CLOUD COMPUTING

DATA SECURITY IN CLOUD COMPUTING

BY

PRATHAM.M

CONTENTS:

ABSTRACT

Recently, a new paradigm known **as "Cloud Computing"** has emerged in which resources from computing infrastructures are offered as services over the Internet. However, this paradigm also poses a number of brand-new problems for access control and data security. If a company or organization outsources its data to the cloud, they are not within the same reliable space as their established infrastructures. This thesis contributes to overcome the data security challenges and issues due to using the cloud for critical applications. The next generation of IT enterprise design will be based on cloud computing. The application software and databases are moved to huge data centers via cloud computing, as opposed to traditional methods, where the management of the data and services may not be completely reliable. However, this distinctive trait creates a number of new, poorly known security challenges. In this term paper the basic information of data security in cloud computing is studied. Benefits of using Cloud Computing, Example for Cloud Computing, Cloud Security, Data privacy protection, web-application security, multimedia data security, threats to cloud security, Security issues in cloud, data security attributes are studied in this research paper.

CHAPTER 1

INTRODUCTION

Cloud Computing : A model for ubiquitous, convenient, on-demand network access to a pool of configurable computing resources, such as networks, servers, storage, applications, and services, is known as cloud computing. It enables these resources to be quickly provisioned and released with little management work or service provider involvement. The term "the cloud" describes the software and databases that run on servers that may be accessed via the Internet. Data all throughout the world house cloud servers. In simple words The on-demand delivery of computing capacity, databases, storage, applications, and other IT resources via the internet with pay-as-you-go pricing is known as cloud computing.

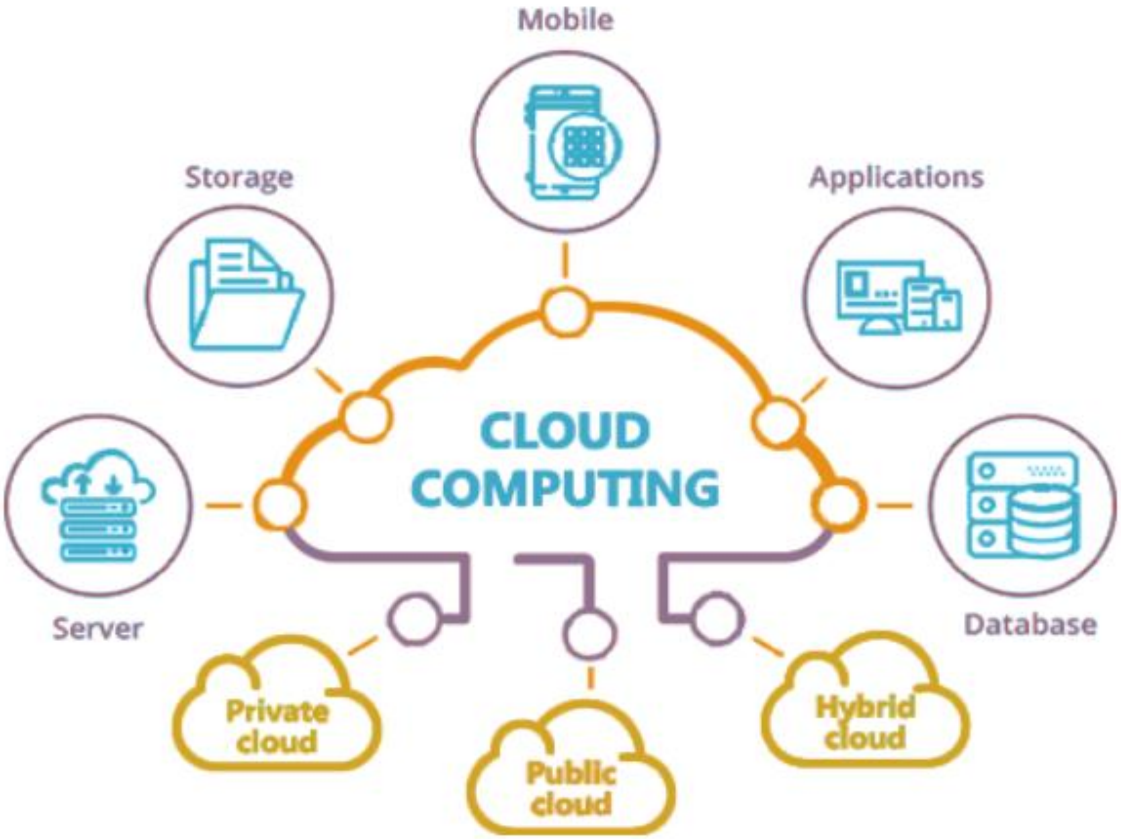


Fig1: Cloud Computing

Cloud Computing is defined as storing and accessing of data and computing services over the internet.

1.1 Cloud Computing Characteristics

- Measured services
- Rapid elasticity
- Massive scale
- Resource pooling
- Easy maintainance
- Geographic Distribution
- Low cost software
- Advanced security

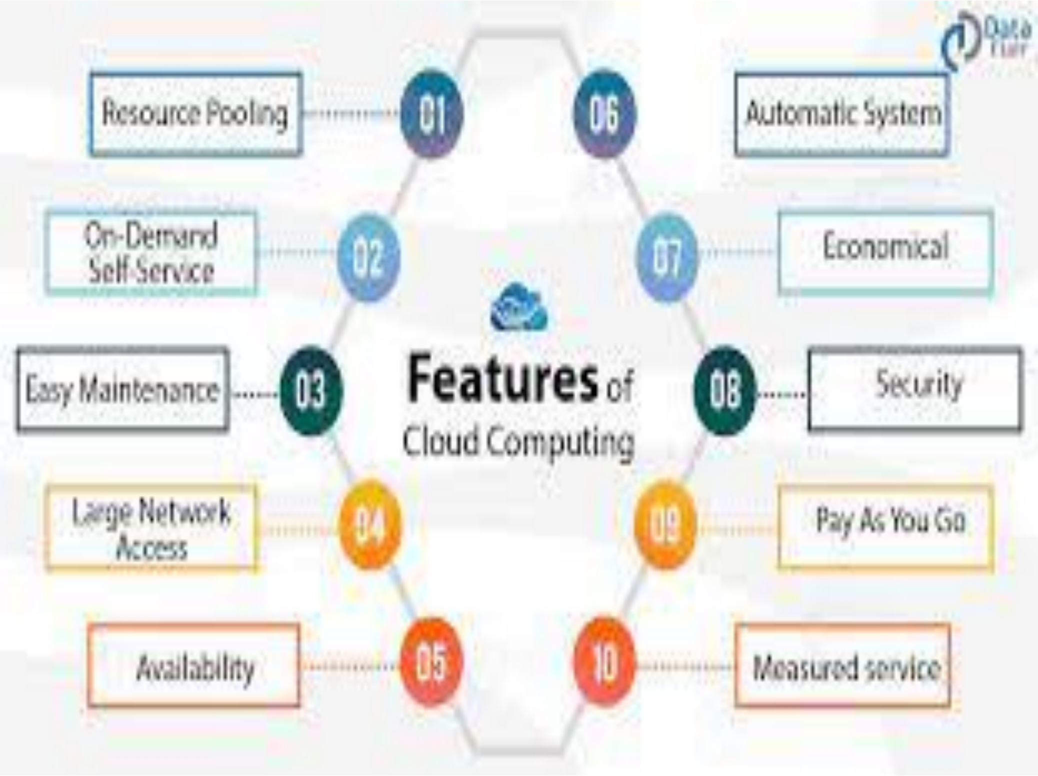


Fig 2: Features of Cloud Computing

1.2 BENEFITS OF CLOUD COMPUTING

Cost saving, mobile storage, anytime anywhere access, better security, energy saving, environment benefits

- Reduced IT costs. Moving to cloud computing may reduce the cost of managing and maintaining your IT systems.
- Scalability.
- Business continuity.
- Collaboration efficiency.
- Flexibility of work practices.
- Access to automatic updates.

