Unit-5

Cloud Security

Cloud Security Fundamentals

Cloud security is the first and foremost concern of every industry using cloud services. A cloud vendor must ensure that the customer does not face any difficulties such as loss of data or data theft. There is a possibility that a malicious user can go through the cloud by impersonating a legal user, thereby infecting the cloud services and hence affecting various customers sharing the malicious cloud services.

Cloud Risk

When infrastructure, applications, data and storage are hosted by cloud providers, there is a huge chance of risk in each type of service offering. This is known as cloud risk.

Organizations such as the Cloud Security Alliance (CSA) offer certification to cloud providers that meet their criteria. The CSA's Trusted Cloud Initiative program was created to help cloud service provider enable industry-recommended standards, secure access, compliance management, interoperable identity and follow best practices.

Cloud Risk Division

Cloud Risks can be divided into the following four major categories:

1. Privacy and organizational risks
2. Technical risks
3. Legal risks
4. Other risks

Privacy and organizational Risks

1. Lock-in
2. Loss of governance
3. Compliance challenges
4. Cloud service termination or failure
5. Supply chain failure

Technical Risks

1. **Isolation failure:** Multi-tenancy and shared resources are defining characteristics of cloud computing. This risk category covers the failure of mechanisms separating storage, memory, routing and even reputation between different tenants. Side channel attacks, SQL injection attacks and guest hopping attacks are example of these.
2. **Resource exhaustions :** Cloud service is fully on-demand pay per use service. There is a chance of risk in proper allocation of resources to cloud users.
3. **Cloud provider malicious insider:** Malicious insider is **an insider who intends to cause damage to the organization for personal gain**. The malicious actions of an insider could possibly have an impact on the confidentiality, integrity and availability of all kind of data, IP, all kind of services.

4. **Intercepting data in transit:** The data is vulnerable while it is being transmitted. Data can be intercepted and compromised as it travels across the network where it is out of a user's direct control. For this reason, data should be encrypted when in transit. Spoofing, man-in-the middle attacks and sniffing types of attacks cloud be possible during transfer-related activities.
5. **Insecure or ineffective deletion of data:** When it comes to deleting or completely destroying old data from your computer, laptop, hard drive or other media devices, it is vital to keep safety and security the main priorities. Many people and even companies often use unsafe methods to destroy or erase confidential data. Simply deleting or reformatting your computer may not be secure or safe enough. Continuing to practice poor data destruction methods will inevitably lead to identity theft and data breaches.

6. **Loss of encryption keys:** This includes disclosure of secret keys (e.g file encryption, Customer private keys) or passwords to malicious parties, the loss or corruption of those keys.
7. **Compromise service engine:** Cloud provider rely on specific service engine that is placed on top of physical hardware. For IaaS, this can be hypervisor. For PaaS, it can be hosted application. Hacking the service engine may be useful to escape the isolation.

Legal Risks

1. **Risk from changes of jurisdiction:** Customer data may be kept in serval jurisdictions, some of which may be high risk. If datacentres are located in high-risk countries (e.g. Those that lack of rule of law and have an unpredictable legal framework and enforcement, monocratic police states, states that do not respect international agreements), sites could be attacked by local authorities and data or systems subject to enforced disclosure or seizure.
2. **Licensing risks:** Licensing conditions, such as per-seat agreements and online licensing checks may become unusable in a cloud environment; for example, software is charged at per instances basis so if our cloud based instance increases, the cost of the software also increases exponentially.
3. **Data protection risks** There may be data security branches that are not intimated to the controller by the cloud provider. The cloud customer may misplace control of the data administered by the cloud provider. This issue is increased in the case of multiple transfer pf data.

