

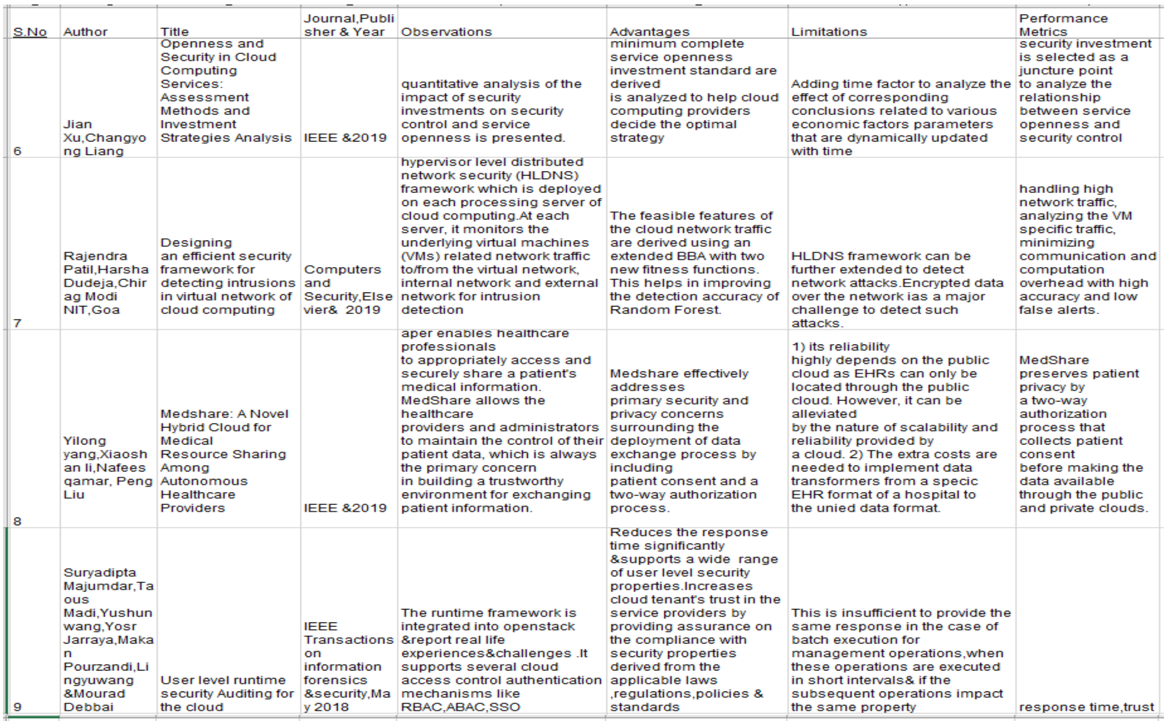
vi.Develop protocols for instant response that recognize and respond to any suspicious or malicious

