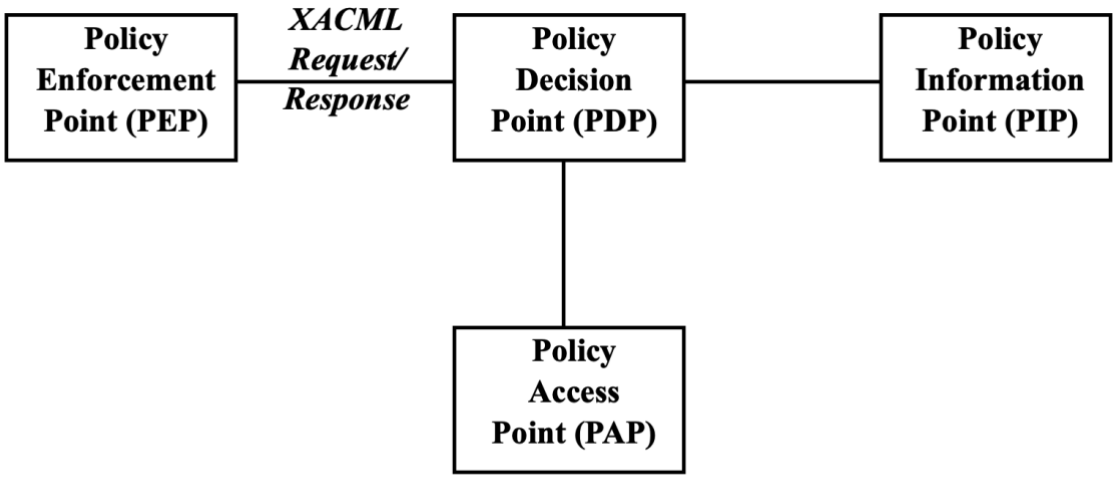
GXS230001 SUMMER 2024 EXAM - 1
GAURAV SHARMA

1 (a) Describe XACML and SAML (b) Describe Security for Web Services?

a) XACML: XACML stands for eXtensible Access Control Markup Language.XML is often known to define its own tags and document structures of web pages through XHTML and as a result, is used widely in storing and transmitting data.
XACML is a Markup Language, but it serves a very different purpose. XACML is a specific markup language. Its usage mainly includes defining access control policies in a computer system.
It allows organizations to create and manage complex rules for determining who can access what resources under what conditions. XACML's architecture includes components like the Policy Administration Point, Policy Decision Point, and Policy Enforcement Point, which work together to evaluate and enforce access decisions. Thus, XACML comes in handy when there are multiple systems involved and we need a standard through which we can define access control.

1. XAML is platform-independent, application-independent, OS independent.
2. Can cater to needs of an organization because it can express complex policies, and implement hierarchical roles, time-bound access, and component- based access control.
3. XACML is more finely grained as it considers objects, subjects, and environments for a module/attribute/component for a given role.
4. XACML can also be looked upon as a request-response protocol. Components of XACML:

- Policy Administration Point (PAP) – creates policies for security and stores it in the appropriate repository.
- Policy Decision Point (PDP) – evaluates access using policies.
- Policy Enforcement Point (PEP) – This will enforce the decisions made by PDP.
- Policy Information Point (PIP) – Assists PEP in enforcing PDP.



Security Assertion Markup Language is abbreviated as SAML:-
The important idea here is much like a web application session, wherein we would want to allow a user to obtain access to some collection of web pages using a single set of credentials for the life of the session. Shuffling around the authentication information—usually in the form of a token—is how SAML accomplishes this.
Thus, the data is protected from any unauthorized access by having the token validated for every page—in fact, it is checked for every microservice/API call made for some page.
JWT Authorization token (OAuth 2.0) is one example of SAML authentication. In the other words, it can be visualized as an access token-supplying identity provider, IDP.
The targeted application is generally hosted by the service provider and IDP maintains the directory for users along with their data. It basically exchanges User Attribute data between SP and IdP.
It appears that systems communicate authorization and authentication data using SAML. As this follows a standard process, it is highly advisable to integrate it with microservices and other applications.
SAML provides single-point authorizations through its three constituents — Assertion, Attributes, and Authorization.
The constituents of SAML are as follows:

1. Identity Provider (IdP): The entity responsible for finding and issuing a valid access token.
2. Service Provider (SP): If the token's IdP is verified, SP will examine it and provide the user access.
3. The SAML Assertion is an XML-based document that contains rights, authentication, and the user's identity.
4. SAML Protocol: This can be thought of as an IdP and SP mapping of rules for access control.
5. Metadata: Contains information on the endpoints, public keys, and component configurations that are involved.

b) Web services security is one of the fundamental elements in contemporary digital infrastructure, aimed at safeguarding data and communication during web-based applications. Given that web services may often exchange data using XML, protecting these documents is critical. Web service security handles significant concerns related to confidentiality, integrity, and authentication.

The major components of web service security are:

1. XML Security: This includes XML Encryption, which addresses document confidentiality, and XML Digital Signatures, addressing document integrity and non-repudiation. These technologies ensure that the XML data is encrypted either in transport or storage and is protected against unauthorized viewing or tampering.

2. WS-SecurityPolicy: Through this framework, the service provider will be able to define clearly and communicate the security requirements. Besides, this specifies how messages will be

secured, the encryption method that will be applied to the message, and what type of credential will be required during authentication.

3. WS-Federation: This is a facility for federation of identity across different security domains. It provides single sign-on and sharing of the identity attributes between trusted partners while improving user experience since it keeps them secure.

4. WS-ReliableMessaging: This specification provides reliable delivery of messages between services even in case of failures in the network or other disruptions that may occur.

5. OAuth and OpenID Connect: It gives standardized ways through which authentication and authorization can be done to secure access to the resources without directly sharing the user's credentials.

