Jagannath University Research Journal (JURJ) Volume No.-II, Issue No.–II, November, 2021, ISSN: 2582-6263

Cloud Computing Security Issues and Risk Assessment – A Review

Ashmeet Kaur Duggal[a],Dr. MeenuDave[b]

[a]ashmeet04@yahoo.co.in, Jagannath University, Jaipur, India
[b]meenu.s.dave@gmail.comJagannath University, Jaipur, India

Abstract: Cloud Computing is a technology aiming to share storage, computation, and various other services transparently among massive users. Organizations use Cloud Computing technology in various service models (SaaS, PaaS, IaaS) and deployment models (Private, Public, Hybrid). Nowadays, Cloud computing security is a significant research area with many constraints, ranging from protecting the hardware and platform technologies to protecting cloud data and resource access (through different end-user devices). Although cloud computing has various advantages, security and privacy concerns have always been the priority of cloud customers and an impediment to its widespread adoption by businesses and organizations. The paper presents a systematic review in cloud computing focusing on identifying the security issues/risks involved, risk assessment, and exploring techniques for protecting users' data from attackers in the cloud. It would help future researchers and cloud users/business organizations to overview the risk factors in a cloud environment. Moreover, to pro-actively map their indigenous needs with this technology.

Keywords: Cloud Computing, Cloud Security Issues, Risk Assessment.

I. INTRODUCTION

Cloud computing is a computing technology that has gained considerable attention in the scientific community and other communities. It represents a model to enable convenient, on-demand network access to a shared pool of configurable computing resources that can be provisioned swiftly and can be made available with minimal management effort [1]. This definition explains cloud computing as having five characteristics, i.e., on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. It provides various on-demand shared resources to customers like software, storage, information, or data. Cloud Computing is a computing platform to share resources that include infrastructures, software, applications, and business processes. Alternatively, in other words, it is a virtual pool of computing resources. It provides computing resources in the collection for users through the internet.

Figure 1 Network of Cloud

Although there are optimal benefits of adopting cloud computing, there are also significant barriers to adoption. One of the most significant barriers during the model's adoption is security [2]. Since cloud computing represents a relatively new computing standard; therefore, its security is the most crucial concern from the customer's perspective and Cloud Service Provider (CSP). Migrating critical applications and sensitive data to the cloud environment is a significant concern for organizations moving beyond their data centers. To alleviate these concerns, a CSP must ensure that customers will continue to have the same privacy and security controls over their applications and services and also provide evidence that their organization is secure and can meet their service level agreements [3]. We are in an era in which information protection is the goal of every organization. The speedy growth of cloud computing has brought many security challenges for users and providers.

Moreover, the risk of attack on personal and organizational data stored in cloud storage by an attacker is high as such computer experts are using many techniques for protecting users" data from an unauthorized party. This paper helps us understand the security issues of cloud computing, which affect the confidentiality and vulnerability of the system. It introduces Cloud Computing, the benefits of cloud computing, brief history/evolution of cloud computing, and explores the deployment models and the service delivery models. It also specifies the risks associated with cloud computing and suggests various security measures to overcome the problem.

1.1 Benefits of Cloud Computing

Before, people used to run applications or programs from software downloaded on a physical computer or server in their organization. Cloud computing's simplified process is based on the Internet, allowing people to access the same application [1]. However, why so many organizations are moving to the Cloud? The reason may be the following:-

(1) Flexibility: For every business organization, the aims are to have more customers. Nowadays, as customer reach to access organization applications increases, every business works online. The quantity of data that an application handles increases day by day, and so is the CPU processing power. The organization needs significant bandwidth; a cloud-based service can instantly meet the demand because of the vast capacity of the services of remote servers.

(2) Disaster Recovery: Disaster recovery plans are no longer required when an organization starts relying on cloud-based services. Cloud computing providers handle most of the issues, and they do it faster. Aberdeen Group found that businesses that used Cloud could resolve issues four times more quickly than those not using Cloud [4].

(3)Automatic Software Update: In 2010, UK companies spent 18 working days per month managing on-site security alone [4]. However, today with Cloud computing, the providers do the server maintenance, including security updates quickly, freeing up their customers' time and resources for another task.