Table 1. Comparision of various performance metrics

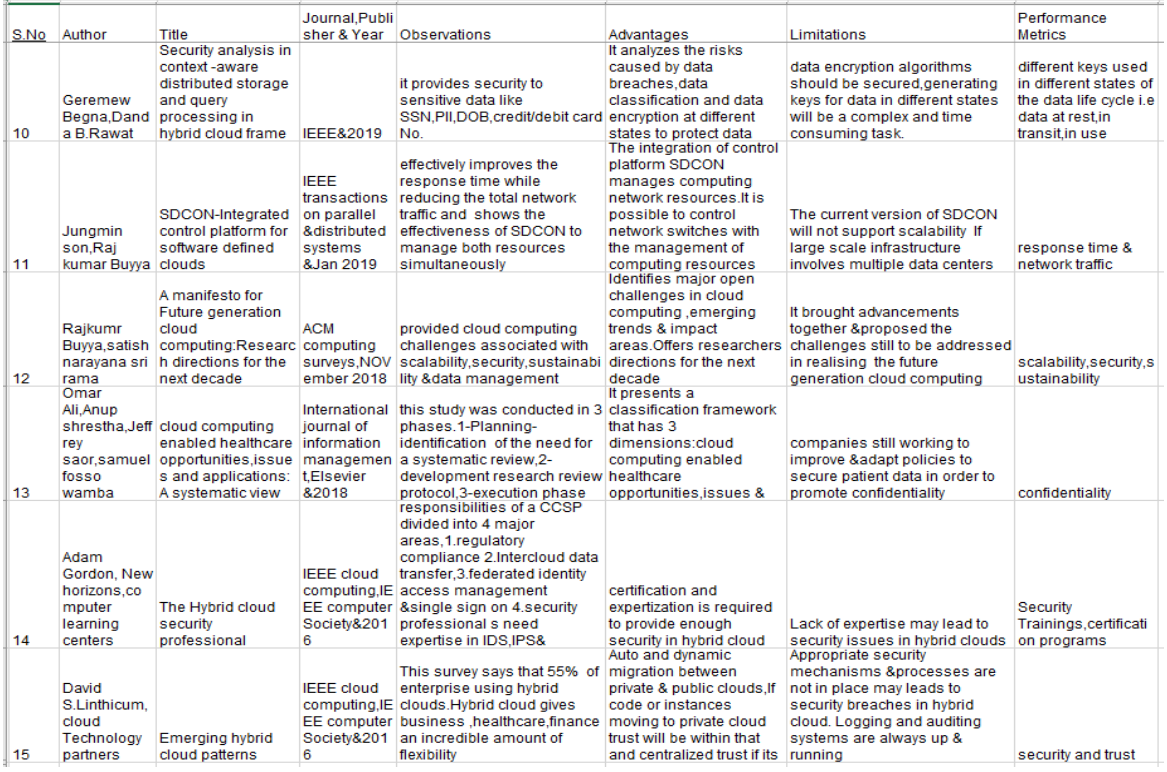


S.No	Author	Title	Journal,Publisher & Year	Observations	Advantages	Limitations	Performance Metrics
1	Mahak Sharma,Rajat sehrawat	A hybrid multi-criteria decision making method for cloud adaption : Evidence from the healthcare sector	Technology in Society,Elsevier & April 2020	Identifies the suitable Cloud service provider which is socially,technically,economically & environmentally appropriate.	The usage of cloud will improve the ability of detection & tracking diseases anytime ,any where & for timely information access.It helps the patients to avail on demand,trustworthy and reliable services.	Future planning is very critical in the management of healthcare industry.they need a robust decision making model.There is no statistical confirmation of the results obtained from MCMD techniques & it should be authenticated with the opinions from domain experts	identifying criteria &sub criteria and their relationships by using ISM,AHP,TOPSIS
2	Tatiana Ermakova,Benjamin fabian,Marta kornacka	Security&privacy requirements for cloud computing in healthcare:Elicitation and prioritization from a patient perspective	ACM Transactions on Management Information systems,&May,2020	This study was done in 3 phases,1.systematic literature review, 2.online survey, 3.determining the priorities of security & privacy requirements	It supports system developers in designing health cloud solutions that satisfy the most highly prioritized security&privacy needs	There is an increase in the stake holder's participation rate is required which provide more better results	security risks
3	Pan Jun Sun	Security and privacy protection in cloud computing:Discussion and challenges	Journal of Networks &Computer Applications, Elsevier&2020	provides research progress of several technologies like access control, CP-ABE,KP-ABE,PRE,fine grain,revocation mechanism,trace mechanism,hierarchical encryption,searchable encryption and compare& analyze the characteristics and application scope of all	Helps the researchers to know about technologies and parameters used for comparing and analyzing the characteristics and scope of all typical schemes	improvement in defense technology and security strategies such as cross-virtual machine side channel attacks,designing of a security defense policy which is independent of CSP	security risks
4	Shekha Chenthara,Khandakar Ahmed,Hua Wang,Frank Whittaker	Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing	IEEE Access &2019	protection of medical data from unautherized disclosure and modification. It supports system developers in designing health-cloud solutions	Accuracy of search and retrieval process of E-health records by dividing the security&privacy requirements of medical data into 3 groups based on CIA triad.	Existing privacy preserving are not providing foolproof security in the E-health cloud	Accuracy
5	Rakesh Kumar, Rinkaj Goyal	On cloud security requirements, threats, vulnerabilities and countermeasures:A survey	Computer Science Review,Elsevier&2019	contributes towards identifying a unified taxonomy for security requirements, threats, vulnerabilities and countermeasures to carry out the proposed end-to-end mapping	examines the cloud service and deployment models, cloud architectural components, cloud security taxonomy, security requirements,	selected security mechanism will not be sufficient and effective to address evolving threat vectors. So, adaptive security, especially trust-based adaptive security, for cloud computing systems seems to be an exciting area for future research	analyzed mappings can be used as a quick reference for effective planning the implementation of recommended countermeasures to address the vulnerabilities in cloud computing

Table 1. Comparision of various performance metrics continuation..