6. Transport Layer Security (TLS): Not WS-specific, but pivotal in securing the communication channel between clients and services.

7. API Gateways: They are the middlemen, falling into place to allow further layers of security—rate limiting, request validation, threat detection.

8. IAM—Identity and Access Management: It is the overarching system that manages user identities, roles, and permissions for several services.

These components, when put in place, provide an overall blanket security framework for Web Services. Sensitivity of data is maintained through confidentiality, authenticity, and nonrepudiation. Moreover, access control to protected resources is guaranteed. Security measures must keep evolving with Web Services in order to mitigate newly identified threats and vulnerabilities that emanate from this changing landscape.

2 A) Describe Security for Cloud Computing (B) Describe Aspects of Cloud Governance?
Answer:-
Cloud computing security refers to a multi-dimensional concept for data, applications, and infrastructure related to cloud computing environments. As more and more organizations are shifting to the cloud, making sure that robust security measures are in place at par with the organization becomes very important.
The security framework of cloud computing can be visualized through multiple tiers in the following manner:

Infrastructure Security:
Network Protection: Firewalls, intrusion detection systems, and virtual private networks protect against external threats.
Compute Security: This involves the security of virtualized environments through instance isolation and hypervisor protection. Storage Safeguards: These involve encryption, both in rest and transit, accompanied by secure access mechanisms to data repositories.

Data Protection:
Encryption: It utilizes some of the strong algorithms in the safeguarding of data both during rest and in transit. Data Governance: Policies related to data classification, retention, and disposal are implemented. Privacy Compliance: These put in check adherence to regulations that incorporate GDPR, HIPAA, or CCPA.

Access Management:
It uses multi-factor authentication and single sign-on solutions for identity verification; incorporates principles of least privilege and role-based access control in privilege control; tracks user activities and access patterns to identify anomalies.

Application Security:
Secure Development: Security in the software development life cycle is a part of the best practices. API Protection provides protection to the application programming interfaces from unauthorized access and attacks. Vulnerability Management provides for periodic scanning of vulnerabilities in the software and remediation thereof.

Operational Security:
Incident Response provides for developing processes to identify, respond to, and mitigate security incidents.
Continuous Monitoring: It is real-time monitoring of the cloud environment against threats.
Compliance Management: It maintains the continued conformity of the relevant industry standards and regulations.

Security features are usually provided by the cloud service provider; however, security is also seen as the client's responsibility. This shared responsibility model varies between the service models. It therefore requires a very succinct understanding of who has which responsibility and fine coordination of efforts to be executed between clients and service providers for optimum security in the cloud. Other ways in which this may be done by organizations intent on enhancing their security in the cloud are:

Security third-party tools and services
Regular security audits and penetration tests
Best Practices for Cloud Security Employee Education
Business Continuity and Disaster Recovery Strategy

b) Cloud governance is a critical framework that aligns strategies of cloud computing with overall business objectives. It deals with the development of comprehensive policies to guide the usage of cloud resources so that the adoption of the cloud supports and enhances the company's mission. Hence, strategic alignment is very important in maximizing the benefits accruing from cloud technologies while maintaining control over the operations.

Security and compliance are one of the building blocks forming the basic functionality of cloud governance within any organization. Enterprises should enforce tight security with State-of-the-Art Identity and Access Management, Data Encryption, and Audits Carried Out Regularly. At

the same time, it has to ensure the accomplishment of different industry specifics on regulations depending on the sector and location of business operations.

It is that part of cloud governance concerned with the optimization of costs related to cloud services. This goes hand in hand with designing strategies for the monitoring and control of usages of cloud resources, well-elucidated budgeting procedures, and forecasting techniques on future spending on clouds. Good financial governance prevents surprise costs and ensures value from cloud investments.

Performance has to be continuously monitored for the effectiveness and efficiency of cloud services to be sustained. Organizations need to define KPIs and provide tools for real-time monitoring and analytics. Due to continuous assessment, there can be continual improvement and cloud resource optimization to meet the changing business requirements.

Data governance in the cloud is inevitable for the integrity, privacy, and compliance of organizational data. It should have a completely detailed policy on data classification, data storage, and data retention. Besides, organizations have to resolve issues of data sovereignty with compliance and regulations of data privacy laws, such as GDPR or CCPA, depending on their jurisdictions of operation.