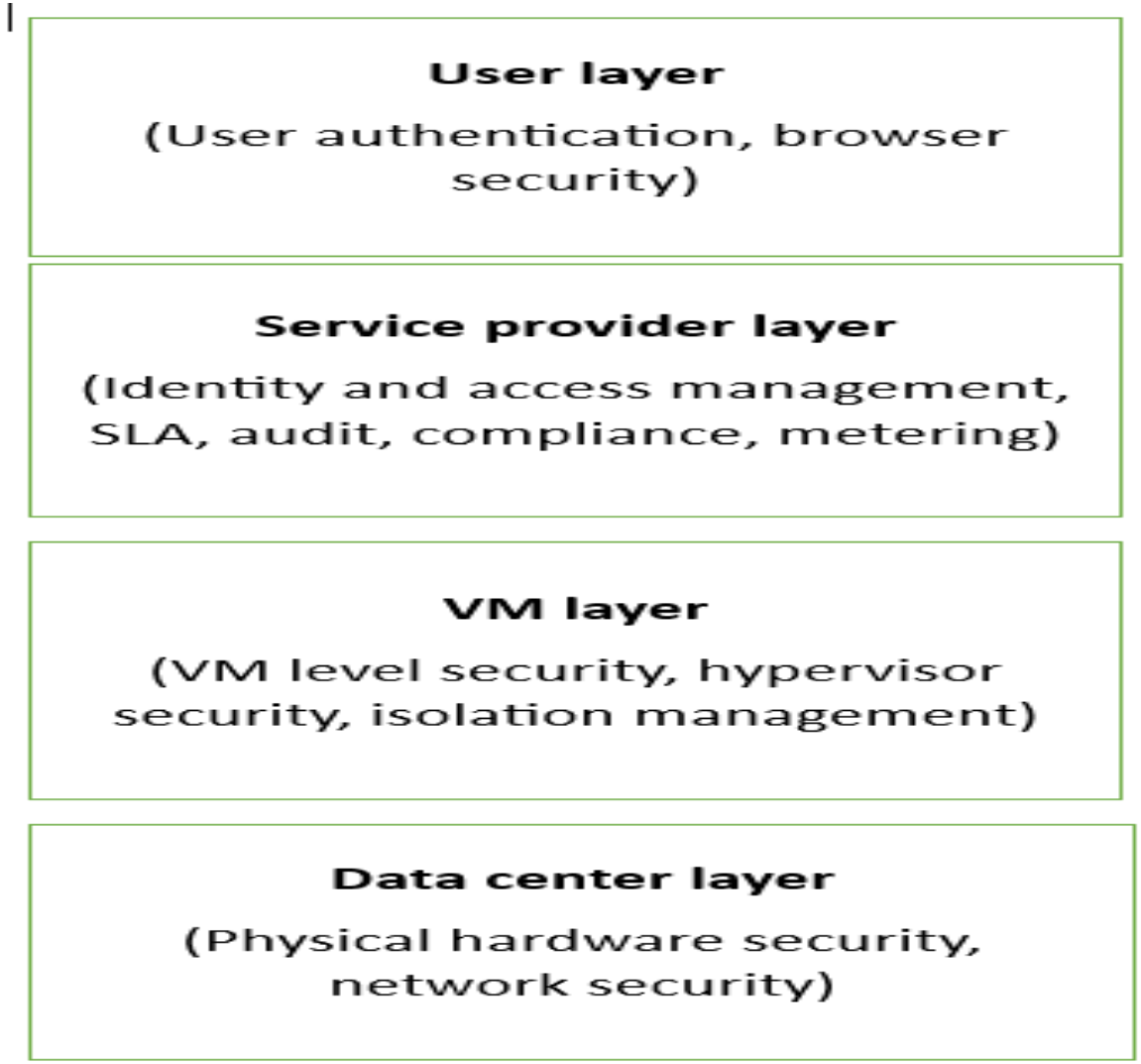
Other Risks

1. **Backup lost or stolen**
2. **Unauthorized access to premises:** Because of inadequate physical security procedures, unauthorized access in datacentres is possible. Generally, cloud providers have large datacentres; therefore, physical control of a datacentre must be stronger because the impact of a breach of this issue could be higher.
3. **Theft of computer equipment:** This risk is mainly related to the datacentre, only authenticated person must be allowed to enter in physical datacentres and dual authentication mechanism should be followed to accesses those machines.
4. **Natural disasters:** Natural disasters are possible any time so there must be perfect disaster recovery plan.

Cloud Computing Security Architecture

Architecture view of the security issues to be addressed in a cloud computing environment for providing security to the customer. This architecture defined four layers on the basis of cloud computing services categorization.

Cloud Computing Security Architecture



- **Data Centre Layer:** This layer is related to traditional infrastructure security concerns. It consists of physical hardware security, theft protection, network security and all physical assets security.
- **VM Layer:** This layer involves VM level security issues, VM monitoring, hypervisor-related security issues and VM isolation management issues.
- **Service provider layer:** This layer is responsible for identity and access management, service level agreement (SLA), metering, compliance and audit- related issues.
- **User layer:** This is the first layer of user interaction. It is responsible for user authentication and authorization and all browser- related security issues.