(4) Work From Anywhere: Till the time, there is internet access, customers, and organization employee can access their information anywhere. Also, since documents are stored directly onto the Cloud, anyone with authorized access can access the documents and work on the same project simultaneously, avoiding time lost and documents with several untraceable versions.

(5) Favouring the Environment: For smooth operations, more servers are required by many small to corporate size companies. Server utilization rates are about 5-10%, whereas cloud utilization rates are in the 70% range. This is because cloud computing eliminates in-house servers; there is no need for the constant climate control involved in maintaining servers and eliminating carbon footprints.

(6) Security:Many laptops with vital information are reported lost or stolen. The outcome of this can be some profound monetary implications. However, data can still be accessed irrespective of the machine when everything is secure on Cloud.

1.2 Evolution of Cloud Computing

In 1960, John McCarthy stated that computing services could also be sold like water and electricity. Furthermore, in 1999, the Salesforce Company started distributing the applications to the customers through a convenient website [3]. Amazon started Amazon Web Services in 2002, and they were providing Computation and storage services. In around 2009, big companies like Microsoft, Google, HP, and Oracle started providing cloud computing services [4]. Nowadays, every person uses cloud computing services in their daily life, such as Google Photos, Google Drive, and iCloud. Cloud computing services will become the basic need of IT industries in the future.

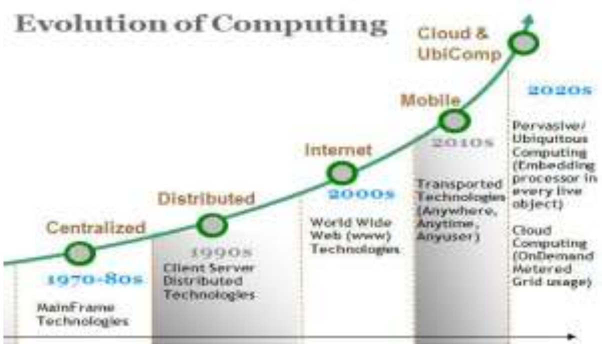
Evolution of Computing
Cloud & UbiComp
2020s
Pervasive/ Ubiquitous Computing (Embedding processor in every live object)
Cloud Computing (OnDemand Metered Grid usage)
Mobile
2010s
Transported Technologies (Anywhere, Anytime, Anyuser)
Internet
2000s
World Wide Web (www) Technologies
Distributed
1990s
Client Server Distributed Technologies
Centralized
1970-80s
MainFrame Technologies

Figure 2 Evolution of Cloud Computing

II. TYPES OF CLOUD COMPUTING

Cloud computing is usually classified in two ways: The location of cloud computing and the type of services offered.

2.1 Based on Location of the Cloud [5]

Public Cloud: In Public Cloud, the Cloud vendor hosts all the computing infrastructure at his premises. The customer does not have any visibility and control over the location of the computing infrastructure. Different cloud customers can share computing infrastructure.

Private Cloud: The computing infrastructure is allocated to an organization, and resource sharing with other organizations is not allowed. Compared with Public Clouds, Private clouds are more expensive and more secure.

Hybrid Cloud: Organizations can histcritical applications on private clouds, and applications with relatively fewer security concerns can be placed on a Public Cloud. The combination of both private and public clouds together is called a hybrid Cloud. A related term is Cloud Bursting. Organizations use their computing infrastructure for standard usage in Cloud bursting but access the Cloud for high/peak load requirements, ensuring that they gracefully handle a sudden increase in computing requirements.

2.2 Based upon the Services Offered [5]

Infrastructure as a service (IaaS):IaaS provides essential storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, and data center space are pooled and are made available to handle workloads. The customer would typically deploy his software on the infrastructure. Amazon EC2, Amazon S3, Rack space Cloud Servers, and Flexi scale are a few leading vendors that provide infrastructure as a service.

Platform as a Service (PaaS): Encapsulation of a software layer is done with a development environment and can be offered as a service. Upon this, other higher levels of service can be built. The customer can develop his application freely, which runs on the provider's infrastructure. Typical players in PaaS are Google's Application Engine, Microsoft Azure, Salesforce.com.