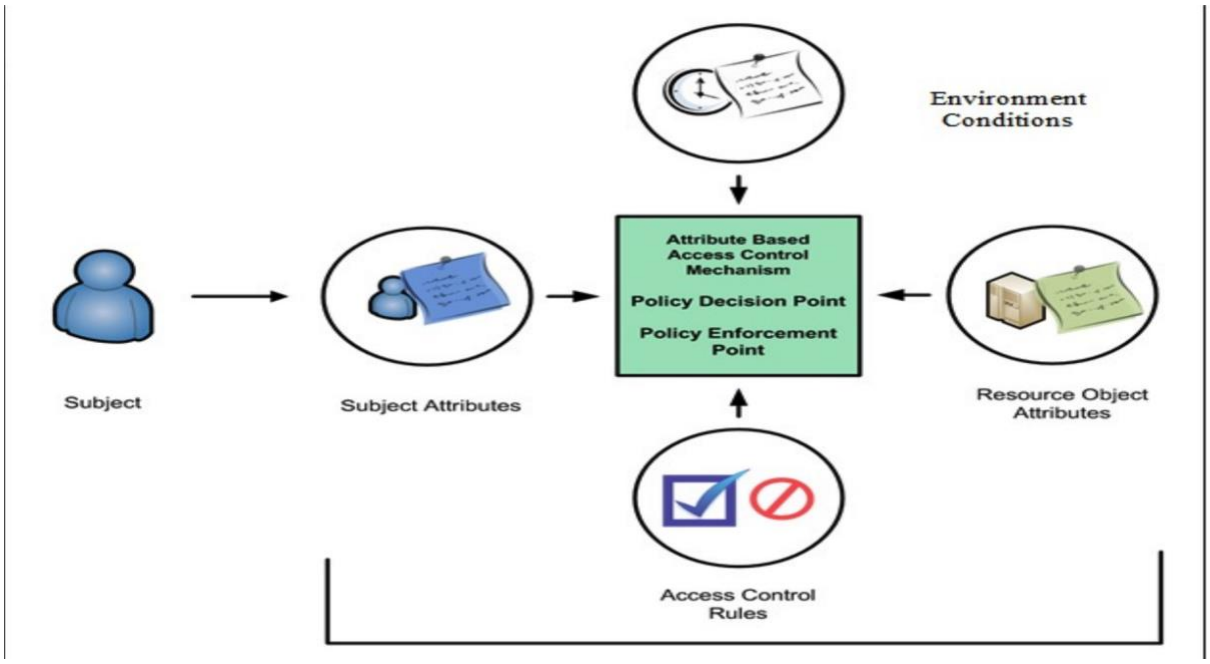
Vendor management makes up an important part of governance in the cloud, more so in multi-cloud or hybrid cloud scenarios. Establishing criteria for the selection and evaluation of cloud service providers, negotiating good SLAs with vendors, and devising strategies to prevent vendor lock-in are all needed. The approach does guarantee flexibility and optimum service delivery.

Successful cloud governance requires attention to skills and training needs. This means the identification and closure of gaps in skills related to cloud technologies, offering continual training and certification programs to IT staff, and developing a culture that supports continuous learning to be able to work effectively within the cloud environment to manage and innovate.

3. (a) Describe how ABAC may be implemented in an organization (b) Describe an approach for Cloud-based Assured Information Sharing ?

ABAC is implemented in any organization by taking a broad strategic view. It would typically start with an organization-wide current assessment of access control mechanisms and identification of requirements in areas that only ABAC can handle. This would be the first phase, and input from various stakeholders—including information technology security teams, compliance officers, and different department heads—would be needed to appreciate holistic access control requirements within an organization.

Now that the ground has been prepared, policy development commences. It is a very critical step whereby fine-grained access control policies are defined by leveraging attributes of subjects, objects, actions, and environmental context. These policies are like the lifeblood of any ABAC system, defining how access decisions will be made. Concurrently, this is where the IT team will work on designing the overall architecture for ABAC with respect to how the system will integrate with other systems and infrastructure.



Core ABAC Mechanism

The next step, often considered the real meat of ABAC, is the management of these attributes. This means the identification of authoritative sources for every attribute, definition of how they will be collected and maintained, and the management of data quality. The organization will need to select appropriate ABAC technologies for implementation. In many cases, commercial solutions can be procured for several of the functions, while others may need custom-developed pieces to meet the organization's needs.

While the technical implementation is ongoing, intense testing by the organization validates the ABAC system for functionality, security, and performance. This phase is important in picking out any issues that may arise and rectifying them prior to full deployment of the system. Meanwhile, the organization develops training programs and documentation to let staff and users work under the new paradigm for access control.

Actual ABAC rollout will often occur in phases: it will initiate with less-critical systems, then move on toward sensitive areas. This approach allows for careful monitoring and adjustments while putting the system into real-world use. During this deployment, feedback from the organization will be collected and used for refinement of policies and processes.

When the ABAC system is rolled out, then comes continuous monitoring, optimization, and maintenance. It contains periodic reviews of policies, updating of attributes, and system enhancement to accommodate evolving security requirements and organizational changes. This kind of organization also lays down the process for constant betterment and continually keeping up-to-date with new developments in the area of ABAC technology and related best practices.