1.3Example for Cloud Computing

i) **Medical Care:**

With the aid of cloud computing, medical personnel can remotely perform tests, host information, and study patients. Doctors can instantly communicate information from any location because to cloud technologies. By enabling immediate massive data file transfers, it also reduces costs. Efficiency is undoubtedly increased by this. In the end, cloud computing technology aids the medical staff in ensuring that patients receive the finest care without undue delay. With the aid of remote conferencing, the state of patients can also be updated in a matter of seconds.

ii) Education:

For distance learning, cloud computing is also beneficial in educational institutions. It provides numerous services for schools, universities, professors, and teachers to connect with thousands of students world wide. Many services are provided without charge to faculty, teachers, professors, and students from different educational institutions by businesses like Google and Microsoft. These services are used by several educational institutions all over the world to increase production and efficiency.

iii) Government:

The government and military of the United States were early adopters of cloud computing. Social, mobile, and analytics technologies are included in their cloud. Nevertheless, they are required to follow stringent compliance and security requirements (FIPS, FISMA, and Fed RAMP). This defends against both domestic and foreign cyber threats.

iv) Analytics for big data:

Data scientists can evaluate diverse data patterns and insights with the aid of cloud computing to make more accurate predictions and decisions. For this, a variety of free and open-source big data analytics and development tools, like Cassandra are available.

v) Communication:

Network-based access to communication tools like social media and email is made possible by cloud computing. A cloud-based infrastructure is also used by WhatsApp to support user chats. The hardware of the service provider houses all the data.

CHAPTER 2

DATA SECURITY IN CLOUD COMPUTING

What is data security in Cloud Computing?
Cloud data security is the combination of technology solutions, policies, and procedures that you implement to protect cloud-based applications and systems, along with the associated data and user access.

Fig3: Data Security

- Why data security important in Cloud Computing?

Your data and applications are accessible to authorised users to cloud security. You'll always have a dependable way to access your cloud applications and data, enabling you to address any possible security issues right away.

- How can we protect data security

Here are some practical steps you can take today to tighten up your data security.

- Here are a few doable actions you can do right away to strengthen your data security.
- Make a backup of your data
- Use secure passwords.
- When working remotely, use caution.
- Be aware of emails that seem off.
- Install malware and antivirus protection.
- Never leave work documents or laptops unattended
- Ensure that your Wi-Fi is protected.

2.1 CLOUD SECURITY

CLOUD SECURITY to address both internal and external security threats to enterprises, a set of procedures and tools known as cloud security was developed. As they carry out their digital transformation strategy and include cloud-based tools and services into their infrastructure an organizations need cloud security.

Cloud computing security risks can affect everyone from businesses to individual consumers. For example, consumers can use the public cloud for storing and backing up files (using SaaS services like Dropbox), for services like email and office applications, or for doing tax forms and accounts.

CLOUD SECURITY CHALLENGES

- ✓ Lack of visibility
- ✓ Multi tenancy
- ✓ Access management and shadow IT
- ✓ Compliance
- ✓ Mis Configurations

What types of cloud security solutions are available?

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

Enterprises using Identity and Access Management (IAM) technologies and services to establish policy-driven enforcement techniques for each user trying to access both on-premises and cloud-based services to provide all users with digital identities, which is IAM's main purpose they might be actively monitored and regulated throughout all data exchange. as needed.

- **Prevention of Data Loss (DLP)**
  Data loss prevention (DLP) services provide a set of tools and services that ensure the security of regulated cloud data. DLP systems protect all data stored, whether at rest or in motion, through a combination of remediation warnings, data encryption, and other preventative measures.

- **Security Information and Event Management(SIEM)**
  Security Information and Event Management (SIEM) is a comprehensive security orchestration system that automates threat monitoring, detection, and response in cloud-based environments. IT teams can effectively apply their network security standards with the help of SIEM technology, and they can quickly address any possible threats. The SIEM solution correlates log data across many platforms and digital assets using AI-driven technologies.

- **Continuity of Operations and Disaster Recovery**

Regardless of the security measures businesses have in place for their on-premise and cloud-based infrastructures, data breaches and disruptive disruptions are still possible. When newly discovered vulnerabilities or significant system failures occur, businesses must be prepared to react as quickly as feasible. Disaster recovery solutions are a pillar of cloud security and provide companies with the tools, standards, and services necessary to quickly recover lost data and resume regular operations.

2.2 THE IDEA OF DATA SECURITY

Fig4: Idea of Data Security

Taking Information and making it secure, so that only yourself or certain others can see it, is obviously not a new concept. However it is one that we have struggled with in both the real world and the digital world. In the real world, even information under lock and key, is subject to theft and is certainly open to accidental or malicious misuse. In the digital world this analogy of lock and key protection of information has persisted, most often in the form of container-based encryption. But even our digital attempt at protecting information has proved less than robust, because of the limitations inherent in protecting a container rather than in the content of that container. This limitation has become more evident as we move into the era of cloud computing: Information in cloud environment has much more dynamism and fluidity than information that is static on a desktop or in a network folder, so we now need to start to think a new way to protect information.

Before we embark on how to move our data protection methodologies into the era of the cloud, perhaps we should stop, think, and consider the true applicability of information security and its value and scope. Perhaps we should be viewing the application of data security as less a walled and impassable fortress and more of sliding series of options that are more appropriately termed **“risk mitigation”**.

The reason that I broach this subject so early on is that I want the reader to start to view data security as a lexicon of choices, as opposed to an on/off technology. In a typical organization, the need for data security has a very wide scope, varying from information that is set as public domain, through to information that needs some protection, through to data that are highly sensitive, which, if leaked, could cause catastrophic damage, but nevertheless need to be accessed and used by selected users.

One other aspect of data security that I want to draw into this debate is the human variable within the equation. Computer technology is the most modern form of the toolkit that we have developed since human prehistory to help us improve our lifestyle. From a human need perspective, arguably ,computing is no better or worse than a simple stone tool, and similarly, it must be built to fit the hand of its user. Technology built without considering the human impact is bound to fail. This is particularly true for security technology, which is renowned for failing at the point of human error.