Software as a service (SaaS) :It offers the whole application as an "on-demand" service to the customers. The Cloud runs a single thread of the service & multiple end users are serviced. Itdoes not require an upfront investment in servers or software licenses on the customer's side. The costs are lowered for providers since only a single application needs to be hosted & maintained. Examples are Salesforce.com, Gmail from Google and Hotmail from Microsoft, Google docs, and Microsoft's online version of office called BPOS (Business Productivity Online Standard Suite).

III. RISKS ASSOCIATED WITH CLOUD COMPUTING

Security is one of the significant elements that need to be addressed by cloud computing services during the transmission of critical applications and sensitive data to cloud environments. There are four layers based on cloud computing services viz—user Layer, Service Provider layer, Virtualization Layer, and Data Centre layer. Several security issues occupy a cloud environment that obstructs efficient access and transfer of data, thus leading to a threat-prone environment.

Data Access: - There is a need to maintain some cloud standards or security measures to prevent the threat of accessing sensitive information from the cloud. Hackers and malicious intruders are always active, and they can hack confidential data to use it in other ways.

Lack of trust and authentication: - Various cloud providers provide their services at the "pay per use" package. However, they have forgotten to maintain trust between the user and themselves. They do not offer any auditing mechanism for monitoring services and transactions executed by different users on different cloud platforms.

Data Segregation: - The word segregate means isolating a group of people or platforms. Multi-tenancy is one of the significant characteristics of cloud computing, which states that multiple users can store their data at various locations and access services of different layers. It led hackers to inject into the client code of other systems and can steal their data. There must be some boundary between different layers so that the service should separate data from different users in a secure way.

Data Breaching: - The word breach means violation or infraction. In the cloud computing context, it means data lying on different platforms in the cloud environment may violate policies and legal service agreements.

Virtual Machine (VM) Security:-Performing different instances of the same task on a single physical machine is the primary task of virtualization. Current virtual machine monitors (VMM) cannot isolate instances from each other because anyone can log in as guests and access data in the cloud.

VM Sprawl: - An accessible provision of the virtual machines may lead to out-of-control pop-up blockers on various cloud sites. The blockers will allow advertisements on sites simultaneously, which leads to a lack of management and handling of client requests.

VM Stall: - Most of the companies are working on virtualized servers. Nowadays, virtual machines are increasing day by day due to virtualized deployment. The VM Stall occurs due to a lack of trust in administrators and performance management.

Excessive bandwidth problem:-Utilization of services varies from user to user depending on their capacity of accessing services. It may be possible that a single user may consume more than a shareof proper bandwidth depending on its service.

Verification of Identity and signatures:-ID management disassociated with every individual working in a cloud environment, and it is one issue that is still not adopted by various companies. The cloud providers havethe right to check who is utilizing their services and how. In such scenarios, the provisioning of users is of great concern.

Layer	Components	SecurityIssues
End-User or User layer	Cloud applications, programming tools, and environment.	Security as a Service, Browser Security, and User Authentication
Service Provider Layer	Service Level Agreements (SLA) Monitoring, Scheduler and Dispatcher, Load Balancer, Policy Management.	Identity, Infrastructure, Privacy, Audit and Compliance, File sharing, the transmission of data, and Cloud Integrity.
Virtualization layer	Number of VMs(Virtual Machines), number of operating systems, and their monitoring.	VM escape, Infrastructure, Identity, and Access Management.
Data Center Layer	Servers, CPUs, Memory, and Hardware.	Data Storage, Network, and Server.

