CLOUD COMPUTING (HYBRID CLOUD SECURITY)

**A PROJECT REPORT**

###### ***Submitted by***

##### VINEET JOON (20BCY10094)

**RUCHITA DAS** (20BCY10128)

**PRAJVI PRANJAL** (20BCY10092)

**ZAINAB MUJTABA** (20BCY10217)

*In partial fulfillment for the award of the degree*

*Of*

**BACHELOR OF TECHNOLOGY**

*in*

# COMPUTER SCIENCE AND ENGINEERING SPEC. IN CYBER SECURITY AND DIGITAL FORENSICS

****

**SCHOOL OF COMPUTING SCIENCE AND ENGINEERING**

**VIT BHOPAL UNIVERSITY**

**KOTHRIKALAN, SEHORE**

**MADHYA PRADESH - 466114**

##### DEC 2021

**VIT BHOPAL UNIVERSITY, KOTHRIKALAN, SEHORE**

**MADHYA PRADESH – 466114**

**BONAFIDE CERTIFICATE**

##### Certified that this project report titled “ Cloud Computing (Hybrid Cloud Security)” is the bonafide work of “Vineet Joon(2OBCY10094),

##### Ruchita Das (20BCY10128), Prajvi Pranjal (20BCY10092),

##### Zainab Mujtaba (20BCY10217) who carried out the project work under my supervision. Certified further that to the best of my knowledge the work reported at this time does not form part of any other project/research work based on which a degree or award was conferred on an earlier occasion on this or any other candidate.

**PROGRAM CHAIR PROJECT GUIDE**

Dr. Rakesh R Dr. Saravanan D

Program chair, Division of Cyber Security

And Digital Forensics

Assistant Professor, Assistant Professor,

School of Computer Science and School of Computer Science and Engineering Engineering

VIT BHOPAL UNIVERSITY VIT BHOPAL UNIVERSITY

The Project Exhibition I Examination is held on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ACKNOWLEDGEMENT**

First and foremost I would like to thank the Lord Almighty for His presence and immense

I wish to express my heartfelt gratitude to Dr. Rakesh R, Head of the Department, School of Computer Science and Engineering for much of his valuable support encouragement in carrying out this work.

I would like to thank my internal guide Mr. Saravanan D, for continually guiding and actively participating in my project, giving valuable suggestions to complete the project work. Blessings throughout the project work.

Any attempt at any level can’t be satisfactorily completed without the support and guidance of our professor.

I would like to thank all the technical and teaching staff of the School of Computer Science, who extended directly or indirectly all support.

We would also like to thank our survey participants who have contributed towards survey part of this thesis. Last, but not least, I am deeply indebted to my parents who have been the greatest support while I worked day and night for the project to make it a success.

**LISTS OF FIGURES AND TABLE**

|  |  |  |
| --- | --- | --- |
| FIGURE NUMBER | FIGURE DISCRIPTION | PAGE NUMBER |
| 1 | CLOUD WORKLOAD | 10 |
| 2 | CLOUD SECURITY BREACHES STATICS | 11 |
| 3 | CLOUD SECURITY BREACHES STATICS | 11 |
| 4 | SECURE CLOUD DATA | 12 |
| 5 | HYBRID CLOUD | 14 |
| 6 | DATA SECURITY | 18 |
| 7 | PRACTICES FOR DATA BREACHES | 20 |
| 8 | ATTACK TECHNIQUES IN SUPPLY CHAIN | 22 |

|  |  |  |
| --- | --- | --- |
| TABLE NUMBER | TABLE DESCRPTION | PAGE NUMBER |
| 1 | RISK FACTOR EXTRACTED BY RBS | 16 |

##### ABSTRACT

Cloud Computing has come into reality as a new IT infrastructure built on top of a series of techniques such as distributed computing, virtualization, etc. Besides the many benefits that it can bring forth, Cloud Computing also introduces the difficulty of protecting the security of data outsourced by cloud users. This Research paper will first study the basic concepts and analyze the essentials of data security issues pertaining to Cloud Computing. Then we elaborate on major 4 issues by discussing its nature and existing solutions if available. Specifically, we will emphasize on issues of protecting data, confidentiality/ integrity/ availability, securing data access and auditing, and enforcing the regulations and compliances regarding to data security and privacy. Although many security issues and solutions were identified it has become apparent that much of the research being done only relates to the theoretical side. In this study, we have used the research methods of Systematic Literature Review. We have also preferred you tube videos to know views of various experts. Thus, this review shows that while plenty of issues have been identified future research should focus more on the practical implications of these security risks.