VM Security Challenges

1. Communication between VMs or between VMs and the host:

VMs serve some key requirements for any organization such as the following:

- Consolidation of different services into one physical computer.
- Providing a general hardware platform to host multiple operating systems.
- Sharing one physical computer resource among multiple companies or organizations.

2. VM escape:

VMs allows us to share the resources of the host computer and provide isolation between VMs and their host.

In an ideal situation, any program that runs under the VM should not communicate to any other program inside that or any other VM, but because of some architecture limitations or some other bugs, software affect this isolation.

It may so happen that a program running inside a VM can totally bypass the VM layer and acquire full access to the host system. Such a situation is known as VM escape. Because of the host's privileged position, the result may be a total collapse in the security model of the system.

3. VM monitoring from the host:

It is not normally considered a limitation or a bug when one can start monitoring, changing or communicating with a VM application from the host. In this case, the host itself starts controlling; therefore, the host requires more strict security environment compared to each individual VM. The host can affect VMs behaviour in the following ways, although it depends on the kind of VM technology being used.

- Start, stop, pause and restart VMs.
- Monitor and configure resources available to the VMs, including CPU, disk and network usage of VMs.
- Monitor the applications running inside the VM.
- View, copy and possibly modify the data stored on the VM's virtual disks.

4. VM monitoring from another VM:

The hypervisor memory is implemented properly then individual VM protection takes place automatically. It will not disturb other VM's memory address space. Because VMs do not have direct access to the host file systems, VMs should not be able to directly access the virtual disk of each other's VM on the host machine.

If network traffic is more complicated then there could be an issue with isolation depending on how the network connections are set up with the VMs, but if there is a dedicated physical channel for each host VM, then guest VMs should not be able to sniff each other's network packets.

There could be the case of a virtual hub also, if the VM uses a virtual hub for connecting all VMs host machine, then guest VM may sniff the packets of the host VM or other guest VMs using ARP poisoning or some other spoofing technique. Virtualization technology must ensure all possible preventions to such attacks.

5. Denial of service:

Because various computing resources like CPU, memory, network and hard disk are shared among multiple VMs and host machine. This may create a denial of service attack against another VM.

This can be avoided by limiting the access of VM resources. There are many virtualization techniques that are used for restricting the allocation of resources to individual VMs. If proper virtualization configuration is implemented, the host machine can prevent denial of service attack among hosts and guest VMs.

6. External modification of a VM:

In a business application scenario, user's VMs have the privilege of accessing employee databases through a secured application. Database security is more critical in a virtual environment. Database is placed inside a secured VM environment so that any external user is not allowed to access the database outside of the application. If a VM where database is installed becomes accessible from outside because of a malicious attack, then the database can be corrupted or modified and the system trust can be broken.

This secure VM should be executed by digitally signing every VM and validating the signature before execution. The signing key should be used very carefully and never be placed anywhere else, otherwise it can be compromised.

7. External modification of the hypervisor:

Because the hypervisor is mainly responsible for the enablement of virtualization while making the process of more self-protected and secure VM, it does not affect the working of any underlying hypervisor. Therefore, the first thing is to protect the hypervisor from any external unauthorized access and changes.

8. Mixed trust level VMs:

Enterprises must take care of mission critical-related information while leveraging the benefits of virtualization. After applying some self-protection system and some external security mechanism such as integrity checking, file monitoring, log assessment, firewall protection and antivirus detection, the VM cab be more secure in mixed environments.

9. Resource contention:

Whenever some resource-consuming operations like malware or antivirus scanning, files and patch updates are executed on VMs, the results of these operations produce high loads on the systems and hamper server applications and VDI environments.

To avoid such situations, each VM requires additional significant memory footprint because just like traditional architecture, the antivirus must be installed on each operating system and the same kind of protection is required for each VM too.

More virtualization-sensitive technology is needed for optimal resource utilization and increasing VM performance so that dedicated antivirus and file scanning should not affect the memory footprint on the virtual hosts.