2.3 CLOUD DATA PROTECTION

The term "cloud data protection" refers to a group of data storage and security techniques used to safeguard data as it is stored, transferred, and accessed in a cloud environment. When it comes to the data in question, data that is stored is referred to as "data at rest" and data that is in motion as "data in motion."

In contrast to data security, data protection relates to the copying of your data rather than its actual security. A data protection programme is designed to ensure that your sensitive data is still intact in the event of loss or damage, whereas data security prevents data from being accessed or distributed by unauthorized parties in the first place.

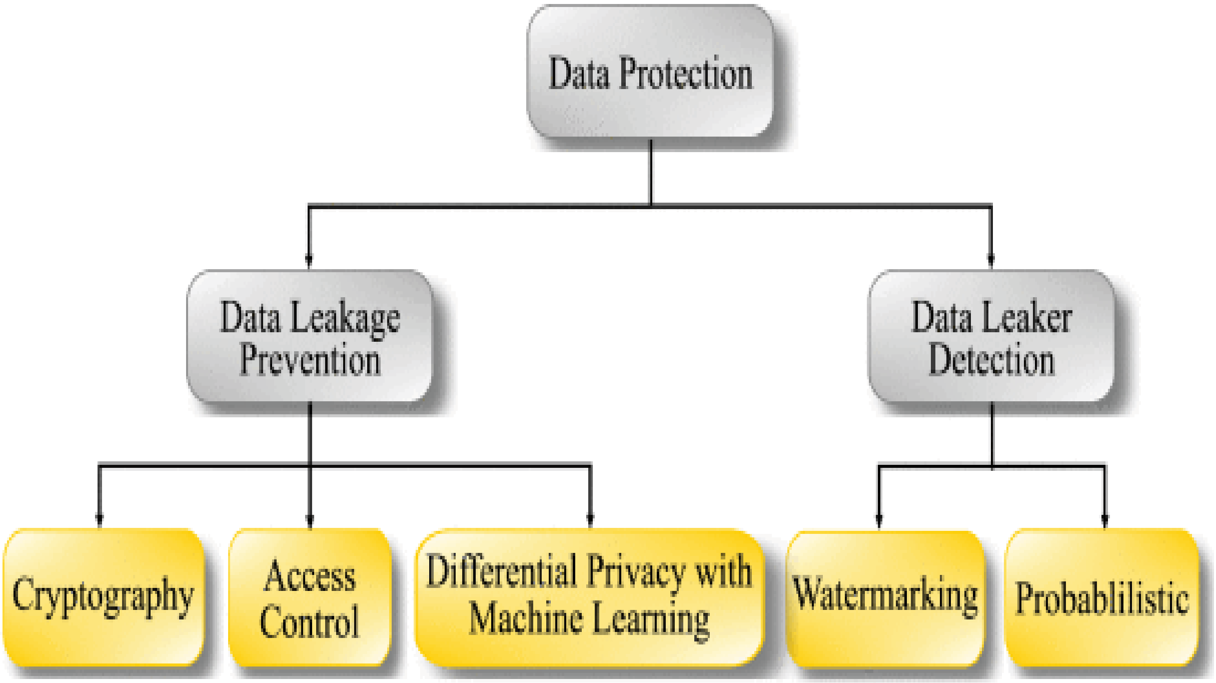


Fig5: Data Protection

The technique of protecting a firm's data in a cloud environment, regardless of where it is situated, whether it is in motion or at rest, and whether it is handled internally by the company or externally by a third party, is known as cloud data protection. If we can start off our view of data security as more of a risk mitigation exercise and build systems that will work with humans then perhaps the software we design for security data in the cloud will be successful.

2.4 TECHNOLOGIES FOR DATA SECURITY IN CLOUD COMPUTING

i) Data Base Outsourcing And Query Integrity Assurance

Outsourcing data bases has grown in importance as a part of cloud computing in recent years. Over the past ten years, a terabyte of data has been transmitted over great distances for substantially less money thanks to the quick development of network technology. The entire cost of managing data is also five to ten times greater than the costs of initial collection. As a result, there is interest in outsourcing database management responsibilities to third parties who can do so at a significantly lower cost thanks to the law of large numbers. The advantages of this new outsourcing model include lowering the expense of running a Database management system (DBMS) independently and allowing business owners to concentrate on their core operations. Clients submit queries to the unreliable service provider while the database owner outsources its data management chores. Let T represent the data that will be outsourced. Preprocessed, encrypted, and stored at the service provider are the data T are. A user converts a set of queries from the encrypted database to Q against T in order to evaluate the queries. The authenticity of data returned from a data repository can be verified using a method, system, or computer programme. Using one encryption for the primary data set and another for the secondary data set, a data store has two sets of encrypted data.