**CONTENT**

|  |  |  |
| --- | --- | --- |
| CHAPTER NUMBER | CHAPTER NAME | PAGE NUMBER |
| 1 | PROJECT DISCRIPTION | 7 |
| 2 | RELATED WORK INVESTIGATION | 9 |
| 3 | REQUIREMENT ARTIFACTS | 13 |
| 4 | DESIGN METHODOLOGY AND ITS NOVELTY | 14 |
| 5 | ANALYSIS | 17 |
| 6 | PROJECT OUTCOME | 20 |
| 7 | CONCLUSION | 23 |

**CHAPTER 1**

**PROJECT DISCRPTION**

Humans are moving from thousands of years from Ice age to Iron Age, Iron Age to Industrial Age and finally to the Informative Age that’s what we call digitalization. What does this digitalization provide us nothing just internet? Internet connect us from faraway places give us a place to express our thoughts worldwide by writing blogs, send instant messages and many more.

Internet connect us worldwide and help us to know that world is not what we thing it is. During this pandemic internet proves its worth without it people leaving their homes perform their daily task. Do you ever thought what would have happen if suddenly a smooth going life come to a halt and stuck in a room with four people? Nothing more than depression.

“I don’t need a hard disk in my computer if I can get to the server faster… carrying around these non-connected computers is byzantine by comparison.” – Steve Jobs, late chairman of Apple.

Everything is moving to servers and computer we need storages which can neither bother our work nor took much space. Here where cloud technology places its role. To put it simply cloud computation delivery computing services which includes servers, storages, database, networking, software, analytics and intelligence over internet. So, now we don’t have to worry about the storage nor its accessibility.

Cloud is further divided in two parts namely private and public. Private cloud is best for security as it provides accessibility only to the authorized person where as public cloud provides an IT model where the computer services and infrastructure is managed by the third party available in public. Now we know that both the clouds have some shortcomings to overcome these we have hybrid cloud. Hybrid cloud combines and unifies both cloud from on-premises infrastructure into create a single, flexible, cost optimal IT infrastructure.

Flying by the seat of the pants must have been a great experience for the magnificent men in the flying machines of days gone by, but no one would think of taking that risk with the lives of 500 passengers on a modern aircraft. The business managers of a modern enterprise should not have to take that risk either. We must develop standard cloud metrics and ROI models, so that they can have instruments to measure success.” – Dr. Chris Harding, director for interoperability and SOA at The Open Group

As said by the Dr. Chris Harding we can not risk lives of people. We studied about the cloud computation to hybrid cloud. Further we narrow down our project into four major challenges faced by the hybrid cloud. We go through many scholars reports available on net. As we are in our homes and this topic is still not much familiar to the local people. We have gone through courses, videos and webinars of the experts. From their what we learn more about the challenges and draw down some recommendation to secure hybrid.

**CHAPTER 2**

**RELATED WORK INVESTIGATION**

CLOUD COMPUTATION

"There was a period when every household, town, farm, or hamlet had its own water well," said Vivek Kundra, the first CIO of the United States.

Today, we can get clean water from shared public utilities by just turning on the tap; cloud computing operates in a similar way. Cloud computing services, like water from your kitchen faucet, may be turned on and off as needed. As with the water company, a staff of devoted professionals ensures that the service supplied is safe, secure, and available 24 hours a day. When the tap isn't turned on, you're not just saving water, similarly in cloud if you are using a resource than you are not paying for resources.

A virtualized pool of computing resources is referred to as a "CLOUD." Cloud computing is a computer paradigm in which duties are delegated to a collection of networked connections, software and services. It gives customers access to supercomputer-level processing capacity. Users have access to resources as needed. The underlying cloud architecture consists of a pool of virtualized computers, storage, and networking resources that are pooled and launched as platforms to run workloads and meet SLAs (SLA). Cloud architectures also feature provisions to provide the best service delivery for clients while maximizing resource efficiency for providers. It has the ability to manage a wide range of workloads, including batch back-end activities and user-oriented interactive applications. Rapidly deploy physical or virtual computers to boost workload and expedite deployment. Support for redundancy, self-healing, and highly scalable programming models, so that workloads can be recovered from a range of hardware/software failures that are unavoidable. Monitor resource utilisation in real time and rebalance resource allocation as needed. The primary principle of cloud computing is to reduce the processing burden on users' terminals by continuously enhancing the "cloud's" handling ability, eventually reducing users' terminals to simple input and output devices, and offering the cloud's powerful computing capacity on-demand. All of this is accessible via a conventional browser or other connection and a simple Internet connection.