Unit-5 (Part-2)
Cloud Database

Contents

- Cloud Database- Operational Model for Cloud Database, Types of Cloud Database

- Cloud File System- Distributed File System Basics, Concept of GFS and HDFS, Comparison of Features

Cloud Database

Cloud database is a database that runs on a cloud computing platform like Amazon EC2, Rackspace and GoGrid. There are two ways to deploy a database- users can either run the database inside a secured virtual machine (VM) or subscribe for particular database services managed by a cloud service provider. Currently, there are some SQL-based and some NoSQL-based database offerings.

Operation model for cloud database:

1. **VM Image:-** Cloud platforms allow users to purchase VM instances for a limited time. A cloud provider facilitates more security for running databases inside a VM. If users have their own VM image, then they upload it and run the database inside that or do so through preinstalled databases. Oracle, for example, provides preinstalled image with the Oracle database 11g for Amazon EC2 instances.
2. **Database as a service:-** Some cloud platform and infrastructure service providers offer database services just as other services offerings, in which case we do not need to launch any instance or individual VM for database installation. All database licensing, updating and configuration are managed by the cloud provider. Application owners have to, each month, pay-per-use of database volume. AWS provides many data-base services offering to their customers including relational database services(RDS) and NoSQL services such as Amazon RDS, Amazon DynamoDB, Amazon SimpleDB and Amazon Redshift.

   The traditional application owner prefers RDS and in RDS, users have many choices such as MySQL, Oracle, SQl Server or PostgreSQL database engines. All enterprise licensing issue and updates are taken care of by the provider.

Architectural and common Characteristics

- **Fast Deployment**: Cloud databases are the perfect choice when you urgently need a database, as they can be up and running in minutes. Cloud databases eliminate the need to purchase and install hardware and set up a network.
- **Accessibility**: Users have quick access to cloud databases remotely through the web interface.
- **Scalability**: You can expand cloud database storage capacity without disruptions and meet the requirements. Cloud database scalability is seamless due to DBaaS implementation, which is a major benefit for growing businesses with limited resources.
- **Disaster Recovery**: Data backups are regularly performed on cloud databases and kept on remote servers. These backups enable a business to stay online in cases of natural disasters, equipment failure, etc.

- **Lower Hardware Costs**: Cloud database service providers supply the infrastructure and perform database maintenance. Hence, companies invest less in hardware and have fewer IT engineers for database maintenance.
- **Value for Money**: Many DBaaS solutions are available in multiple configurations, allowing companies only to pay for what they use and turn off services when they don't need them. Cloud databases also save money by not requiring operational costs or expensive upgrades.
- **Latest Tech**: Cloud database providers upgrade infrastructure and keep it updated with new tech. This brings significant savings as companies don't have to allocate funds on new tech or staff training.
- **Security**: Most cloud database providers encrypt data and invest in the best cloud security solutions to keep the databases safe. Although there is no impenetrable security system, it is a safe way to protect data. Since cloud database providers use automation to enforce the best security practices, there is less room for human error compared to using on-premises databases.

Types of Cloud Databases

Many cloud providers offers RDS nowadays. Some popular and most adopted RDS across the globe are as follows:

1. **Amazon relational database service:** Amazon RDS is very popular and widely adopted Web service. It looks like other AWS services and provides easy management consoles for operating RDS on cloud. Amazon RDS is a highly cost-efficient and secured service. Currently it supports Oracle, SQL Server, MySQL and PostgreSQL database. Amazon RDS specifically offers two types of RDS instances.
    - On-demand instances: An on-demand instance offering is a pay-per-use instance with no long-term commitment.
    - Reserved DB instances: Reserved DB instances give the flexibility of one-time payment for the DB instance if the database usage is predictable. There also an offer of 30%-50% price cut over the on-demand price.

2. Google cloud SQL: Google cloud SQL is a MySQL database service that is managed by Google, and the entire management, data replication, encryption, security and backups are handled by Google's cloud infrastructure. Google claims maximum availability of its data because its data centers are located across every region of the world.

3. Heroku Postgres: Heroku Postgres is a relational SQL database offered by Heroku. It is accessible through all programming languages supported by Heroku. It basically provisioned as an add-on service. Heroku Postgres offers fully reliability of services, which means around 99.99% uptime and 99.999999999% durability of data. One of the advance features of Heroku Postgres is Dataclips, which enables users to send the results of the SQL query via the URL.