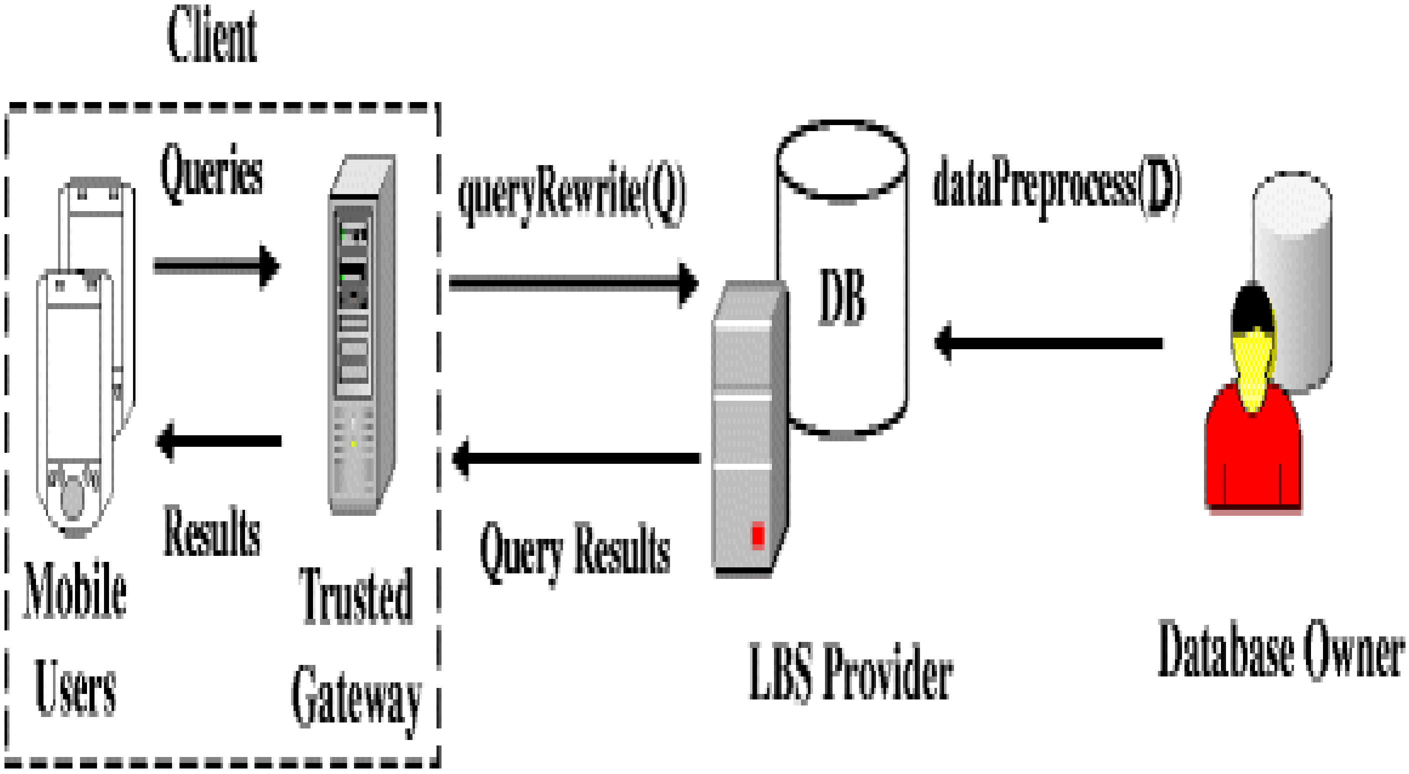


Fig6: Data Base Outsourcing And Query Integrity Assurance

There are two security concerns in database outsourcing. These are **data privacy** and **query integrity.**

ii) Data Privacy Protection

Hacigumus et al proposed a method to execute SQL queries over encrypted database. In order to avoid having to decrypt the data description, their method is to process as much of the service providers' queries as possible, leaving the client to handle the remaining queries. An order-preserving encryption method for numeric values was proposed by Agarwal et al, allowing any comparison operation to be applied directly on encrypted data. Updates can be handled by their method, and new values can be added without necessitating changes to the encrypted versions of existing values. Generally existing methods enable direct execution of encrypted queries on encrypted datasets and allow users to ask identity queries over data of different encryption. The ultimate goal of this research direction is to make queries in encrypted database as efficient as possible while preventing adversaries from learning any useful knowledge about the data. Research in this field did not consider the problem of query integrity.

iii) Query Integrity Assurance in database outsourcing

A procedure, a system, and a software application for verifying the accuracy of data retrieved from a data storage. The primary data set and the secondary data set are both encrypted using different methods in a data store. A portion of the primary data set makes up the secondary data set. To retrieve a primary data result from the primary data collection, a client conducts a meaningful query against the data store. At least one validating query is sent to the data store using a query interface. A secondary data result from the secondary data set is returned by each validating query. If the data satisfying the substantive question is included in an unencrypted secondary data result, the query interface gets the secondary data result and issues a data invalid notification.

iv) Data Integrity In Untrustworthy Storage

While the Transparent cloud provides flexible utility of network-bases resources, the fear of loss of control on their data is one of the major concerns that prevent and users from migrating to cloud storage services. Actually it is a potential risk that the storage infrastructure providers become self-interested, untrustworthy, or even malicious. There are a variety of reasons why a storage service provider might stop being dependable, like trying to hide the effects of an operational error or downplaying the system's vulnerability after data have been stolen by an enemy. This section describes two technologies that allow data owners to check the accuracy of their data even when it is being held by remote, unreliable storage providers.

Actually, before the term “cloud computing” appears as an IT term there are several remote data storage checking protocols. According to further study, a remote data procession checking technique must meet the following five criteria in order to be used in practise.

1. The verifier shouldn't be required to process an entire copy of the material being checked as a prerequisite. Additionally, it is unnecessary for a verifier to maintain a duplicate copy of the content being verified in real life. It should be sufficient to store a larger contents digest of the data at the verifier as long as it serves its purpose adequately.

2. Given the unreliable prover, the protocol needs to be very strong. A malevolent prover has a motive to conceal the data integrity violation. The protocol must be reliable enough for such a prover to fall short of persuading the verifier. The amount of information exchanged during the verification operation should not lead to high communication overhead.

3. The protocol ought to be effective in terms of computation.

4. The verification should be able to be performed an unlimited number of times.

5. There shouldn't be a lot of communication overhead caused by the information transmitted throughout the verification operation.

v) WEB-APPLICATION BASED SECURITY

A Cloud Computing environment resources are provided as a service over the internet in a dynamic, virtualized and scalable way. Through cloud computing services, users access business application on –line from a web browser, while the software and data are stored on the servers. Web security is therefore more crucial than ever in the age of cloud computing. The first gate protecting the huge cloud resources is the website server. The impact of any web security vulnerability will be exacerbated at the level of the entire cloud because the cloud may function continuously to handle millions of dollars' worth of daily online transactions. Web attacks techniques are often referred as the class of attacks. When any web security vulnerability is identified is identified, attacker will employ those techniques to take advantage of the security vulnerability. The types of attack can be categorized in authentication, authorization, client-side attacks, command execution, information disclosure, and logical attacks. Due to the limited space, this selection introduces each of them briefly. Interested readers are encouraged to explore for more detailed information from the material cited.

The concept of designing websites to work as expected even when they are attacked is known as web application security (sometimes referred to as Web App Sec). The idea entails a set of security measures built into a web application to safeguard its resources from potentially harmful agents.

vi) MULTIMEDIA DATA SECURITY STORAGE

With the rapid development of multimedia technologies, more and more multimedia contents are being stored and delivered over many kinds of devices databases, and networks. Multimedia Data security plays an important role in data storage to protect multimedia data. Recently, how storage multimedia contents are delivered by both different providers and users has attracted much attentions and many applications. This section briefly goes through the most critical topics in this area.

CHAPTER 3

CHALLENGES WITH DATA MIGRATION

After you decide to rollout a cloud service within your organization you need to migrate some and login, profile details, user data, and corporate information to the cloud. Cloud providers must be templates and procedures to conveniently migrate in house data to public clouds.

However we must be aware of inherent challenges during and after migration , which are as follows:

i. **Liability Concerns:** Cloud providers have a maximum data value for damage claims in a SLA. This value may be much lesser than the data value or the effort needed to fix data integrity problems.

ii. **Compliance Concerns:** The cloud provider must comply with various regulatory and important requirements, such as the Federal Information Security Management Act(FISMA), the Hereby Insurance Portability and Accountability Act (HIPAA), and the International organization in Standardization(ISO), mandated by your business vertical for data protection and proxcy.

iii. **Connectivity Concerns:** There can be several faults in WAN links between the consumer and the provider. It is supported by various connectivity providers and is outside the contract of the consumer or the provider.