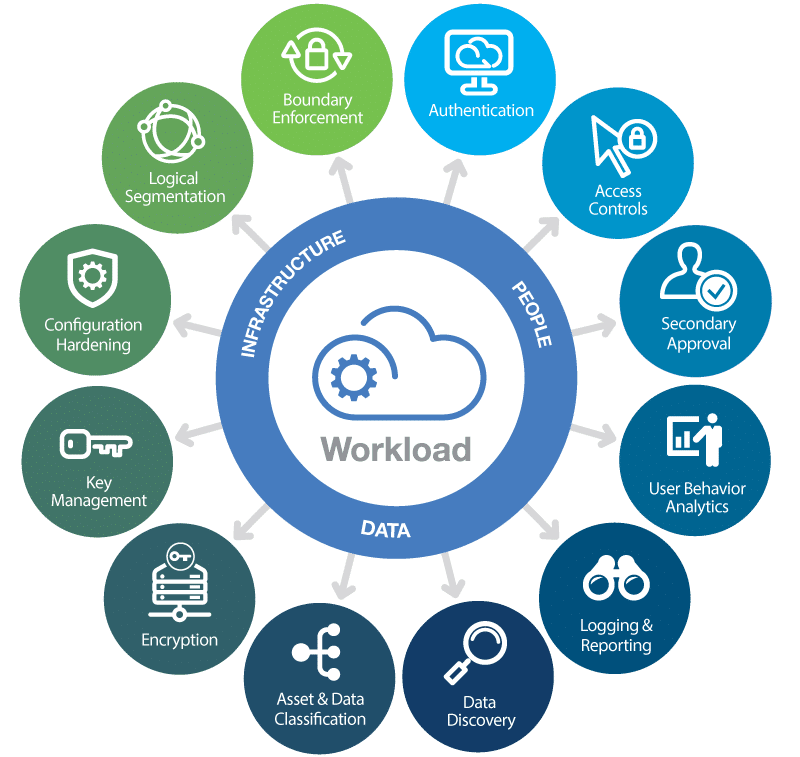


FIGURE – 1

With the introduction of cloud technologies, seeing its benefits everyone started using cloud in different sectors specially in business sector. We all know every coin has two sides more it look feasible to use more harm it can cause. The more we use the technology, more we have to think about our data security. It might be possible our data is bouncing around local and remote computers which are always connected to the internet. Hacker took the advantage and steal your private data. That data could be stored anywhere as a result, protecting it becomes more complicated than before.

There are two main reasons why cloud security is necessary:

* Convenience takes precedence over security. Cloud computing is rapidly gaining traction as a key method for both business and personal use. New technology is being introduced at a faster rate than industry security regulations can catch up, putting additional responsibility on users and providers to evaluate accessibility issues.
* Storage with multiple tenants and centralization. Every component, from fundamental infrastructure to minor data like emails and documents, may now be located and accessed remotely via web-based connections that are available 24 hours a day, seven days a week. All of this data collection on a few major service providers' systems can be quite harmful. Large multi-organizational data centres can now be targeted by threat actors, resulting in massive data breaches.

Malicious actors are increasingly probing cloud-based targets for exploits, which is unfortunate. Despite the fact that cloud providers take on many of their clients' security responsibilities, they do not handle everything. This means that even non-technical people must educate themselves on cloud security. Users, on the other hand, are not alone in their cloud security duties. Knowing the breadth of your security responsibilities will make the overall system considerably safer.



FIGURE-2

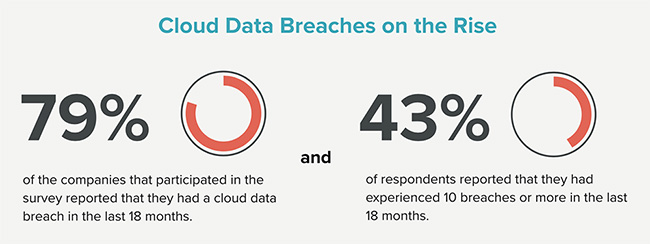


FIGURE-3

MEASURES TO KEEP CLOUD SECURE

One of the most effective ways to secure your cloud computing systems is to use encryption. Encrypt your data before storing it in the cloud, or utilise a cloud provider that will encrypt your data for you as part of the service. End-to-end encryption may be excessive if you're merely using the cloud to store non-sensitive data like corporate images or films. It is, nevertheless, critical for financial, secret, or commercially sensitive information.