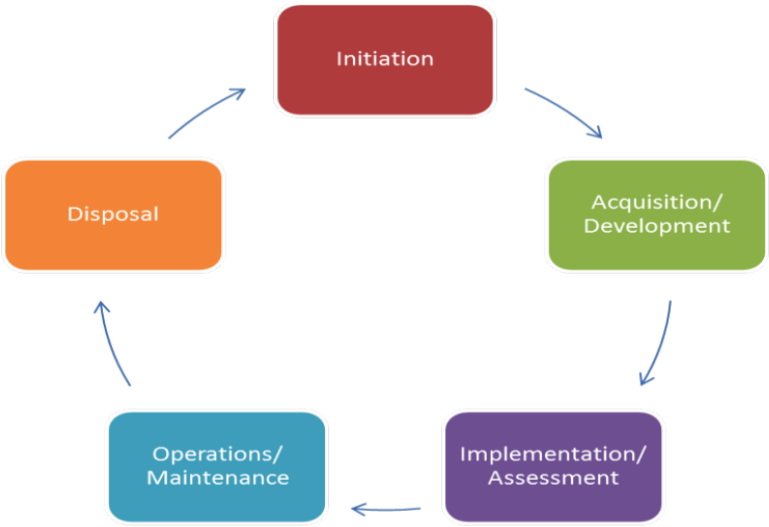


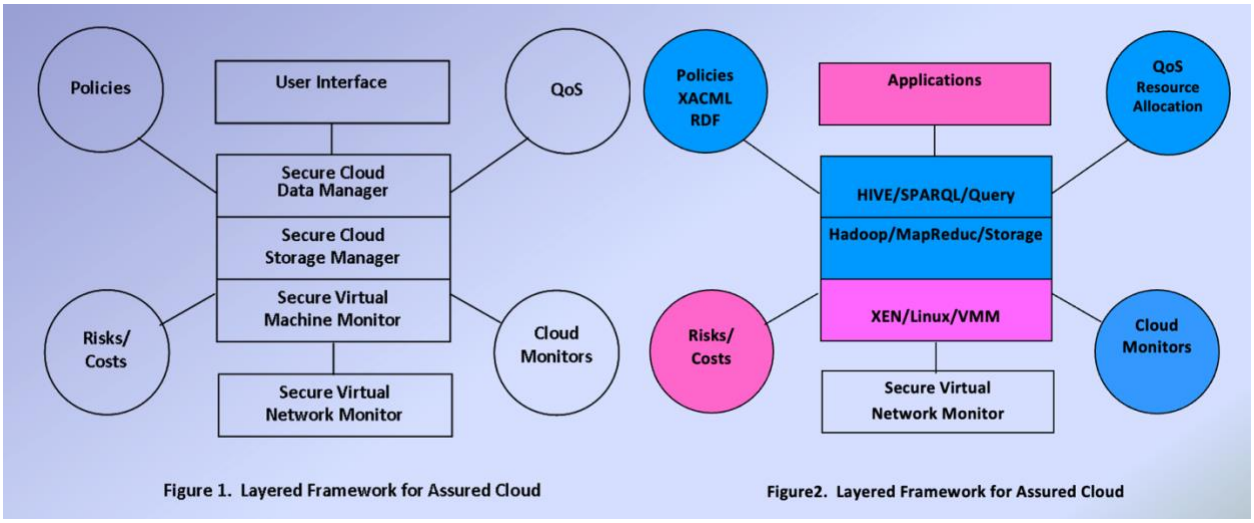
Figure 6: ACM NIST System Development Life Cycle (SDLC)

Following this end-to-end approach will ensure that an organization deploys ABAC effectively and, hence, the development of access control in a fully functional manner while maintaining flexibility in case of changing security landscapes and business needs.

b) Cloud-based assured information sharing is the most critical part of current data management since organizations are moving their operations to the cloud. Certainly, this move brings reduced maintenance costs and high accessibility with scalable infrastructure. This, at the same time, introduces new challenges in assuring the security and privacy of an organization's data.

Thus, the most serious concern regarding cloud-based information sharing models is how to safeguard the confidentiality and integrity of sensitive data, which is transferred from one system to another and from one user to another. Whereas in the case of the traditional approach to storage, which was centralized, now, in a cloud environment, the data must be transferred and stored at multiple locations, making it more vulnerable to various security threats. It is not only the confidentiality of the sensitive information that may be at risk but also its integrity and privacy of communication.

To mitigate these issues, assured information sharing in the cloud must manifest in the form of a multifaceted approach. In general, this is comprised of different distinct elements. First, putting in place robust, policy-based mechanisms of information sharing enables an organization to define and enforce tight rules regarding who can have access to what data and in which kind of situations. Second, risk assessment tools will contribute to finding the vulnerabilities that might exist in the sharing process and build mitigation strategies up front. Thirdly, advanced security measures—such as active firewalls that include intelligent algorithms—can detect and block unauthorized/suspicious access in real-time.



Layered framework for assured cloud computing

All these challenges can comprehensively be solved only in a layered framework for assured cloud computing. At the bottom layer, secure data storage systems like HDFS guarantee protection of data at rest. This can be furthered by access control mechanisms that enable the fine-grained permission management, probably by standards such as XACML. On data processing and querying, tools like Hive for relational data or SPARQL for semantic data could be used, all keeping the data secure while being analyzed.

The top layer for this construct would be the application interface, which deals with the presentation of processed and secured data to the end-user. Within all the layers, there are consistent security policies and encryption protocols that ensure data is always guarded—whether resting, in transit, or in use. It allows organizations to derive the power of cloud computing in ensuring information sharing while keeping tight control over their sensitive data, hence striking a balance between the needs for collaboration and security in the modern digital landscape.

4. Describe an approach for Cloud-based Malware Detection ?

Malware detection in the cloud is challenging due to the distributed and dynamic nature of cloud environments. Traditional methods for malware detection most often do not meet all the requirements needed to effectively identify such malware within these complex systems. Therefore, new identification approaches are necessary in order not to fall behind malicious software—since this scale of infrastructure and its dynamic landscape has come to stay.

This is one of the more interesting strategies for identifying cloud-based malware: using machine learning with real-time data analytics. In a cloud environment, executables and file flows are treated as a continuous stream of data that permits ongoing monitoring and classification. Due to the use of ensemble learning techniques like random forests or gradient boosting, it will learn new patterns and threats. It is a dynamic classification model trained on a very different set of features extracted from files, network traffic, and system behaviors to transparently distinguish