4. HP cloud relational database for MySQL: HP cloud RDS automate application deployment, configuration management and patch-up task database. It currently supports command line interface (CLI). It also provides database snapshot facility in multiple availability zones for providing more reliability. It is also built atop an OpenStack-based MySQL distribution, which provides database interoperability from one cloud provider to other.

5. Microsoft Azure SQL database: Earlier it was known as SQL Azure. It is the most important component of the Microsoft Azure cloud service; however, it can be operated as a standalone cloud database also. The database can be synched easily with other SQL server databases within the cloud infrastructure of the company or organization. With Microsoft Azure SQL database, the performance of database can be predicted irrespective of whether the service chosen is basic, standard or premium.

6. Oracle database cloud service: Oracle database cloud offers two options for users: one is a single schema-based service and another is fully configured Oracle database installed virtual machine. Oracle database can be quickly provisioned, and the user can spin up a database instance with just a few clicks. It also provides flexibility in the management option: self managed service or fully managed by Oracle.

7. Rackspace cloud databases: Rackspace cloud databases are based on open standards. These Currently support MySQL, Percona and MariaDB databases. Rackspace cloud provides high database performance using container-based virtualization. It provides automated configuration, which reduces operational costs and team effort. Rackspace cloud is built on top of an open source technology like the OpenStack cloud platform.

Limitation with Existing Database

Following are some of the key limitations that became the reason behind the birth of NoSQL databases. Traditional databases are unable to:

1. Store data in TB/PB; even a good processor cannot process millions of rows.
2. Process TB of data on a single machine.

Types of NoSQL Database

1. **Key-value store:** Based on table keys and values (e.g. AWS DynamoDB).
2. **Document-based store:** Document-based database stores records that are made of tagged elements (e.g. MongoDB, CouchDB).
3. **Column-based store:** Data divided into multiple columns and every storage block contains data of each column (e.g., Apache HBase, Cassandra).
4. **Graph-based store:** A network graph storage that uses edges and nodes for storing data (e.g. Neo-4)

Distributed File System Basics

Distributed file system (DFS) is basically used for storing huge amount of data and provides accessibility of stored data to all distributed clients across the network. The objective of the DFS is to provide a system for all the geographically distributed users as a common file system for data sharing and storage.

An Internet search engine is the most common example of DFS, which is used for indexing millions of Web pages. There are a number of DFS that solve this problem in different ways. Some popular file systems are:

1. Andrew file system (AFS)
2. Network file system (NFS)
3. Microsoft distributed file system (DFS)
4. Apple filing protocol (AFP)
5. Google file system (GFS)
6. Hadoop distributed file system (HDFS)

Concept of GFS

Google invented and implemented a scalable DFS to handle their huge internal distributed data exhaustive applications and named it the Google File System. In 2002-03, Google launched its file system based on DFS architecture but added some advance features that are driven by Google's unique workload and environment.

Google File System Architecture

A cluster of a Google file system contains a single master and multiple chunk servers that are associated with many clients. The master holds the metadata of chunk servers. All the data processing happens through these chunk servers. The client first contacts the master and retrieves the metadata of the chunk server, which is then stored in the chunk servers. So the next time, client directly connects to the chunk servers.