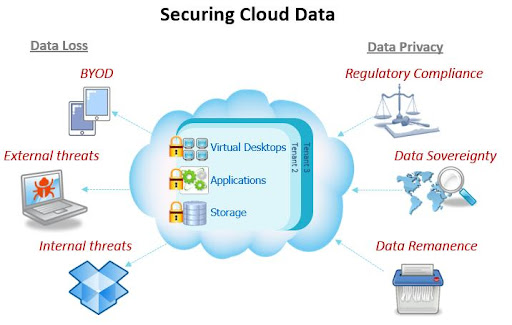


FIGURE - 4

There are encryption options available by a cloud provider:

* Communications encryption with the cloud in their entirety.
* Particularly sensitive data encryption, such as account credentials.
* End-to-end encryption of all data that is uploaded to the cloud.

When data is moving across the cloud, it is more vulnerable to being intercepted. It's vulnerable while it's travelling from one storage location to another or being transferred to your on-site application. As a result, the ideal cloud security option for vital data is end-to-end encryption. Your communication is never made available to outsiders without your encryption key when you use end-to-end encryption.

If you're utilising encryption, keep in mind that keeping your encryption keys safe and secure is critical. Keep a backup of your important files and, ideally, don't save them in the cloud. You should also update your encryption keys on a regular basis so that anyone who has access to them is locked out of the system when you make the switch.

Another effective strategy in cloud security is configuration. Basic vulnerabilities, such as misconfiguration problems, are the source of many cloud data breaches. By avoiding them, you lower your cloud security risk significantly. If you're not sure you can handle it on your own, you could wish to hire a third-party cloud security solutions provider.

**CHAPTER 3**

**REQUIREMENT ARTIFACTS**

VISION STATEMENT

The project aims to provide certain practical solutions of the major challenges faced by the companies in Hybrid Cloud Security.

SCOPE:

The scope of the project is to understand the security threats and identify the appropriate security techniques used to mitigate them in Cloud Computing (Hybrid Cloud Security).

The project identifies the four major challenges in Hybrid Cloud Security:

* Visibility and Control
* Compliance and Governance
* Data Security
* Data Chain Security

The above major challenges hinder the company to work with Hybrid Cloud Security. In this project, we have tried to list out some practical approach and solutions for the challenges.

**CHAPTER 4**

**DESIGN METHEDOLOGY AND ITS NOVELITY**

This project is designed as a research-based project. We have gone through various research papers and webinars of the experts and the industrialists. To understand various challenges faced by the companies while they work with hybrid cloud computing and tried to find out its possible solutions.

We came across four major challenges and methods to combat them. The project compiles of the major challenges along with some of the most approachable and practical solutions.

Hybrid cloud is a cloud computing environment that orchestrates between two types of platforms: local private clouds and third-party public cloud services. It provides enterprises with flexible deployment options, by allowing workloads to move between private and public clouds as computing needs and costs change.



FIGURE - 5

ADVANTAGES OF HYBRID CLOUD COMPUTATION

First cost, Private cloud services are relatively expensive on default. On the contrary, the public solutions are the cheapest. Using Hybrid cloud means that you could easily acquire the benefits of public cloud solutions while using Private cloud for data. Therefore, organizations can be benefited from both in infrastructure and application support in terms of expense.

Second reliability, Hybrid cloud services offer greater reliability since it reduces potential downtimes. This means that in case of any failure or disaster, the businesses can continue their operations with minimum interruptions.

Third deployment, Hybrid cloud is designed according to the need of organizations (Optimization process). It is a part of both Public and Private cloud services. Therefore, in order for making data transfers faster, the IT employees can minimize latency.

Fourth scalability, many of the operations that seems to be non-critical can be moved to the public cloud while lowering the demand for the private one. Hence, clients can be benefited from the scalability provided by the public cloud service.

Fifth flexibility, you can use Hybrid cloud to store sensitive and confidential data on a private cloud data centre while others on a public cloud.

Sixth agility, the customization ability of a Hybrid cloud ensures that the company is agile enough to fulfil the client's needs. Apart from doing the work of connecting old systems to new ones, the Hybrid cloud has the capability to create an underlying structure that compromise business demands.

Seventh, Service segmentation can aid an organization's control over how data is accessed and kept. For example, layering your security by keeping more sensitive data on premises while offloading other data, applications, and activities to the cloud. Separating data can also help your company stay legal and comply with data standards.

Eighth, Hybrid cloud environments can also be used to achieve redundancy. Organizations can keep their operations running in the event that one of their data centres is taken offline or infected with ransomware by using daily operations from public cloud servers and backing up systems on local data servers.