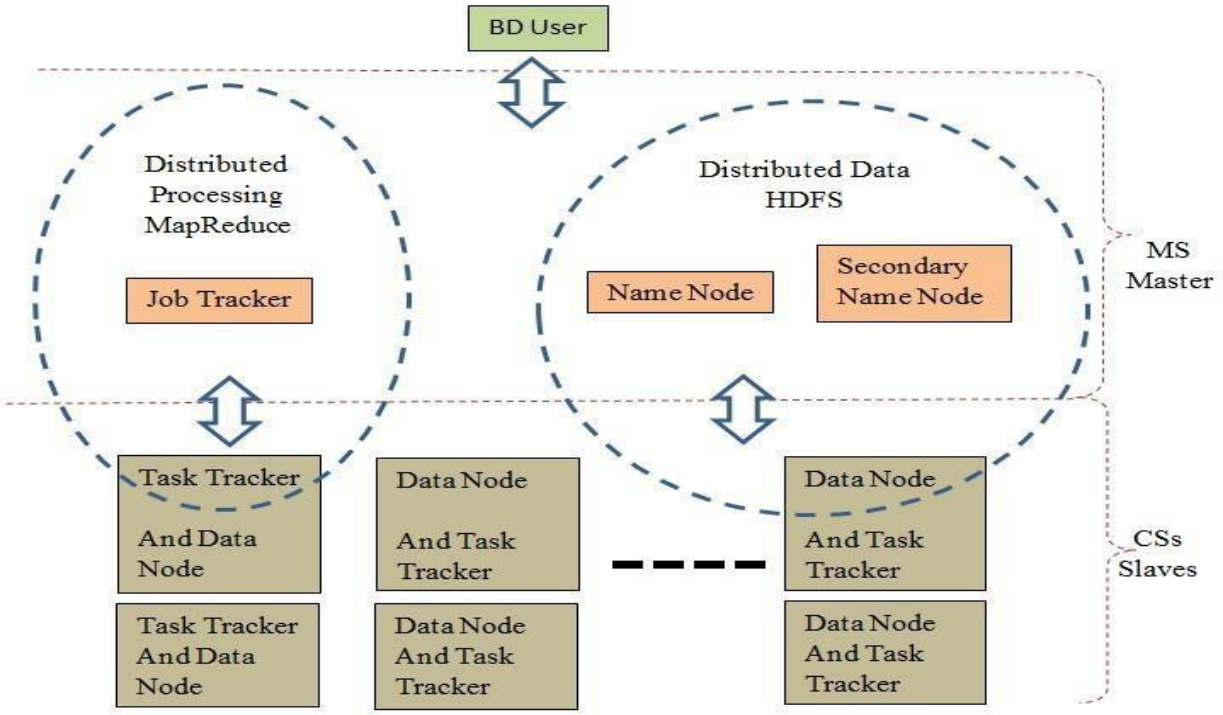
between benign and potentially malicious activities to a very high degree of accuracy that improves over time.

In this approach, sensors are deployed across the cloud infrastructure that will capture the relevant data points. These sensors feed information back to a central analysis engine to process this data stream in real-time. The trained machine learning models are then used by the engine to classify the incoming files and activities, flagging those that may be treated as a potential threat for further investigation. The system allows feedback loops, through which security analysts can validate the decisions made by the model for more accuracy and fewer false positives.

While this approach provides broad benefits of being more scalable and flexible, one must find the edges. With these techniques that today's malware uses to evade detection, it is unlikely to reach a 100% detection rate with any single method. Therefore, this machine learning-based approach should be part of a greater set of measures in the cloud security strategy that includes regular vulnerability assessments and sound access controls and encrypted data storage and transmission.

Any organization, therefore, must consider the regulatory and compliance implications of having such a system in place. Moreover, it must be aware of data privacy regulations and make sure that during the detection process, sensitive information is kept safe. It is through the proper security policies and practices, combined with advanced technical solutions, that organizations will be able to detect and respond to malware threats in cloud computing much more effectively.

5. Describe an Access Control Model for Big Data and the Cloud?



The proposed access control model has considered some of the special challenges big data processing systems are raising, among which are those arising from their ultra-high dimensionality and distributed nature. It attempts to provide secure access control across the Big Data cluster, which typically consists of a Master System (MS) and multiple Cooperating Systems (CSs).
Some important components of this access control model are:

1. SA: This is a sort of agreement between the big data source provider and the MS over security classes of the different types of big data sources. The former facilitates trust and allows for the establishment of a security level for data processing.

2. TCSL: CS List managed by the MS, where CSs are organized according to classes of security defined by SA, to support the MS's decisions related to trusting CSs for specific data items and processes.

3. MSP: MS Access Control Policy, the access control rules to be administered by MS on CSs specifying how CSs are supposed to handle the distributed big data items and processes.

4. CS Access Control Policy, CSP: This policy is maintained at each CS and governs the access to its portions of the distributed big data and to the processes executing at a local CS, based on its processing capacity and security needs.

5. Federated Attribute Definitions, FAD: This is a shared dictionary across the MS and CSs. It ensures that all access control policies get uniformly applied across the cluster.

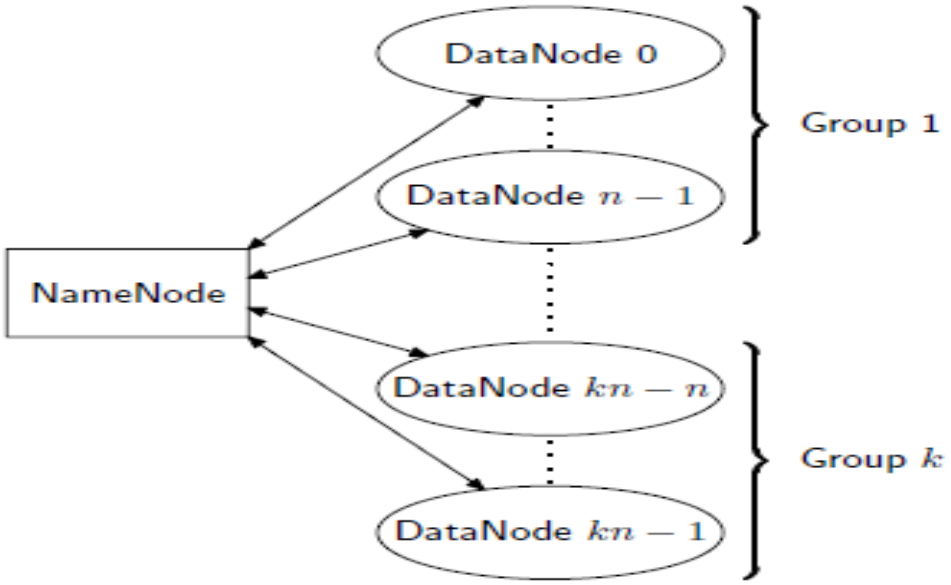
It coordinates these components to enforce access control at the MS and CS levels. If the MS distributes data or processes to a CS, then it will become the subject; big data or required CS resources become the objects. It is for the CSP to determine allowed actions based on the security class of the data, the trust level of the CS, and local resource constraints.