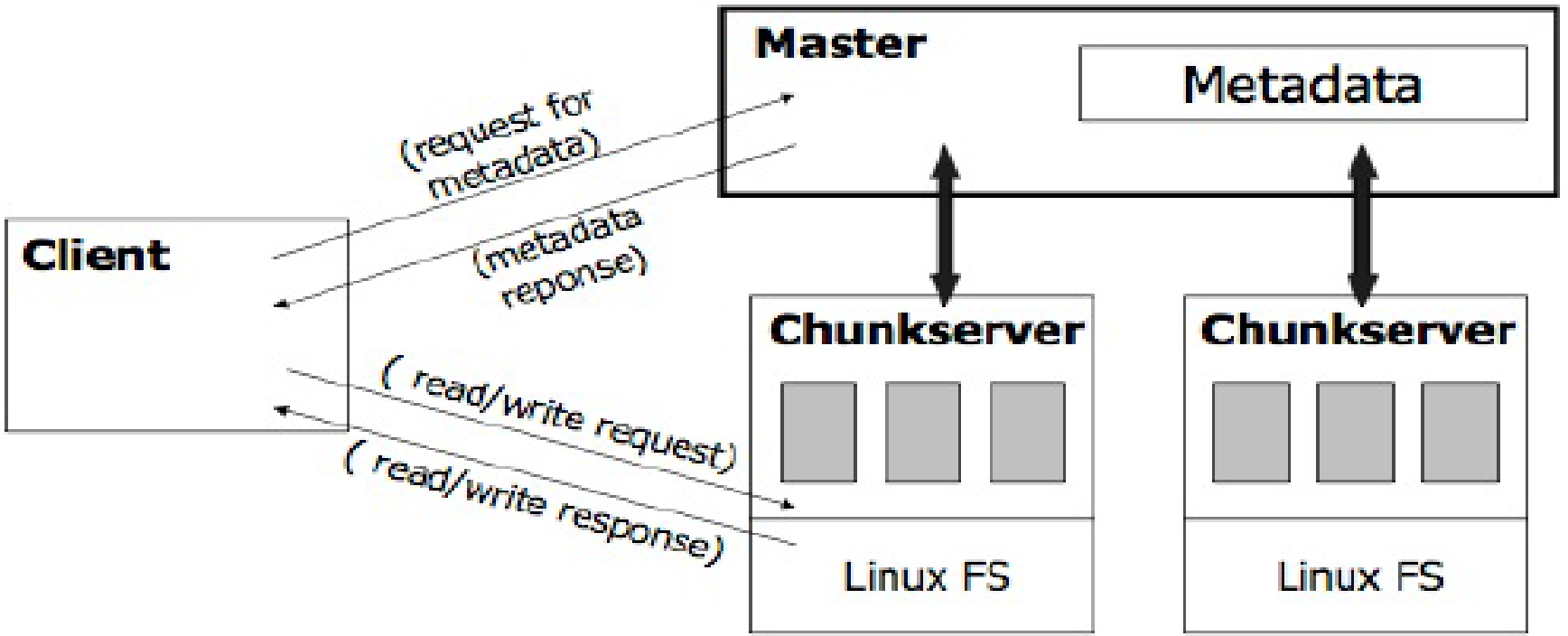

Master
Metadata
Client
(request for metadata)
(metadata reponse)
(read/write request)
(read/write response)
Chunkserver
Chunkserver
Linux FS
Linux FS

Figure 1

Following a are the details of each component of GFS:

1. Chunk: A chunk is very similar to concept of block in a file system, but chunk size is larger than the traditional file system block. The block of chunk is 64 MB. This is specifically designed for the Google environment.
2. Master: Master is a single process that runs on entirely separate machine for security purposes. It only stores metadata-related information, chunk location, file mapping information and access control information. The client first contacts the master for information about metadata and then connects to that particular chunk server.
3. Metadata: Metadata is stored in the memory of a master, therefore, master operations are much faster. Metadata contains three types of information:
   - Namespaces of file and chunk
   - Location of each chunk
   - Mapping from file to chunk

Concept of HDFS

HDFS is a DFS based on GFS that provides high throughput access to application data. It uses the commodity hardware with the expectation that failures will occur and provides portability across heterogeneous hardware and software platforms. HDFS is acquired by Hadoop Apache open source project, which is very popular these days for its ability to handle big data.

The Hadoop core consists of two modules:

1. Hadoop distributed file system: Used for storing huge amount of data.
2. MapReduce programming mode: Used for processing of large set of data.