Table 1 –Security Issues Associated with Cloud Computing [37]

Alternatively, in other words, we can categorize the Cloud computing risks into two categories:

3.1 Risks from Cloud Providers Perspective

3.1.1 Data Security, Data Privacy & Risk Control

Data security and data privacy risks are mitigated through data encryption, and it is the responsibility of CSP to handle these rudimentary risks [6]. To ensure data integrity, data confidentiality, and data availability, the storage provider must offer encryption schema and scheduled data backups [7]. It is the responsibility of CSP to adapt added security measures to ensure the security of the data. These security measures involve encryption techniques for the security of data and fine-grained authorization for controlling user access of the data [8]. Providers are more accountable for the privacy and security of data and application services in the public cloud than in the private Cloud [9]. One major problem with data encryption is the responsibility of key management. Ideally, it is the data owners. However, since the user lacks the expertise to handle the keys, they usually hand over critical management operations to CSP. However, it becomes tedious for CSP to handle critical management operations for a growing number of users [10, 11]. CSP is responsible for data security while it is being processed, transferred, and stored [12]. CSP does not have permission for access to the physical security system of data centers. The CSP can only handle the security settings remotely and is unaware of whether they are implemented or not. If the security settings fail to implement completely, it becomes a significant security risk for CSP[13].

- **Identity and Access Management (IAM)**

It improves operational efficiency regulatory compliance by managing the major security concerns, automated provisioning, authentication, and authorization services. This issue was solved using various techniques such as single sign-on, federated identity, access control list, Directory-based service, access based on attributes [21]. The CSP should offer strict access control mechanism to avoid unauthorized access. In the Cloud computing model, administrative access is provided through the internet, which increases the risk of unauthorized access to data and other resources. Hence, it is important to control and monitor administrative access [7]. Data in the Cloud is distributed to the cloud user, bringing jurisdiction and privacy [11]. As per a study, 37% of cloud providers were sure about security for user authentication before granting access,whereas only 50% of cloud users considered IAM the cloud provider's responsibility. Therefore, achieving compliance requirements could prove to be problematic[15].According to [14], when data is outsourced to a cloud, it is critical to enforce reliable and secure data access between several users. The user cannot even trust a server because the user's private data can be exposed in case of server compromise. Encrypting data differently and disclosing the corresponding decryption keys only to authorized users can be a solution. However, this approach compromises performance as well as scalability [16].

- **Multi-tenancy**

It is an essential attribute of cloud computing as itincreases the use of underlying hardware resources and allows for efficient resource provisioning. Multi-tenancy security and privacy are critical challenges for the Public Cloud [16]. The CSP may store the customers' personal and financial data, and therefore, CSP is responsible for customers' data security. Some service providers use job scheduling and resource management techniques, but most providers use virtualization to maximize the use of hardware [18].These two methods/techniques allow attackers to have full access to the hostand cross-VM side-channel attacks through which the attackers can extract information from a target VM on the same machine. In multi-tenancy, data from multiple tenants are likely to be stored in the same database; the risk of data leakage between them is high [12]. Data is kept in a shared environment with the data from other customers, which poses considerable risk of multi-tenancy for CSP. A mechanism is needed through which CSP must guarantee data isolation between clients, and they should be liable for ensuring this isolation [19].

- **Data Availability and Backup**

It is challenging for CSP to guarantee adequate availability and backup of data because the data are hosted distantly in the cloud. Therefore, it is challenging to back up data and recover data in case of failure [18]. Several areas will threaten the data available in the cloud environment, including the availability of cloud computing services; whether the CSP would continue to operating in the future? Whether the cloud storage services provide backup? [10]

3.1.2 Organizational Risks

Organizational risks are categorized as the risks that may impact the organization's structure as an entity. It may include the loss of business reputation, failure, or termination of the acquisition [28].

- **Organizational Change**

Management Resistance to change from organizational politics changes to people's work is a significant corporate risk. To mitigate this, use insight from administrative change management and involve key stakeholders in the adoption procedure [21].

- **Resource Planning**

As perHosseini et al. [21], the risk of resource planning is losing control over resources, leading to ambiguous roles and responsibilities. So to overcome this, it is essential to clarify roles and responsibilities before cloud adoption.

- **Organizational Security Management**

The existing security management models have greatly changed when enterprises adopt the cloud. It is required to re-evaluate the current security models and develop security standards to ensure the deployment and adoption of secure clouds [9].

3.1.3 Technical Risks

Technical risks are the failures associated with the technologies and services provided by the CSP (Customer Service Provider), including resource sharing isolation problems malicious attacks on the CSP risks related to portability and interoperability [20]. These risks are related to hardware, including poor hardware maintenance, unresponsive system, reduction in availability, and hardware failure [6].