S.No	Author	Title	Journal,Publisher & Year	Observations	Advantages	Limitations	Performance Metrics
6	Jian Xu,Changyong Liang	Openness and Security in Cloud Computing Services: Assessment Methods and Investment Strategies Analysis	IEEE &2019	quantitative analysis of the impact of security investments on security control and service openness is presented.	minimum complete service openness investment standard are derived is analyzed to help cloud computing providers decide the optimal strategy	Adding time factor to analyze the effect of corresponding conclusions related to various economic factors parameters that are dynamically updated with time	security investment is selected as a juncture point to analyze the relationship between service openness and security control
7	Rajendra Patil,Harsha Dudeja,Chirag Modi NIT,Goa	Designing an efficient security framework for detecting intrusions in virtual network of cloud computing	Computers and Security,Elsevier& 2019	hypervisor level distributed network security (HLDNS) framework which is deployed on each processing server of cloud computing.At each server, it monitors the underlying virtual machines (VMs) related network traffic to/from the virtual network, internal network and external network for intrusion detection	The feasible features of the cloud network traffic are derived using an extended BBA with two new fitness functions. This helps in improving the detection accuracy of Random Forest.	HLDNS framework can be further extended to detect network attacks.Encrypted data over the network ias a major challenge to detect such attacks.	handling high network traffic, analyzing the VM specific traffic, minimizing communication and computation overhead with high accuracy and low false alerts.
8	Yilong yang,Xiaoshan li,Nafees qamar, Peng Liu	Medshare: A Novel Hybrid Cloud for Medical Resource Sharing Among Autonomous Healthcare Providers	IEEE &2019	aper enables healthcare professionals to appropriately access and securely share a patient's medical information. MedShare allows the healthcare providers and administrators to maintain the control of their patient data, which is always the primary concern in building a trustworthy environment for exchanging patient information.	Medshare effectively addresses primary security and privacy concerns surrounding the deployment of data exchange process by including patient consent and a two-way authorization process.	1) its reliability highly depends on the public cloud as EHRs can only be located through the public cloud. However, it can be alleviated by the nature of scalability and reliability provided by a cloud. 2) The extra costs are needed to implement data transformers from a specic EHR format of a hospital to the unied data format.	MedShare preserves patient privacy by a two-way authorization process that collects patient consent before making the data available through the public and private clouds.
9	Suryadipta Majumdar,Taous Madi,Yushunwang,Yosr Jarraya,Makan Pourzandi,Lingyuwang &Mourad Debbai	User level runtime security Auditing for the cloud	IEEE Transactions on information forensics &security,May 2018	The runtime framework is integrated into openstack &report real life experiences&challenges .It supports several cloud access control authentication mechanisms like RBAC,ABAC,SSO	Reduces the response time significantly &supports a wide range of user level security properties.Increases cloud tenant's trust in the service providers by providing assurance on the compliance with security properties derived from the applicable laws ,regulations,policies & standards	This is insufficient to provide the same response in the case of batch execution for management operations,when these operations are executed in short intervals& if the subsequent operations impact the same property	response time,trust



S.No	Author	Title	Journal,Publisher & Year	Observations	Advantages	Limitations	Performance Metrics
10	Geremew Begna,Danda B.Rawat	Security analysis in context -aware distributed storage and query processing in hybrid cloud frame	IEEE&2019	it provides security to sensitive data like SSN,PII,DOB,credit/debit card No.	It analyzes the risks caused by data breaches,data classification and data encryption at different states to protect data	data encryption algorithms should be secured,generating keys for data in different states will be a complex and time consuming task.	different keys used in different states of the data life cycle i.e data at rest,in transit,in use
11	Jungmin son,Raj kumar Buyya	SDCON-Integrated control platform for software defined clouds	IEEE transactions on parallel &distributed systems &Jan 2019	effectively improves the response time while reducing the total network traffic and shows the effectiveness of SDCON to manage both resources simultaneously	The integration of control platform SDCON manages computing network resources.It is possible to control network switches with the management of computing resources	The current version of SDCON will not support scalability If large scale infrastructure involves multiple data centers	response time & network traffic
12	Rajkumr Buyya,satish narayana sri rama	A manifesto for Future generation cloud computing:Research directions for the next decade	ACM computing surveys,NOVember 2018	provided cloud computing challenges associated with scalability,security,sustainability &data management	Identifies major open challenges in cloud computing ,emerging trends & impact areas.Offers researchers directions for the next decade	It brought advancements together &proposed the challenges still to be addressed in realising the future generation cloud computing	scalability,security,sustainability
13	Omar Ali,Anup shrestha,Jeffrey saor,samuel fosso wamba	cloud computing enabled healthcare opportunities,issues and applications: A systematic view	International journal of information management,Elsevier &2018	this study was conducted in 3 phases.1-Planning-identification of the need for a systematic review,2-development research review protocol,3-execution phase	It presents a classification framework that has 3 dimensions:cloud computing enabled healthcare opportunities,issues &	companies still working to improve &adapt policies to secure patient data in order to promote confidentiality	confidentiality
14	Adam Gordon, New horizons,computer learning centers	The Hybrid cloud security professional	IEEE cloud computing,IEEE computer Society&2016	responsibilities of a CCSP divided into 4 major areas,1.regulatory compliance 2.Intercloud data transfer,3.federated identity access management &single sign on 4.security professional s need expertise in IDS,IPS&	certification and expertization is required to provide enough security in hybrid cloud	Lack of expertise may lead to security issues in hybrid clouds	Security Trainings,certification programs
15	David S.Linthicum, cloud Technology partners	Emerging hybrid cloud patterns	IEEE cloud computing,IEEE computer Society&2016	This survey says that 55% of enterprise using hybrid clouds.Hybrid cloud gives business ,healthcare,finance an incredible amount of flexibility	Auto and dynamic migration between private & public clouds,If code or instances moving to private cloud trust will be within that and centralized trust if its	Appropriate security mechanisms &processes are not in place may leads to security breaches in hybrid cloud. Logging and auditing systems are always up & running	security and trust