3.1 CHALLENGES WITH DATA SECURITY

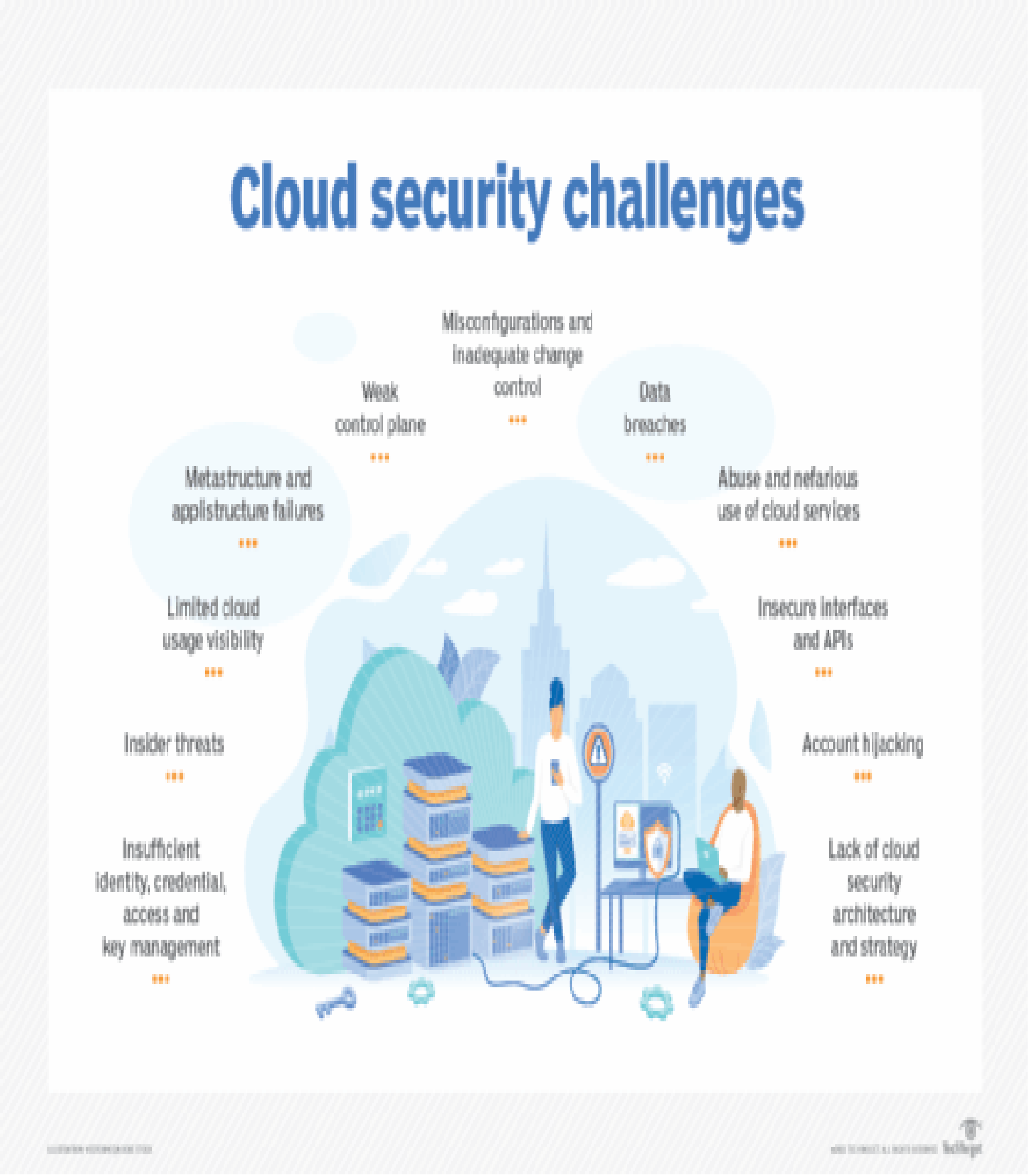

Cloud security challenges
Misconfigurations and inadequate change control
Weak control plane
Data breaches
Metastructure and applistructure failures
Abuse and nefarious use of cloud services
Limited cloud usage visibility
Insecure interfaces and APIs
Insider threats
Account hijacking
Insufficient identity, credential, access and key management
Lack of cloud security architecture and strategy
TechTarget

Fig 7:Security Challenges

Challenges with data security are as follow:

- **Security Risks-** Due to inherent multi-tenancy and ease of access within a cloud the data subjected to various security risks, which continues to be a serious concern.
- **Quality of Service-** The second concerns, after security is quality of service. Apprehensions about performance, long response time, and wan induced latency, inhibit many potential customers from readily accepting cloud service. The cloud provider must be able to ensure that response time and performance do not pose any impediment to cloud adoption.
- **Data Availability**-The third concern, after security and quality of service, is data availability. After a customer starts using cloud service and data, there are chances of unexpected downtime. There have been several outages at cloud providers despite their redundancy and replication.

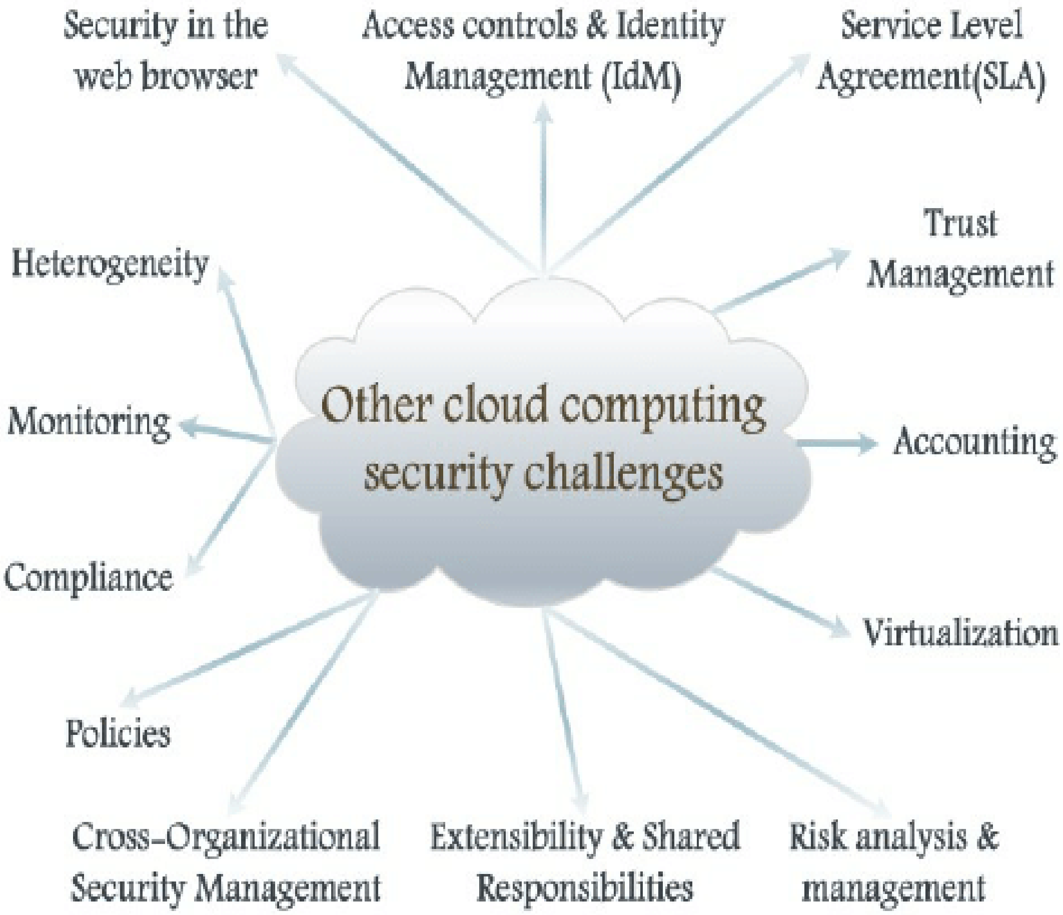

Security in the web browser
Access controls & Identity Management (IdM)
Service Level Agreement(SLA)
Heterogeneity
Trust Management
Other cloud computing security challenges
Monitoring
Accounting
Compliance
Virtualization
Policies
Cross-Organizational Security Management
Extensibility & Shared Responsibilities
Risk analysis & management