DISADVANTAGES OF HYBRID CLOUD MANAGEMENT

First security, Security is a common concern for users who wants to load confidential information into a Hybrid cloud. Due to the nature of Hybrid cloud, many security vulnerabilities are present inside them. Therefore, ensuring adequate security is a difficult process. In fact, the responsibility of securing the data completely lies upon the users. Proper precautionary measurements have to be taken to ensure that the data is well protected.

Second visibility, maintaining visibility over a hybrid cloud service is a complicated process to carry out. Because of these reasons there can be cost issues since there are more idle instances. In addition to that there can be incompliance with certain important regulations.

Third investment, while a Hybrid cloud is inexpensive in terms of operations, it needs significant investment for building the enterprise cloud. Hybrid cloud does not solely depend on public cloud, it needs the service of Private cloud as well. Private cloud on default requires cloud architects and qualified IT employees to manage them. This may not seem easy for companies with limited IT resources.

Fourth compatibility, Cloud compatibility has found to be another issue for a Hybrid cloud environment. Especially with the infrastructures. An on-premises infrastructure can perform more than the public infrastructure. This can affect the performance level of the Hybrid cloud severely.

Fifth networking, Network bottlenecks can occur when there is a data transmission between the Public and Private cloud models. Always in the Public cloud, the data transmission is done through the public internet. Public internet is known for being too slow where it can affect the performance level significantly. Especially for apps and functions that require fast operations.

Sixth control, Lack of control has always been an issue for the users using the hybrid cloud. we need to make changes over a private infrastructure so that it can be adapted to the public cloud. The problem is the users have no control over this.

As discuss in the previous slide hybrid cloud lack in security which eventually lead to lack in protection of data, applications, and infrastructure both on premises and in public cloud. This includes business processes, workloads and management across multiple its environment. So, our objective is to know about the security challenges of hybrid cloud.

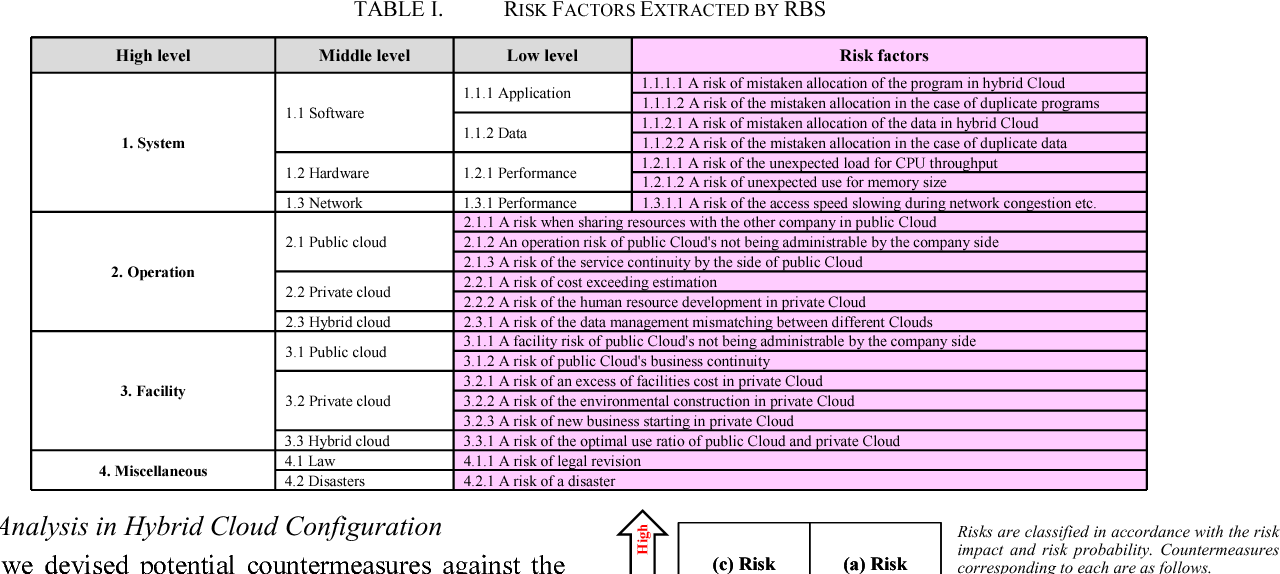


FIGURE - 5

**CHAPTER 5**

**ANALYSIS**

CHALLENAGES OF HYBRID CLOUDS

**1.Visibility and Control**: Combining public and private clouds or infrastructure can dramatically increase complexity while also increasing risk. To handle this complexity and avoid security holes, organizations must have a high level of visibility and control. Consider this: You can't properly safeguard something if you can't see it and evaluate it.