- **Portability in the Cloud**

Interoperability between clouds is due to incompatibilities betweens platforms. The solution is to use cloud middleware to ease cloud interoperability [21].

- **Application Development**

The risk of service interruption at the provider's side results inexpensive outages, unavailability of services, or data loss. The solution offered by the authors is to use multiple CSPs and monitor applications from outside the Cloud [21].

- **Lack of Interoperability**

Standards Cloud computing lacks interoperability standards. Standard of communication and data export format does not exist between and within CSP, making it difficult to establish appropriate security frameworks [18]. For CSP, universal standards are also recommended to ensure interoperability among CSP[7].

3.1.4 Compliance and Audit Risks

These risks are related to lack of jurisdiction information, changes in the jurisdiction, illegal clauses in the contract, and ongoing legal disputes. CSP and customers are responsible for abiding by the rules and regulations defined in audit SLAs and the contract on a regular basis[22]. Traditional service provider is subjected to external audits and security certifications. If a CSP fails to adhere to these security audits, it displays a reduction in customers' trust [23]. CSP should define security policies with recovery methods in case of disasters. Also, the ability to restore data entirely in a pre-established amount of time [19].

3.1.5 Physical Security

- **Data Location and Data Centre**

CSP should guarantee a secure operation of the cloud data centre to provide a secure physical location for customers' data [24]. CSP manages the infrastructure, including servers, networks, storage devices. CSP should implement and operate appropriate infrastructure controls, including staff training, physical location security, and network firewalls. Overcoming these risks is of great significance because if the physical access control is weak, hackers can steal entire servers, despite being protected by firewalls and Encryption[24]. The cloud provider has the responsibility to store and process data in specific jurisdictions, and also, it should be responsible for obeying the privacy regulations of those jurisdictions [25].

3.2 Risks from Cloud Customer Perspective

3.2.1 Data Security, Data Privacy & Risk Control

- **User Access**

The customer is fully responsible for managing all software security controls. These include application access control, software patching, IAM, and virus protection [24]. One significant risk is how a customer faces the privileged status of CSP and security issues such as fault elimination, data damage, and migration [26].

- **Data Privacy and Security**

It is a crucial security concern for the end-users to know about the privacy and protection of their data from CSP to ensure data privacy is not compromised. However, eventually, the customers are responsible for the security and integrity of their data even it resides on the provider's premises[15]. The loss of encryption key or free access code will cause a severe problem for cloud service users [35]. Accordingly, a lack of cryptographic management information will slowly lead to sensitive damages like data loss and unexpected user data leakage to the outside world. Customer data and commercial secrets should not be leaked while residing on CSP premises [24]. According to the CSA group [30], the burden of avoiding data loss does not fall entirely on the provider's shoulder. The data will be lost if a customer encrypts data before placing it in the cloud and loses the encryption key.

- **Data Segregation**

Cloud customers are responsible for determining the techniques used by the provider to segregate the data. It must ensure that encryption schemes are deployed and sufficient to provide security [29]. We cannot assume Encryptions a single solution for data segregation problems since encryption accidents may destroy the data [23].

- **Data Availability**

When the client's data is uploaded into the cloud, clients lose control over the data on the cloud. If customers' data and information on the cloud are either lost or hacked, it is difficult to retrieve the original data[31].

- **Secure Data Deletion**

Appropriate, error-free, and timely data deletion may be impossible and undesirable. One of the reasons is that the extra copies of data reside at various locations, and the other reason is that the disk to be destroyed also contains data from other clients [19]. Data is supposed to be obliterated when it is no longer required. However, due to the physical characteristics of the storage medium, the deletion of the data may still exist and can be restored. It may cause a risk of sensitive data disclosure to the customer [11].

3.2.2 Technical Risks

- **Infrastructure Capabilities**

It is challenging to show CSP that their cloud performance is not following their agreed SLA because of the server's workload and the variable nature of the network. It causes disputes and litigation. A simple solution is to evaluate the cloud performance under appropriate investigation before adopting it. Another solution is to use third-party monitoring tools to verify system performance [21].