4.Conclusion

The cloud computing is a springing trend adopted by most of the organizations.as it is having many advantages along with few disadvantages. This paper contributes towards the research expostulations and solutions that helps to fix the security issues occurred while storing and maintaining the data in the hybrid cloud.

References

1. Mahak Sharma, Rajat sehrawat,” A hybrid multi-criteria decision making method for cloud adaption : Evidence from the healthcare sector”in Technology in Society & 23 April 2020, 0160-791X/©2020 Elsevier Ltd.

2. Tatiana Ermakova,Benjamin fabian,Marta kornacka,” Security privacy requirements for cloud computing in healthcare: Elicitation and prioritization from a patient perspective "in ACM Transactions on Management Information Systems, Vol. 11, No. 2, Article 6. Publication date: May 2020.
3. Pan Jun Sun,” Security and privacy protection in cloud computing: Discussion and challenges” in Journal of Network and Computer Applications, 2020 Published by Elsevier Ltd.
4. Shekha Chenthara,Khandakar Ahmed,Hua Wang,Frank Whittaker,” Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing” in IEEE Access &2019.
5. Rakesh Kumar, Rinkaj Goyal,” On cloud security requirements, threats, vulnerabilities and countermeasures: A survey ”in Computer Science Review &2019, Elsevier.
6. A.Viji Amutha Mary, Mercy Paul Selvan, Christy, Public Auditing for Secure Cloud Storage using MD5 Algorithm, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-3, September 2019.
7. Jian Xu,Changyong Liang,” Openness and Security in Cloud Computing Services: Assessment Methods and Investment Strategies Analysis, IEEE ,2019
8. Rajendra Patil,Harsha Dudeja,Chirag Modi,NIT,Goa,” Designing an efficient security framework for detecting intrusions in virtual network of cloud computing”in Computersand Security,Elsevier, 2019
9. Yilong yang,Xiaoshan li,Nafees qamar,Peng Liu,” Medshare: A Novel Hybrid Cloudfor Medical Resource Sharing Among Autonomous Healthcare Providers” IEEE &2019
10. Suryadipta Majumdar,Taous Madi,Yushun wang,Yosr Jarraya,Makan Pourzandi,Lingyuwang &Mourad Debbai,” User level runtime security Auditing for the cloud”inIEEE Transactions on information forensics &security,May 2018.
11. Geremew Begna,Danda B.Rawat,”Security analysis in context -aware distributed storage and query processing in hybrid cloud frame work” IEEE&2019
12. Jungmin son,Raj kumar Buyya,” SDCON-Integrated control platform for software defined clouds”in IEEE transactions on parallel &distributed systems ,Jan 2019
13. Rajkumar Buyya,satish Narayana sri rama,”A manifesto for generation cloud computing:Research directions for the next decade” in ACM computing surveys, November 2018
14. Omar Ali,Anup Shrestha,Jeffrey saor,Samuel fosso wamba,”cloud computing enabled healthcare opportunities,issues and aaplications:A systematic view” in International journal of information management,Elsevier&2018
15. Adam Gordon,New horizons,computer learning centers,”The Hybrid cloud security professional” in IEEE cloud computing,IEEE computer Society,2016
16. David S.Linthicum,cloud Technology partners, “Emerging hybrid cloud patterns”in IEEE cloud computing,IEEE computer Society,2016
17. Nagarajan, G., Minu, R. I., Vedanarayanan, V., Jebaseelan, S. S., & Vasanth, K. (2015). CIMTEL-mining algorithm for big data in telecommunication. International Journal of Engineering and Technology (IJET), 7(5), 1709-1715.
18. Rajendran, P. K., Muthukumar, B., & Nagarajan, G. (2015). Hybrid intrusion detection system for private cloud: a systematic approach. Procedia Computer Science, 48, 325-329.
19. Sajith, P. J., and G. Nagarajan. "Optimized Intrusion Detection System Using Computational Intelligent Algorithm." In Advances in Electronics, Communication and Computing, pp. 633-639. Springer, Singapore, 2021..
20. Nagarajan, G., R. I. Minu, and A. Jayanthiladevi. "Brain computer interface for smart hardware device." International Journal of RF Technologies 10, no. 3-4 (2019): 131-139.