Maintaining complete visibility and control is also necessary for tracking changes (such as configurations) and ensuring that each team member works efficiently together. It is possible to maintain a transparent and smooth-running infrastructure by automating when possible and employing the correct mix of technologies.

**2.Compliance and Governance:** For a while, the highly regulated industry organizations were somewhat reluctant to use cloud computing. They even banned it. Otherwise gripped it for noncritical and no sensitive tasks and data.

Cloud technology with passing time has now advanced to a level that organizations from all industries are using it at a certain degree. That said, hybrid infrastructure does bring forward unique demanding situations for agencies withinside the healthcare, financial, government, and different regulated sectors.

One of the most important demanding situations comes not from anyone regulation, however from the truth that many companies are nevertheless manually checking to see that they're compliant and meeting custom or regulatory security baselines for security compliance and auditing requirements. It's a tedious, complex, and error-inclined procedure to start with, however it will become even greater so while coping with a mixture of heterogeneous structures withinside the cloud and on premises. When configuration adjustments are made manually, generally those adjustments may go undetected, so procedures aren't repeatable, sharable, and reproducible—all musts, in case you are making plans on passing a security audit.

Here, again, corporations have to be searching out a manner to automate the scanning and remediation of security controls with the usage of open-supply tooling. The purpose is to offer crystal-clean visibility into responsibilities and permit for scalability of these tasks—from the container stage to individual structures to the hybrid infrastructure as a whole.

**3.Data Security:** Sensitive information can be compromised in a number of ways. A data breach of any form may be disastrous for a business, whether it is damaged, deleted, improperly accessed, or just lost. Even the most secure private cloud might put data at risk in a hybrid cloud environment by sharing it with its public equivalent. Data security is always the responsibility of the person or organisation that owns the data, thus businesses that use a hybrid cloud model must take great care to evaluate the security standards and data policies of their selected public cloud provider. However, the hybrid cloud risks here go beyond the provider. Organizations must account for the possible security threats provided by such devices, which may or may not be protected or connected to other networks, in a workplace where individuals may access customer data with their own devices via the public component of the hybrid cloud. With so many points of access to the hybrid cloud, it's critical that tight, top-to-bottom rules establish and rigorously implement security protocols.

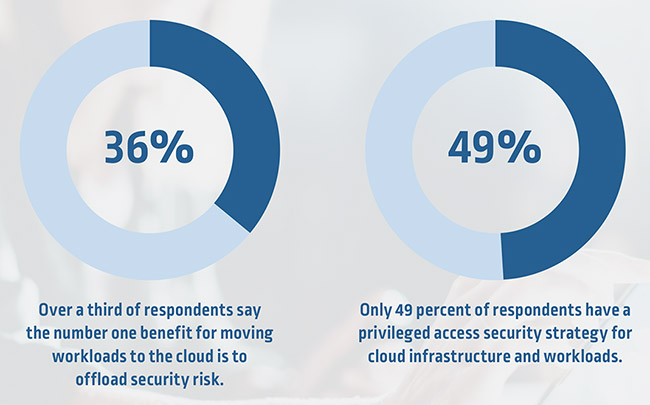
Security of data in the cloud is one of the main issues that prevent cloud migration. While private cloud data centres may be physically located on-premise, they still follow the cloud computing model: data stored in the private cloud is accessed through a private IT network infrastructure, which is susceptible to infringements, data leaks, eavesdropping, and man-in-the-middle attacks. Organizations may use both public and private clouds using hybrid cloud computing. Reduced security threats are one of the advantages; but, as the entire IT infrastructure gets more complex, further security measures are necessary.

FIGURE - 6

**4.Supply Chain Management:** Cloud computing emerges as a valuable technology that adds to this optimization by delivering infrastructure, platform, and software solutions via the internet for the entire supply chain. In supply chain management, using cloud-based services yields both financial and operational benefits. Lower infrastructure costs compared to on-premises infrastructure, supply chain visibility, platform scalability, and flexibility through collaboration with supply chain partners are just a few examples. Virtualization, distributed computing, networking, and online services are all part of cloud computing. "A Cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers," according to the Wikipedia definition. Clients, data centres, and distributed servers are all components of the cloud. It offers features like as fault tolerance, high availability, scalability, flexibility, decreased user overhead, lower total cost of ownership, and on-demand services, among others

The main benefit of cloud-based solutions is that they are easier to use. Cloud removes compatibility issues by providing easy access to all parts of the supply chain through the use of the same platform. It allows participants in a single supply chain system to share information about the supply chain. Using their member id and password, supply chain members can access and add themselves to the cloud collaboration environment. After that, all users were given permission to utilize the same platform to run simple processes and applications, reducing supply chain partners' response times. Another advantage is visibility, which allows for quick communication among supply chain actors.