- **Application Development**

The objective is to allow developers to develop their applications over the provided platform. Hence, the customers are mainly responsible for protecting their developed applications and the platform. Momentarily, the providers isolate the customer's applications and development environments [9].

- **Portability**

As per K. Popovic and Z. Hocenski [32], the risk of compatibility occurs if the customer wants to change the provider because the storage services offered by one CSP may be incompatible with another provider's service.

3.2.3 Compliance and Audit Risks

- **Disaster Recovery**

Cloud Customers should know what will happen to their data if a disaster occurs. Therefore, the customer's primary security responsibility is to ask whether the provider will recover the data thoroughly and how long it will take. [29]

- **Legal Challenges**

Cloud Service Provider is more susceptible to legal and regulatory concerns and commits to keeping and processing customers' data in specific jurisdictions that provide security and data privacy as promised in their SLAs. Even then, the organizations are primarily responsible for protecting their data stored at the CSP site [33]. The computer processing power or the storage one buys via a Cloud service may be in another country or divided between multiple countries. Despite cost and efficiency advantages, it raises legal issues by exporting customers' data abroad [27][36].

3.2.4 Physical Security

- **Data Location**

CSP stores data in multiple physical locations redundantly, and the customer is unaware of the location. Therefore, it isoften difficult to determine whether appropriate security measures are in placeto secure customer data on the customer's side [21]. The customer cannotcontrol the cloud computing environment's downtime, i.e., when the CSP machines are not accessible or are going through updates. This situation brings immense discouragement to the confidence of customers [34].

IV. DISCUSSION AND ANALYSIS

In Table 2, we suggest the probable security measures that help mitigate the identified risks to some extent. (CP) represents the risks related to cloud providers, whereas (CC) is related to the cloud customers.

Table 2–Risks and Suggested Security Measures

S.No.	Category	Risks	Security Measures
1.	**Data Security & Privacy**	Ensuring customer's data availability in the cloud (CP).	CSP took specific security measures to prevent outages and cyber attacks.
		Risks in relation to data security and privacy (CP), (CC)	• To mitigate these risks is using APIs to implement robust access control, implementing encryption to protect data traffic. • Analyze that data is protected while designing, as during runtime. • Provide effective mechanisms for key generation, storage, and data destruction.
		Avoiding unauthorized access to customer's data in the cloud (CP), (CC)	Can be resolved by successfully implementing management, authentication, and authorization techniques on customer and provider's end.
		Risks related to the multi-tenancy (CP)	CSP should adopt effective encryption methods to guarantee data isolation between clients.
		Risks related to data deletion (CP)	The provider should define policies to set up procedures to destroy persistent media before throwing it out.
2.	**Technology**	Lack of standard	It should be mentioned in the

		technology in the cloud computing environment (CC)	initial contract if the cloud service provider uses the standardized technology, and the end-user must ensure that.
		Compatibility issue between cloud and IT systems at customer's end (CC)	The solution is to implement a hybrid cloud, which can handle many of these compatibility issues.
3.	Organizational	Risks related to Planning Resources, Change Management (CC)	Involves stakeholders in cloud adoption procedures
		Risks involved in security management (CC)	Re-evaluation of existing security standards before adopting cloud.
4.	Physical Security	The physical security of a cloud service provider's data centers are composed of servers, data storage, and network devices (CP)	Cloud providers must implement certain policies and procedures in place to prevent physical security breaches; these include physical location security like alarms, CCTV cameras, etc.
5.	Compliance	Enforce regulatory obligations in a cloud environment. (CP)	• CSP must abide by all the defined regulations within a country in regard to cloud security. These regulations include HIPPA, and FISMA • CSP has to contend with the Legal Systems under various Jurisdictions with not so much clarity as to where the data is stored and how it travels by passing through contrasting Legal Jurisdictions.
		Business Continuity and Disaster Recovery (CP)	Recommends data redundancy across multiple infrastructures to avoid vulnerabilities in the event of a major failure

V. PROPOSED SOLUTION

- Cloud providers should address information security and privacy risks associated with deploying information into any cloud computing environment.