The model solves major challenges of big data access control, including the following:
1. Distributed computing: It introduces a framework for access management on multiple systems.
2. Data fragmentation and redundancy: It still has security because of consistent policies and attributes, even though data is fragmented or redundantly stored across the cluster.
3. Node-to-node communication: The model establishes trust relationships to secure the MS-CSs communication.

It is an envisioned scheme, and a lot of access control mechanisms can be implemented using different specifications. ABAC is a good fit, as it grants flexibility with respect to attributes and policy management. The model focuses on delivering complete access control in big data environments and balancing security needs with the high-performance requirements of big data processing.

6. Describe Security for Hadoop?

Hadoop security, as represented by the Hatman system, is a solution to one of the fundamental challenges: how to ensure the integrity of data and computation in cloud environments. The fundamental problem here is that all cloud systems are vulnerable under compromised nodes, so even one node can potentially taint the integrity of large numbers of distributed computations.



System Architecture

Hatman is a reputation-based trust management system that provides dynamic assurance of node integrity in Hadoop clusters based on output consistency across replicas of jobs. It extends the current Hadoop NameNode—master—with trust information for the DataNodes—the slave nodes—that are stored centrally at the NameNode, but performs most of the computations at DataNodes. This design assures high scalability with a reduced attack surface on the NameNode.

The centerpiece of Hatman's approach rests in job replication and result consistency checking. User-submitted jobs are replicated across different groups of DataNodes; the size of these groups is specified by users to provide both parallelism and a replication factor for security. Results from these replicated jobs are checked for consistency, and consistency checks themselves are implemented as distributed Hadoop jobs. It is this clever design that has used the computing power of the cluster to enhance its own security.

Trust computation in Hatman is done by agreements and disagreements between node results, summarized in a trust matrix. This matrix is used to periodically compute a global trust vector

for all nodes by the EigenTrust algorithm. Thus, it can determine and return to the user the most trustworthy result and therefore filter possibly corrupted data.
It allows several types of activities within it: user-submitted jobs, bookkeeping activities for comparing results and computing trust, and "police activities" — these are dummy jobs submitted for determining node reliability when the load is low. This multifaceted approach will then keep assessing and fine-tuning the trust levels of nodes incessantly.

The Hatman security model assumes that an attacker may compromise DataNodes but not NameNodes, together with the fact that communications between these two are cryptographically protected. It fundamentally focuses on computational integrity violations and does not focus on breaches in confidentiality or denial-of-service attacks.

One of the main strengths of Hatman is that it is highly scalable, allowing it to reap most of the security features that are computationally based. For example, reliability higher than 90% was achieved after only 100 jobs in scenarios when 25% of the nodes were malicious during experiments.

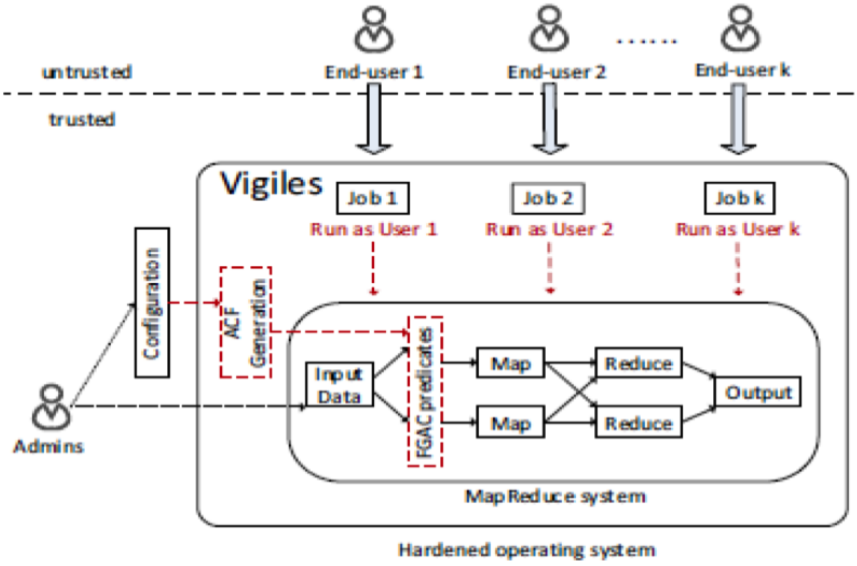
In summary, Hatman represents a sophisticated, data-centric approach to Hadoop security. It holds great promise by providing a scalable solution to the critical challenge of maintaining computational integrity in today's large-scale cloud environments by implementing its security measures in such a way that is distributed as Hadoop itself. Further research will be required to counter increasingly sophisticated attacks and to evaluate performance in larger cloud deployments.

7. Describe Security for MapReduce?

The Vigiles system serves as an example of how security for MapReduce satisfies the crucial requirement for fine-grained access control (FGAC) in massive data processing environments. This method is intended to improve the security of MapReduce systems while maintaining and enhancing their adaptability without altering the underlying source code.

The fundamental idea of Vigiles is to use reference monitors (RMs) to enrich the front-end API of the cloud by rewriting it as a middleware layer using FGAC. These cloud-resident RMs filter data access outputs to stop unwanted access to key-value pairs that are disallowed by policy at runtime. Unlike the coarse file-level access control commonly seen in MapReduce systems, this technique enables the enforcement of complicated security restrictions at a granular level.
The user defined FGAC predicates in Vigiles are implemented as RMs. In so doing, therefore, the predicates can, therefore, apply to a record in any of three ways: through rejection, granting, or modification before the access is granted. This flexibility thus allows elaborative access control policies that can adapt to various data sensitivity levels and difference in user clearances.