Fig 8: Cloud Computing Security Challenges

CHAPTER 4

SECURITY ISSUES IN CLOUD COMPUTING

There is no denying that cloud computing offers a number of benefits, but there are also some security concerns. These Security Issues in Cloud Computing are listed below.

i. **Data Loss:** One of the problems with cloud computing is data loss. This is often referred to as a data leak. We are aware that someone else has access to our sensitive data and that we do not have complete control over our database. Therefore, it is feasible that hackers will access our sensitive data or personal files if the security of a cloud service is breached.

ii. **Hackers' interference and Insecure APIs** –As far as we are aware, if we are discussing the cloud and its services, we are also discussing the Internet. Additionally, we are aware that using API is the simplest way to interface with the cloud. Therefore, it is crucial to protect the APIs and interfaces that external users use. However, there aren't many services accessible to the general public in cloud computing either .The vulnerability of cloud computing lies in the possibility that other parties could access these services. Therefore, it's likely that hackers could simply harm or hack our data using these services.

iii. **User Account Hijacking**- The most important security concern with cloud computing is user account hijacking. if a hacker manages to take control of a user's or an organization's account. The hacker is then completely free to engage in Unauthorized Activities.

iv. **Changing Service Provider**-Another significant security concern with cloud computing is the inability to switch service providers or vendors. Changing vendors will present a variety of challenges for many enterprises. For instance, if a company wants to switch from Amazon Web Services (AWS) to Google Cloud Services, they will encounter a num4ber of issues, such as the need to transfer all of their data, as well as issues related to the fact that the two cloud services utilise various different techniques and functions. Additionally, it's probable that AWS costs are different from those of Google Cloud and other services.

v. **Lack of Skill**: The primary issues faced by an IT company with unskilled employees include challenges with changing to a different service provider, needing an extra function, not knowing how to use a feature, etc. So, in order to work, one needs to be skilled.

vi. **Denial Of Service (DOS) Attack-** An excessive amount of traffic on the system can result in a denial of service (DOS) attack. Large companies like those in the banking industry, the government sector, etc. are the primary targets of DOS assaults. Data loss occurs during a DOS attack. Therefore, it costs a lot of money and takes a lot of time to handle data recovery.

CHAPTER 5

THREATS TO CLOUD SECURITY

- **Misconfiguration-** Any flaws, holes, or faults in cloud configuration could put your environment at danger when you utilize the cloud. Security lapses, external hackers, ransom ware, malware, or insider threats that gain access to your network through weaknesses are some examples of these cyber threats.

- **Unauthorized Access-** Once someone has gained illegal access to data or computer networks, they can harm a company in a number of different ways. They might blatantly take documents, data, or other data. They might use that access to further hack user accounts.

- **Insecure Interfaces/APIs-** Although APIs are increasingly useful for streamlining cloud computing procedures, they frequently raise security issues, especially if left unprotected. Insecure APIs can be used by adversaries to compromise or steal private and sensitive data.

- **Hijacking of Accounts-** In the cloud services, account or service hijacking continues to pose a severe security risk. When someone steals your personal information and uses it to access your accounts, this is known as account hijacking (bank account, e-mail account or social media account).

- **Lack of Visibility-** The term "cloud visibility" describes the capacity to have a thorough understanding of all the activity within your cloud network. You now have more control over your cloud infrastructure, allowing you to keep an eye on concerns with performance and cost-effectiveness while also monitoring cloud security.

- **External Sharing of Data-** Data sharing is made simple with the help of the cloud. Many clouds provide users the choice of sending an explicit email invitation to a collaborator or sending a link to a shared resource that anybody with the URL can access.

- **Malicious Insiders Threats-** Any organization that deals with them faces serious security risks. A malevolent insider already has authorized access to a network's sensitive resources and data within an organization. It is difficult for an unprepared business to identify a malicious insider because attempts to get this degree of access are what most attackers use to show themselves to their target. It is significantly more challenging to identify a malicious insider on the cloud. Many conventional security solutions are less effective with cloud deployments because businesses have less control over the underlying infrastructure. This makes it much more challenging to identify malevolent insiders because cloud-based technology is frequently vulnerable to security flaws and is directly accessible from the public Internet.

- **Cyber attacks-** Because cybercrime is a business, the targets that the criminals choose are those who will be most profitable to them when they launch their attacks. Cloud-based infrastructure can be accessed directly from the public Internet, but it also frequently lacks adequate security and holds a lot of confidential and priceless data. A successful attack can likely be performed numerous times with a high probability of success because the cloud is utilised by numerous different companies. The cloud deployments of businesses are so frequently the target of hackers.

- **DOS Attacks**- Many firms' capacity to conduct business depends on the cloud. They run significant internal and customer-facing applications as well as keep business-critical data in the cloud. This indicates that a successful Denial of Service (DoS) attack against cloud infrastructure is probably going to have a significant effect on a variety of different companies. The cloud-based resources of a company are thus seriously threatened by DoS attacks where the attacker requests a ransom to end the attack.