- Cloud providers should ensure that data in the cloud environment is tamper-proof protected through encryption at the kernel level. Communication between the customer and the provider's server is secure, thus avoiding the risk of any man-in-the-middle attacks to gain access to the encryption keys.

- Cloud providers should use industry-standard encryption to make data unreadable and unusable to those without the encryption key. Rendering the information useless, dramatically reduces the risks associated with data theft, exposure to unauthorized parties, or data seizure through a judicial subpoena.

- Providers should provide a unique policy-based approach to key management and data access, allowing users to determine which server gets access to secure data.

VI. CONCLUSION

Upcoming security challenges need to be addressed as individuals, government, non-governmental organizations, and small and large-scale enterprises plan to deploy their data and other applications in private, community, and public cloud environments. Encrypting sensitive data used by cloud-based virtual machines centralized key management allows the user (and not the cloud provider) to control cloud data and ensure that cloud data is accessible according to established enterprise policies. Optimal cloud security practices should include these policies to provide better and optimal security parameters. This paper discusses the benefit of using cloud computing, its evolution, the risk and challenges of this technology, and emerging threats, which attack the confidentiality and vulnerability of the information in the cloud. In the end, a viable solution for information security in private, public, and community cloud services was proposed.

VII. REFERENCES

[1]. Rebollo, O., Mellado, D (2012) Systematic Review of Information Security Governance Frameworks in the Cloud Computing. Journal of Universal Computer Sc. 18(6), 798–815.

[2]. Monjur Ahmed, Mohammad Ashraf Hossain (2014). Cloud Computing & Security Issues In The Cloud. Intern. Journal of Network Security & its Applications (IJNSA).

[3].Gururaj. R. et al (2017). A Comprehensive survey on Security in Cloud Computer. The 3rd International Workshop on Cyber security & digital investigation.

[4]. Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez (2013), An analysis of the security issues for cloud computing, Journal of Internet Services & Application.

[5]. AshmeetkaurDuggal, Dr.Meenudave (2018). Improving File Accessing Efficiency and Cloud Storage Performance – A Review. 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT).

[6].Djemame, K., Armstrong, D.(2011). Risk Assessment Framework & Software Toolkit for Cloud Service Ecosystems. In: Int. Conference on Cloud Computing, GRIDs, and Virtualization.

[7]. Harauz, J., Kauifman, M., Potter, B. (2009). Data Security in world of cloud computing. IEEE Security and Privacy 7(4), 61–64.

[8]. Kavitha, V, Subashini, S. (2011). A survey on the security issues in service delivery model of cloud computing. Journal of Network & Computer Applications 34(1), 1–11

[9]. Takabi, H., Joshi, J.B.D. (2010). Security & Privacy Challenges in Cloud Computing Environments. Published. IEEE Security and Privacy 8(6), 24–31.

[10]. Chen, D., Zhao, H. (2012). Data Security & Privacy Protection Issues in Cloud Computing. In: Int. Conference on Computer Science & Electronics Engineering, pp. 647–651.

[11]. Rahul, S.S., Rai, J.K.(2013) Security & Privacy Issues In Cloud Computing. International Journal of Eng. Research and Technology (IJERT) 2(3).

[12]. Hashizume, K., Rosado, D.G., Medina, E.F., Fernandez, E. (2013). An analysis of the security issues for cloud computing. Journal of Internet Services & Applications 4(5).

[13]. Reddy, V.K., Thirumala, R.B., Reddy, L.S.S., Kiran, S. (2011). Research Issues in Cloud Computing. Global Journal of Computer Science & Technology 11(11).

[14]. Srivastava, P., Pal, D., Krishna, R., Kumar, S. (2012). A Novel Open Security Framework for the Cloud Computing. International Journal of Cloud Computing & Services Science 1(2).

[15]. Basu et al. (2019). Cloud computing security challenges & solutions-A survey. Ieeexplore.ieee.org.

[16]. Ren, K., Wang, C., Wang, Q. (2012). Security Challenges for the Public Cloud. Journal of Internet Computing IEEE 16(1).

[17]. NH Hussein, A Khalid (2016). A survey of cloud computing security challenges & solutions. International Journal of Computer Science & Information Security,researchgate.net.