Vigiles' system architecture serves as an application firewall separating the underlying OS/MapReduce system from untrusted end users. It wraps the OS/MapReduce system, handles access control filters (ACFs), and authenticates users to require Vigiles for all user activities. This design aids in thwarting numerous attack vectors and illegal access to data.



System Architecture

Vigiles' ACF synthesis and injection procedure is one of its primary features. ACFs are created using aspect-oriented programming techniques and injected into the MapReduce system based on configurations supplied by the admin. To guarantee that every data access travels via the FGAC predicates, this injection takes place at the Record Reader interface level. Vigiles also handles potential security breaches by caging MapReduce jobs in a secure environment. Since it accepts only managed Java bytecode programs, it can employ relatively secure sandboxing techniques to prevent a wide class of security breaches.

It showed such impressive performance, with the overhead of empirical results being only about 1% as compared to implementations that modify the source code of Hadoop. Its high efficiency, modularity, and flexibility make Vigiles a very promising way to implement fine-grained access control in a MapReduce environment.

In conclusion, Vigiles represents a significant step for MapReduce security. It is modular, efficient, and fine-grained without much modification of the underlying MapReduce system. In such a way, the requirements for implementing strong security measures in big data processing setups can be matched with adequate performance and flexibility of systems.

8. (a) Describe Backup and Recovery for the Cloud, (b) Describe Mobile Cloud and the associated security issues?

a) Cloud backup and recovery are core requirements of modern data management strategies, much so in cloud computing. Cloud backup refers to a service where data and applications from the servers of a business are backed up and stored in remote servers. Through the process, businesses can still have access to their files and data even when the system fails, goes out of

service, or experiences other disasters. Basically, this means copying and storing files on another server, probably at another location, which offers an added layer of protection against localized failures.

This is important to note that while the cloud can provide backup services for other systems, the cloud infrastructure itself also requires backup. Cloud service providers should be able to replicate their entire cloud environment—at associate data centers located in different places. This redundancy is critical to ensure continuity of services and integrity of data in case large-scale failures or disasters occur.

Security is paramount during cloud backup. Indeed, measures such as end-to-end encryption are usually put in place by providers during transit and storage. That includes access control policies over modules and data that are backed up, fending off malware attacks, and ensuring that no unauthorized access occurs during recovery. But these security considerations don't apply just to cloud-based backup services; they do to the backup of cloud infrastructure itself.

Cloud recovery makes use of virtualization technologies that let it offer very scalable and automated solutions for data backup and recovery. It encapsulates an entire server—from operating system to applications, patches, and data—and creates servers as a part of virtual servers. Cloud recovery provides rapid failover and failback, hence bringing down the recovery time drastically compared to conventional approaches. It facilitates the restoration of interdependent processes in the correct order and to the right recovery point to minimize business process disruptions.

Cloud DR embodies strategies for backing up applications, resources, and data to a cloud environment. Several benefits are attached to this approach, such as the automation of many processes, quicker scaling regarding business requirements, enhanced protection of corporate resources, and better business continuity. However, tight security has to be maintained in the recovery process, wherein access control policies and prevention of attacks are very essential, and verification has to be made that the recovered data is not accessed by unauthorized parties.

b) Mobile Cloud Computing is a method of delivering mobile applications using cloud computing. It basically shifts complex computational tasks from the mobile to the cloud infrastructures so that more powerful and efficient mobile apps can be built. This approach gains much importance in catering to the expectations of the modern customer—access to applications from any device at any time, remotely.
Some of the major benefits of MCC are: Broader reach due to independence of platforms because cloud-based mobile apps work on any device and under any operating system. It has real-time analysis capabilities as data is centrally stored and processed. The user experience is enriched within many device categories so long as the internet connection is good. Cost effectiveness, under pay-as-you-go models, is another major advantage since on-premises servers will no longer be required.
MCC finds several applications, from interactive experiences like financial tickers and voting applications through social media, commerce and banking applications, and mobile gaming to healthcare solutions. These applications use the cloud to help host data-intensive tasks and provide real-time updates. In MCC, mobile apps send their data requests across the internet to

the cloud servers, which process these requests and respond accordingly. It avails various forms of cloud resources: distant immobile clouds, proximate immobile computing entities, proximate mobile computing entities, and hybrid solutions combining the above-mentioned approaches.

Security Issues: some key points on security in MCC include:

New security challenges:

- The integration of mobile computing with cloud computing introduces new classes of security and privacy challenges.
- Medium Wireless: Communication between mobile devices and clouds is through wireless networks, adding more security issues.
- Data Storage: The data is stored in cloud infrastructure. This raises questions about data locality and privacy.
- It gives rise to new security challenges related to integration among the mobile and cloud technologies. The communication between mobile devices and clouds through wireless networks opens many more security concerns. Questions exist over the locality of data and privacy with the storage of data within a cloud infrastructure.

Existing solutions: Several security solutions are proposed by researchers to counter these threats.
General security measures for clouds:

- Files are stored encrypted.
- Periodic security updates by the cloud service provider
- The use of Artificial Intelligence in searching out vulnerabilities
- Hardware and software firewalls
- Backups of data across multiple servers

Despite all these odds against it, the MCC is usually considered at least a little bit safer than merely storing data locally on some device. Among these different security measures implemented by the providers of clouds are encrypted file storage, frequent security updates, AI-driven vulnerability detection, hardware- and software-based firewalls, and data backups across servers in multiple numbers.