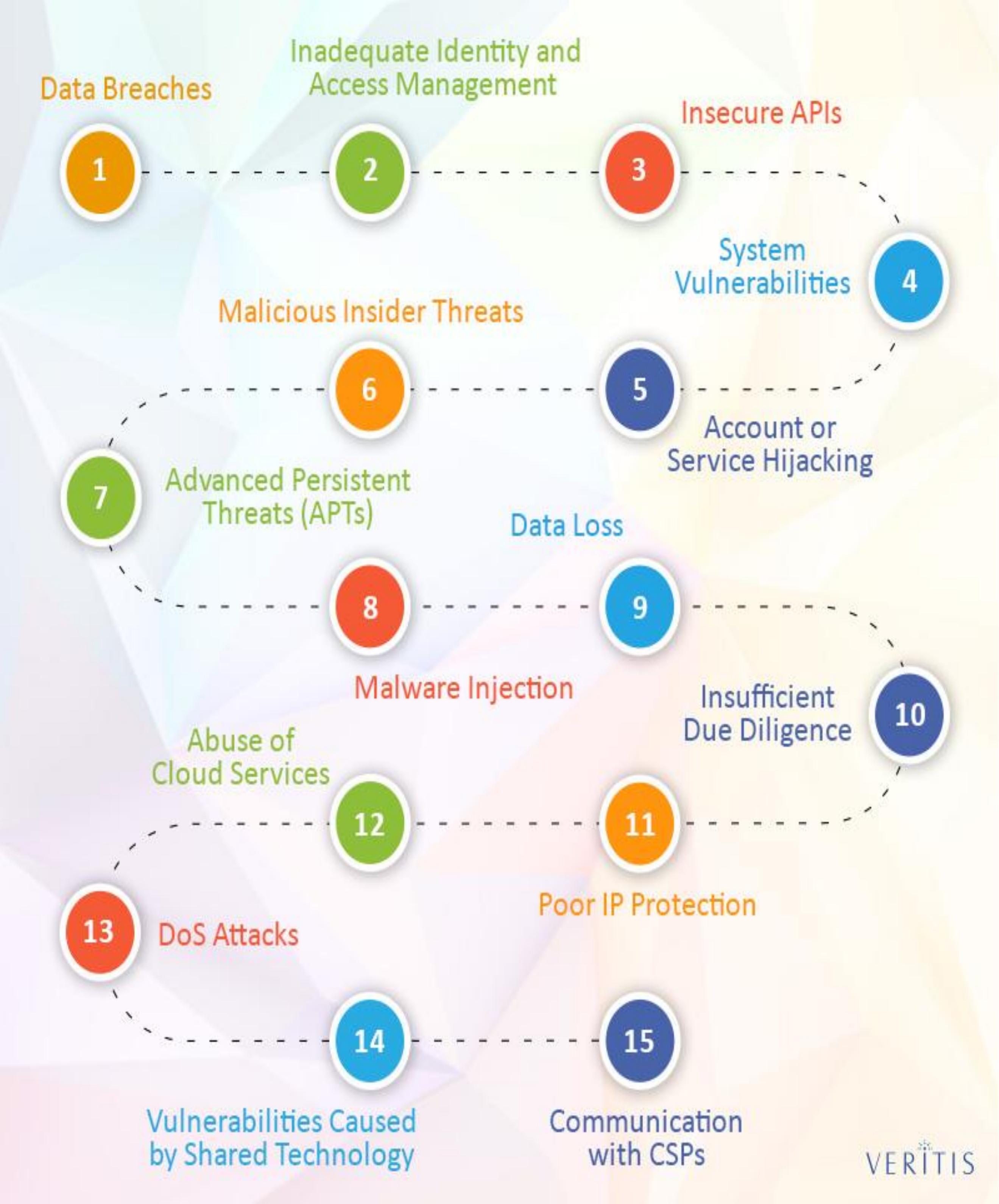
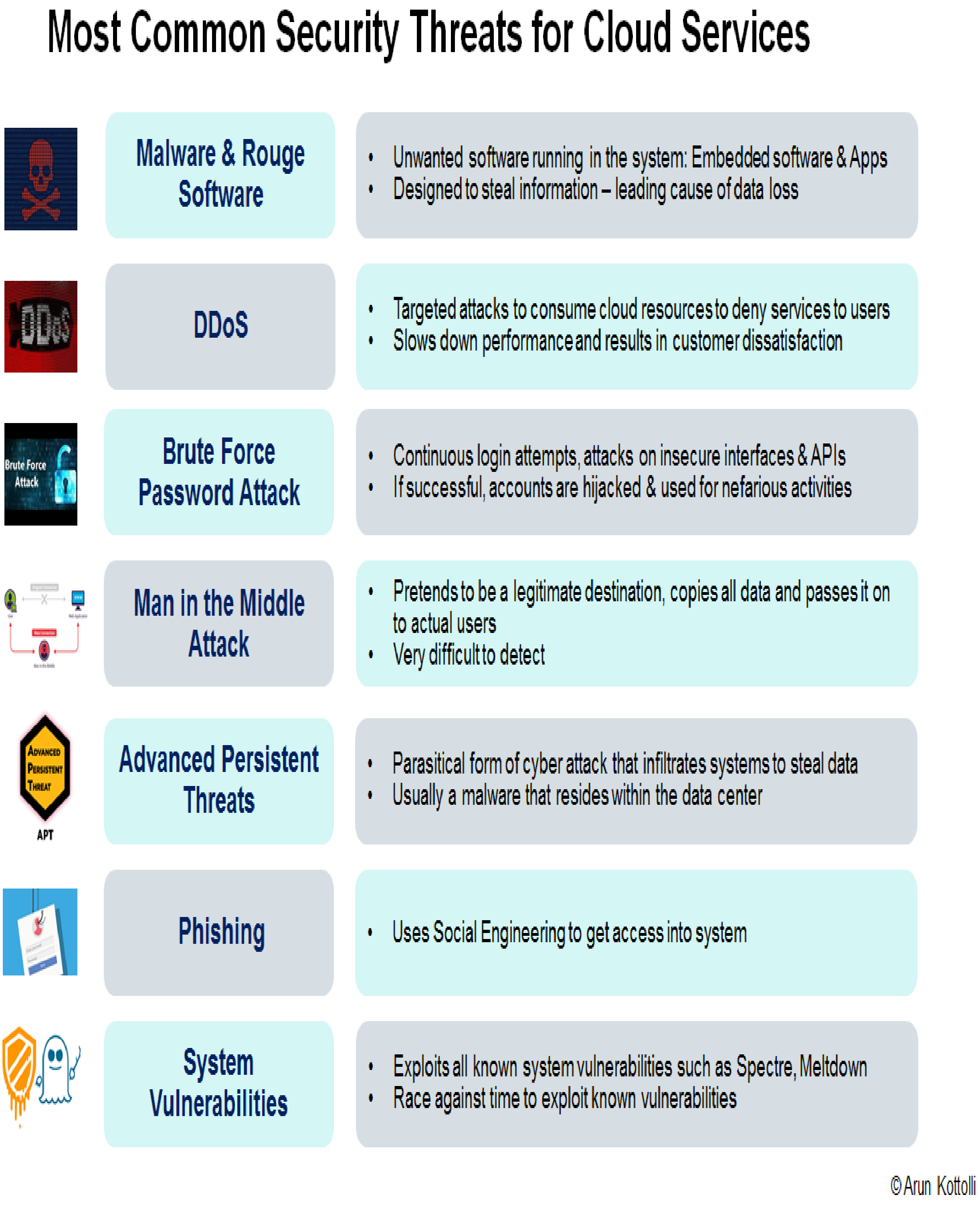

Data Breaches
1
Inadequate Identity and Access Management
2
Insecure APIs
3
System Vulnerabilities
4
Account or Service Hijacking
5
Malicious Insider Threats
6
Advanced Persistent Threats (APTs)
7
Malware Injection
8
Data Loss
9
Insufficient Due Diligence
10
Poor IP Protection
11
Abuse of Cloud Services
12
DoS Attacks
13
Vulnerabilities Caused by Shared Technology
14
Communication with CSPs
15
VERITIS