[18]. Pearson, S., Benameur, A. (2010). Privacy, Security & Trust Issues Arising from Cloud Computing. 2nd International Conference on Cloud Computing Technology and Science.

[19]. Vargas, Ayala, L.C., Vega, M., L.M. (2013). Emerging Threats, Risk & Attacks in Distributed Systems: Cloud Computing. Elleithy, K., Sobh, T. (eds.) Innovations & Advances in Computer, Information, Systems Sciences, & Engineering. LNEE, pp. 37–52. Springer, Heidelberg.

[20]. Rana, S., Joshi, P.K. (2012). Risk Analysis in Web Apps. by Using Cloud Computing. International Journal of Multidisciplinary Research 2.

[21]. Sommerville, I., Khajeh- Hosseini, A., Bogaerts, J., Teregowda, P. (2011). Decision Support Tools for Cloud Migration in Enterprises. IEEE CLOUD.

[22]. Hou, Y., Oetting, J. (2011). Risk Assessment for Cloud-Based IT Systems. International Journal of Grid & High Performance Computing, 1–13.

[23]. Kumar, V., Swetha, M.S. (2012). Cloud Computing: Towards the Case Study of Data Security Mechanisms. International Journal of Adv. Tech. and Engineering Research 2(4).

[24]. Julisch, K., Hall, M. (2010). Security and Control in the Cloud. Information Security Journal: A Global Perspective, 299–309.

[25]. Yu, Y., Miyaji, A., Au, M. and Susilo, W. (2017). Cloud computing security & privacy: Standards & regulations, Elsevier.

[26]. Che, J., Duan, Y., Zhang, T. (2011). Study on the Security Models & strategies of Cloud Computing. International Conference on Power Electronics and Engineering App.

[27]. Prasad, M., Naik, R., Bapuji, V. (2013). Cloud Computing: Research Issues and Implications. International Journal of Cloud Computing & Services Science 2(2), 134–140.

[28]. Dahbur, K., Mohammad, B. (2011). A Survey of Risks, Threats & Vulnerabilities in Cloud Computing. International Conference on Intelligent Semantic Web-Services & Applications.

[29]. Bisong, A., Rahman, S.M. (2011). An Overview of Security Concerns in Enterprise Cloud Computing. International Journal of the Network Security & its Applications 3(1).

[30]. Ramachandran, M. (2015). Software security requirement mgmt as an emerging cloud computing service. International Journal of Information Mgmt., 36(4), pp 580-590.

[31]. Ahmad, T., Amanul, Al-Nafjan, H.M., M., Ansari, A. (2013). Development of Cloud Computing and Security Issues. Information. and Knowledge Management 3(1), http://www.iiste.org.

[32]. Popović, K., Hocenski, Ž. (2010). Cloud computing security issues and challenges. MIPRO.

[33]. Jansen, W., Grance, T. (2011). Guidelines on Security & Privacy in Cloud Computing. NIST.

[34].Ahmed Alrehaili, Aabid Mir, Mir Junaid (2020). A Retrospective of Prominent Cloud Security Algorithms. International Journal of Innovative Technology & Exploring Engineering, 9(3), 2275-3075.

[35]. Lee, K. (2012). Security Threats in Cloud Computing Environments. International Journal of Security & Applications 6(4).

[36]. Sharma, M., Bansal, H., Sharma, A.K. (2012). Cloud Computing: Different Approach and Security Challenges. Intern. Journal of Soft Computing & Engineering 2(1).

[37]. Peter Mell , Timothy Grance (2011). The NIST Definition of Cloud Computing. NIST Special Publication 800-145.

AUTHOR’S BIOGRAPHY

Ashmeet Kaur Duggal received her Master of Computer Application Degree from Guru Gobind Singh Indraprastha University, India, in 2010. Presently the author is working as an Assistant Professor (IT Department) in Sri Guru Tegh Bahadur Institute of Management & IT since 2011 and has ten years of Teaching Experience. The author has publications under her name in various renowned journals and International Conferences. Her research interests include Cloud Computing, its efficiency, storage, security and Load balancing Policies. Currently, the author is pursuing Ph. D. in Computer Science from Jagannath University, Jaipur, India.