As a result, visibility is a critical issue for SCM since it not only helps firms coordinate their operations and manage multiple customers, but it also allows the customer network to see the entire system in real time.

Cloud-based systems can give real-time inventory and shipment visibility, as well as better logistics tracking. Companies can better regulate their system capacity by utilising cloud computing. Companies require sufficient capacity during periods of high demand in order to meet this increased demand. As a result, they should possess the necessary database for the entire year utilising common on-premises systems in order to respond to the high demand for only a few weeks.

When we use services like Software as a service-features a complete application offered as a service on demand. Platform as a service-encapsulates a layer of software and provides it as a service that can be used to build higher-level services. and Infrastructure as a service-provides basic storage and compute capabilities as standardized services over the network. with supply chain management we get modern supply chain management.

**CHAPTER 6**

**PROJECT OUTCOME**

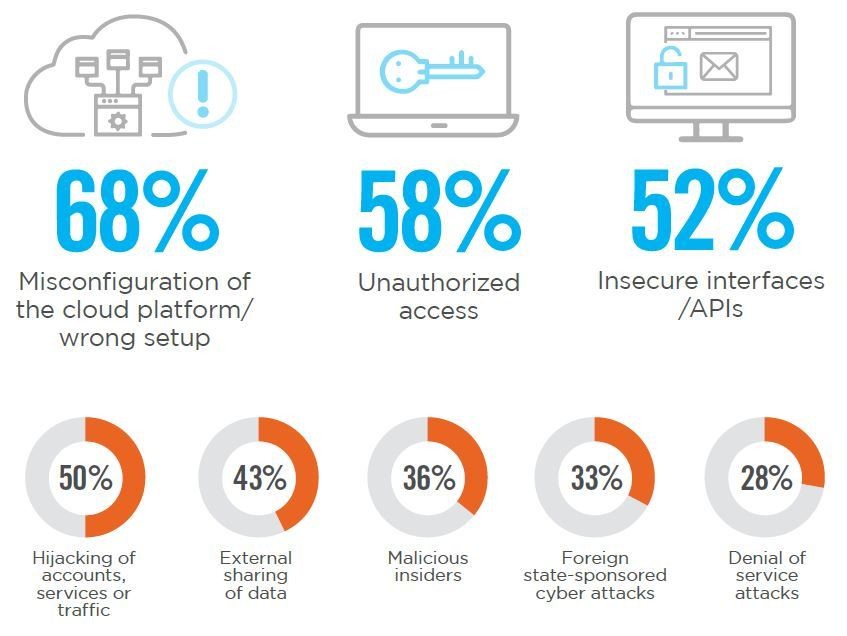


FIGURE -7

We can observe in the figure 6 there so many possibilities of data breaches in hybrid cloud. An advanced breach and attack simulation platform mitigates the risk posed by data leakage, eavesdropping, breaches, and so on by offering continuous automatic security testing. It’s system function similarly to an autonomous purple team, mimic attacks along plausible pathways using modern adversary tactics, letting businesses to test their defenses and keep 24/7 insight into the real health of their security posture.

Maintaining this kind of comprehensive visibility into growing vulnerabilities is vital in complex hybrid cloud setups where changes occur often leading to many flaws. After discovering any vulnerabilities, the systems give priority to remediation assistance, allowing firms to handle any issues that arise as rapidly as possible. When dealing with complicated hybrid installations, technology is the natural solution because to its automated and continuous nature lead to many attacks.

How do you solve the problems mentioned above? It’s pretty simple. You have two choices: you either learn to do these new things yourself, or you bring in outside experts to help you.

For business purpose first approach should be organize expertise growth it may not benefits quickly but its better than appointing people as it will take time to make them understand the situation where as you can also short of supplies. In this case much of your time will be wasted. At a data breach time is most cuscial.