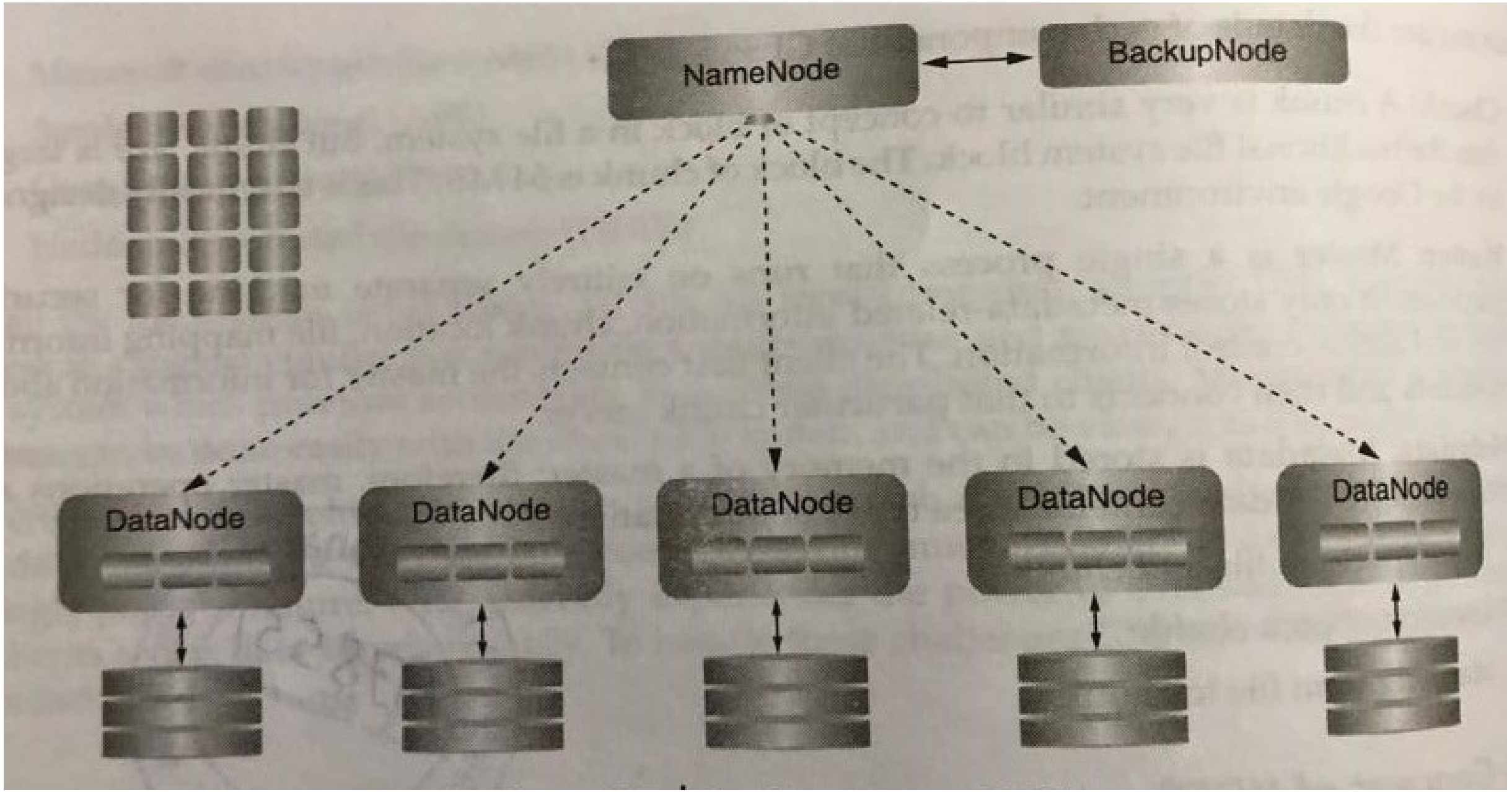
Architecture of HDFS

The working architecture of HDFS is almost similar to GFS.

An HDFS cluster consists of multiple commodity machines that can be classified into the following three types:

1. Name node (runs on master machine)
2. Secondary name node or backup node (runs on separate machine)
3. Data node (runs on slave machine)

The working of an HDFS is the same as master slave architecture. Here the master is the name node that contains the metadata of the cluster, but the processing occurs through data nodes. The client first connects to the metadata and receives information about the data node and the next time directly connects to the data node. GFS works the same way as well.


NameNode
BackupNode
DataNode
DataNode
DataNode
DataNode
DataNode

Comparison of features

Hadoop Distributed File System HDFS	Google File System GFS
Cross Platform	Linux
Developed in Java environment	Developed in C,C++ environment
Initially it was developed by Yahoo and now its an **open source Framework**	It was developed & still owned by Google
It has Name node and Data Node	It has Master-node and Chunk server
128 MB will be the default block size	**64 MB** will be the default block size
Name node receive heartbeat from Data node	Master node receive heartbeat from Chunk server
Commodity hardware are used	Commodity hardware are used
‘’Write Once and Read Many” times model	Multiple writer , multiple reader model
Deleted files are renamed into particular folder and then it will removed via garbage	Deleted files are not reclaimed immediately and are renamed in hidden name space and it will deleted after three days if it’s not in use
Edit Log is maintained	Operational Log is maintained
Only append is possible	Random file write possible