Fig9:Threats of Cloud Security



Most Common Security Threats for Cloud Services

Malware & Rouge Software	• Unwanted software running in the system: Embedded software & Apps • Designed to steal information – leading cause of data loss
DDoS	• Targeted attacks to consume cloud resources to deny services to users • Slows down performance and results in customer dissatisfaction
Brute Force Password Attack	• Continuous login attempts, attacks on insecure interfaces & APIs • If successful, accounts are hijacked & used for nefarious activities
Man in the Middle Attack	• Pretends to be a legitimate destination, copies all data and passes it on to actual users • Very difficult to detect
Advanced Persistent Threats	• Parasitical form of cyber attack that infiltrates systems to steal data • Usually a malware that resides within the data center
Phishing	• Uses Social Engineering to get access into system
System Vulnerabilities	• Exploits all known system vulnerabilities such as Spectre, Meltdown • Race against time to exploit known vulnerabilities

©Arun Kottoli

Fig 10: Common Security Threats for Cloud Services

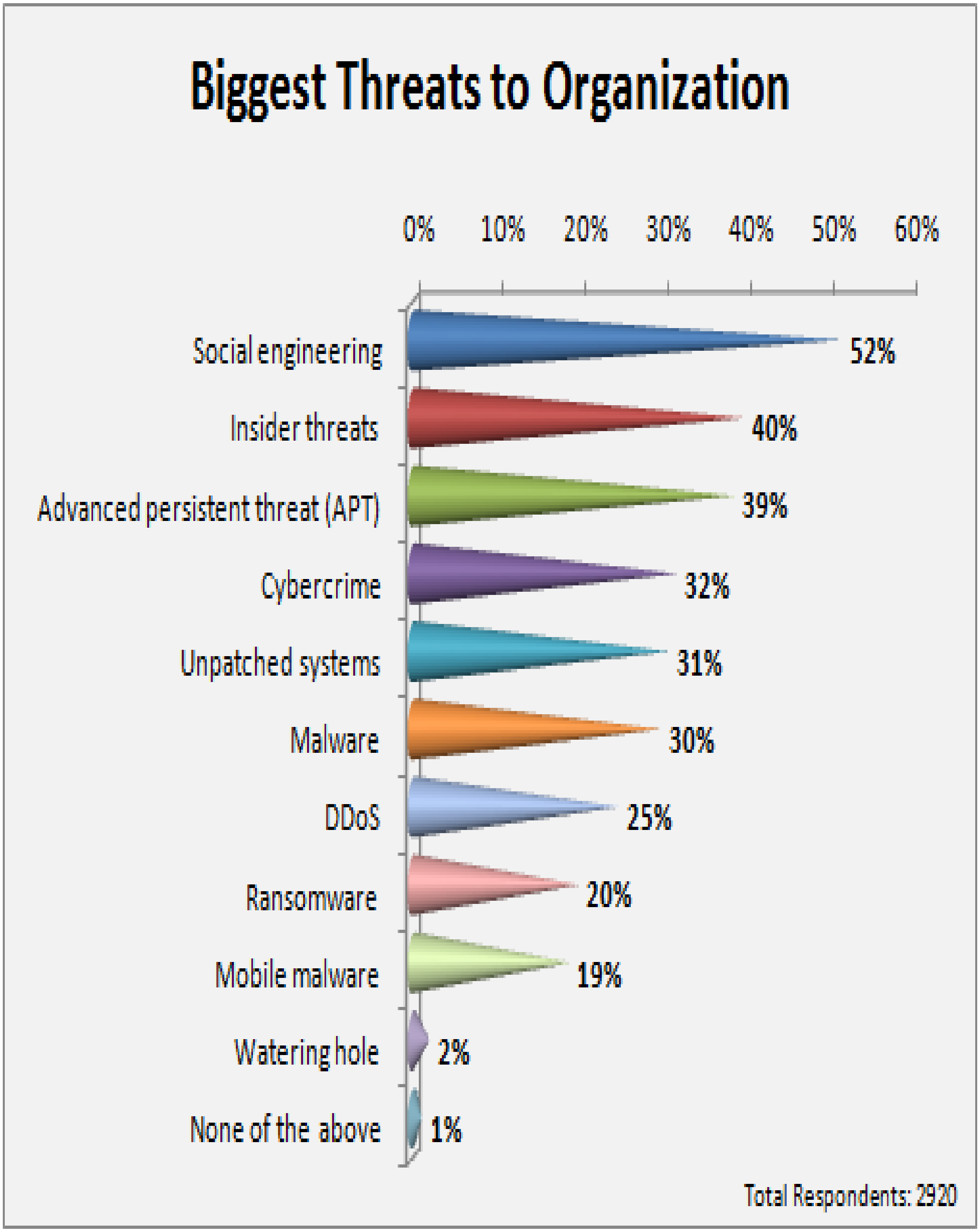


Fig 11: Biggest Threads to Organization

5.1 GENERAL SECURITY ADVANTAGES OF CLOUD BASED SOLUTIONS

i. **Immediate Deployment of Software Patches**: Many software patches address specific security concerns and requirements. Most cloud based solution providers have a term of patch installation specialists who immediately deploy system patches. In this way, the cloud-based systems may have a shorter period of vulnerability after a software patch is released.

ii. **Extended Human-Relation Reach:** Because of their financial strength, cloud-based solutions provider may be able to better vet potential employees who will administer system software. Such vetting may include increased reference checking, security and background checking and periodic screening.

iii. **Hardware and Software Redundancy:** Most cloud-based solutions providers have redundant hardware and software resources they can quickly deploy in an emergency.

iv. **Timelines of Incident Response:** Within a data center, key personnel often perform multiple tasks. A company's security specialist may also be the company's patch administrator. As a result, there are often delays between the start of a security incident and its identification-which may have a catastrophic result. A cloud-based solutions provider, in contrast, likely has experts monitoring systems for intrusion, system utilization, and more. In this way should a security incident occur, the cloud-based solution provider is likely to be more responsive.

v. **Specialists Instead of Personnel:** Again, because of their financial advantage cloud-based solution providers may be better positioned to recruit and hire trained system specialists. A small company that tries to handle its own IT, on the other hand, may have a one-person IT staff-and that employee may have a steep learning curve.

Conclusion

In the fields of cloud computing and information security, data protection is a tough task. The thorough examination of the current answers, however, falls short. In this light a thorough examination of the most effective methods for functionality and pertinent solutions to transfer data securely for data protection in the cloud environment. For each discussed option the most pertinent and sufficient information is highlighted, along with any knowledge gaps and potential future study avenues. The refereed procedures are also subjected to a thorough analysis and comparison. Each technique's applicability is evaluated in light of the surrounding circumstances.

According to the research, no single technique is capable of guaranteeing the data's complete security from all parties involved in the system, whether they are directly or indirectly. Integrating the methods for giving the system total security in the sharing environment will enable the development of a solid solution. Furthermore, it is expected that the exposed analysis will serve as a landmark for upcoming researchers working in the field as well as other emerging applications that require secure data storage and sharing for its protection. This is due to the set of highlights of the addressed remarkable solutions.