When they become available, they are rapidly scooped up. Most businesses have discovered that engaging outside specialists is a superior solution. You quickly acquire the necessary abilities, and you have a diverse team of specialists working with you for as long as you require them. The most crucial thing to look for when selecting hybrid cloud consultants is experience. Your consultant should have extensive experience establishing hybrid cloud systems, with no preference for one particular public cloud provider. Remember that your company is unique and will necessitate solutions adapted to your individual requirements. Therefore, you want all possibilities on the table. Also, make certain that you recruit someone who has a genuine hybrid cloud perspective, rather than someone who encourages you to go all-in on either public or private cloud. As I indicated at the outset of this post, experts believe hybrid cloud is the enterprise's future. Make sure the consultant agrees with that mind-set, or you may find yourself heading backward instead of forward. Look for industry professionals who have used the correct technologies to handle each of the four concerns

I mentioned above: cost, security, compliance, and governance. Tools are available to assist in resolving these challenges, but you must again ensure that your industry expert has expertise implementing and using each of these tools.

Finally, while speaking with hybrid cloud experts, inquire about the future — where hybrid cloud is headed and what your organization needs for success as it expands. This discussion should encompass edge computing, machine learning, and artificial intelligence. Your consultant should be well-versed in your history while also offering insights and ideas to assist you achieve your future objectives. New technology will surely provide new problems to your organization. Make sure you have an experienced companion to assist you efficiently through the risks along the road.

There is little doubt that cloud computing is set to continue its impressive growth trajectory. Some reports suggest that more than a third of all IT departments are now under pressure to migrate all their applications to the cloud.7 As cloud technology continues to mature and with more and more IT decision makers focused on digital or IT transformation, hybrid cloud has clearly emerged as a top priority for the majority of organizations. Even though an exact definition may remain somewhat obscure for many customers and vendors, a well-executed hybrid cloud strategy could well be the difference between seeing your business fly, just about get by, or eventually wither and die.

Supply chain security, as defined by this concept, entails attempt to prevent both items leaving and contraband entering the supply chain. The possibility of "disruption of flows across businesses" in a supply chain. Supply chain risk is defined as the probability, value, and variance in the distribution of supply chain outcomes. As a result, SCS is a part of a company's entire risk management strategy. Despite the fact that the focus of this study is on SCS, it is critical to situate the debate of SCS within the greater construct of supply chain risk management. If data is breach in between of the chain company may face many lose. Possible attacks in supply chain is mention in the below figure.



FIGURE- 8

Supply chain risk management is defined as "the identification and control of supply chain hazards through a coordinated strategy among supply chain stakeholders in order to reduce overall susceptibility.

Due to the unique risks, the supply chain must protect its system to the greatest extent possible. Therefore, organisations are encouraged to lock-down access to all endpoints, thereby reducing the attack surface. Another recommendation is to mandate the use of a virtual private network (VPN) for all communications. To take advantage of the VPN, follow these key points:

Insist that supply chain members use a VPN for all communications and to lock down all IP-enabled devices.

Ensure that the selected VPN solution might be securely deployed in a public cloud, a private cloud, and on-premises.

Select a VPN with robust encryption, preferably one that is CSfC certified.

**CHAPTER 7**

**CONCLUSION**

The flexibility of Cloud Computing, allows users to access and share their software programmes online and access information by using distant server networks rather than relying on primary tools and information housed on their own computers in the future. Cloud computing security challenges are constantly one of the key study areas for academics and developers to discover the right solutions. From the standpoint of this thesis, we recommend that optimum and acceptable security solutions for specific Cloud services be found. There is potential to establish standards to address future difficulties in Cloud security such as physical security, espionage, transparency, data ownership, hypervisor infections, and malevolent insiders. To focus on more particular areas such as regulatory and compliance challenges, jurisdictional legislation, and so on...

**REFRENCES**

1. https://www.brighttalk.com/webcast/15137/497814/data-security-in-hybrid-cloudhttps://techbeacon.com/security/4-hybrid-cloud-security-challenges-how-overcome-themhttp://dspace.sfit.co.in:8004/jspui/bitstream/123456789/1628/1/Group%20No.46%20BECMPN%20A%2021-Data%20Security%20in%20cloud%20Using%20Hybrid%20Encryption%20Algoithm.pd
2. https://www.cnsr.ictas.vt.edu/publication/chapter/BookChapter\_Yu12.pdf
3. <https://books.google.co.in/>
4. https://scholar.google.com/
5. http://blog.logisticsjobs.asia/benefits-and-drawbacks-of-cloud-computing-in-scm/
6. https://www.xmcyber.com/top-4-hybrid-cloud-security-challenges/
7. https://www.xenonstack.com/blog/cloud-governance
8. https://cloud.google.com/security/compliance
9. https://www.bmc.com/blogs/hybrid-cloud-security/
10. https://cloud.netapp.com/blog/blg-cloud-visibility-3-critical-challenges-and-solutions