9. (a) Describe two attacks to the Cloud, (b) Describe aspects of Cloud Monitoring ?

a) The enormous volumes of valuable data that cloud-based systems contain, along with their broad usage, have made them increasingly appealing targets for cybercriminals. There are two noteworthy assaults that are serious risks to cloud security:

1. Man in the Cloud Attack:
This is a rather new attack methodology that was developed targeting a user's cloud synchronization token. The process of the attack is as follows:

- Malware is installed on a victim's device from some malicious website or email.
- Once malware has accessed a user's local files, it replaces the user's real cloud synchronization token with one pointing to the attacker's own cloud account.
- The original token is embedded in files that are to be synchronized.

- The victim, unknowingly, uploads their original token to the attacker's account.
- Once done, the attacker can use this token and get access to the actual cloud data of the victim.

The key to preventing this attack is malware prevention on the user's end.

2. Cloud Malware Injection Attack:
This involves:

- The attacker uploads a manipulated copy of one of the instances of the target system's service into the cloud system.
- Some of the service requests to the victim's service are processed within this malicious instance.
- An attacker must realize control over a victim's previously stored data within the cloud system to do this.

This is an attack surface on the service-to-cloud attack surface. The attacker exploits control over the cloud to use privileged access capabilities against the security of the service instance.

Both these attacks underline that there is at least a strong case for robust security measures within cloud environments: malware prevention, secure authentication procedures, and monitoring of cloud resources and access patterns.

b) Cloud monitoring is an important part of resource and service management within a cloud environment. This involves observation and assessment of the cloud environment to ensure that it works in accordance with its prescribed specifications, delivers expected performance, and adheres to all established security policies. Special software tools and techniques are used in monitoring, assessing, and troubleshooting various areas of a cloud infrastructure, including applications, services, and supporting hardware.

The information gathered through cloud monitoring is useful for a myriad of purposes. It can provide notification of problems that could affect the performance or security of the cloud environment, thus allowing administrators to take action to correct those problems before they have an impact. This is how the stability, security, and availability of cloud services are ensured for end-users. Moreover, such monitoring information might be helpful in optimizing resource usage toward better overall efficiency—it could bring potential cost savings.

Hypervisor-based virtualization shifts the focus of cloud monitoring to the hypervisor layer and VMs under its management. It will retain performance metrics on the hypervisor and individual VMs regarding CPU usage, memory consumption, and network throughput. This level of monitoring also covers any underlying physical hardware, virtual storage devices, and virtual networks. Security relies on hypervisor-based monitoring for detecting unauthorized access attempts, potential data breaches, or malware threats. Due to its responsibility for managing and isolating VMs, the hypervisor is a unique and necessary location for both implementing security policies and detecting violations.

For hosted virtualization that includes a guest operating system, cloud monitoring involves observing the host and guest operating system layers. This includes resource utilization—the rate at which the CPU, memory, and disk space are being utilized—on both the host and guest systems; application performance monitoring for each guest OS; and security-related monitoring in terms of threats to the operating system or applications on guest machines. However, hosted virtualization could still be susceptible to security risks at the host level since it deploys the host operating system to oversee VMs. While monitoring tools can detect some security issues and alerting administrators, their ability to intensely view security threats to the guest operating systems is limited.

Hypervisor-based or hosted virtualization monitoring relies on a variety of virtualization technologies applied. Both remain very important in keeping cloud infrastructure performance, security, and availability. Each, however, has special strong points and considerations when managing and securing cloud environments.

10. (a) Describe security for a cloud product (e.g., AWS) , (b) Describe Virtualization aspects of the Cloud ?

a) In the past years, organizations and individual customers have fast adopted cloud-based solutions that help them bring down the maintenance costs by allowing the remote access to data and save on hefty investments in hardware. This has been an extension of distributed computing but it has come with its own challenges. By moving away from centralized storage, data is inherently transferred and stored in new locations.

Security on AWS is very important; it protects sensitive information, helps organizations maintain regulatory compliance, and ensures service integrity and availability.

Some of the key threats to AWS security are:

1. Breaches: Accidental unauthorized access because of credential theft due to phishing or social engineering—this can be controlled with strong password policies and multi-factor authentication.
2. Distributed Denial of Service (DDoS) Attacks: The AWS infrastructure is hit with traffic to knock down services. Mitigation techniques involve AWS Shield, WAF, and setting up auto-scaling groups.
3. Insufficient Permissions or Encryption: This represents that the most sensitive data is not well protected; it opens doors for undesired access and manipulation. Prevention involves implementing strong encryption, access control, and periodical security audit measures.
4. Insecure APIs: Exploiting API vulnerabilities to obtain unauthorized access or control Mitigation strategies include secure coding practices, leveraging AWS IAM, and monitoring of API activity.

AWS has the following security-as-a-service offerings in place:

- Identity and Access Management: Controls over user access to AWS resources
- Network Security: Protection of network infrastructure and traffic
- Encryption Services: Protection of data at rest and in transit.

- AWS Security Hub: Unify security monitoring across AWS accounts.
- Amazon Guard Duty: Continuously detect threats.
- AWS WAF: Protect against common web exploits.
- Amazon Macie: Automatically discover and classify sensitive data.
- AWS Key Management Service: Manage encryption keys.
- AWS CloudTrail: Log API calls for visibility into account activity.
- AWS Trusted Advisor: Receive security recommendations and best practices.

In summary, security at AWS deals with providing protection for confidentiality, integrity, and availability of data. AWS has detailed methods for access control, encryption, monitoring, and compliance auditing. It provides a very wide selection of security services, making strong protection of cloud environments quite easy to achieve.

b) Virtualization in cloud computing has increased due to various advantages like reduced infrastructure cost, better options of scaling on-demand, enhanced resource use, and enhanced security. Virtualization is one such method that creates a virtual version of something physical. It is basically access to the storage, processing capacity, and safety features of another terminal from one's own terminal, just as a remote desktop is obtained.

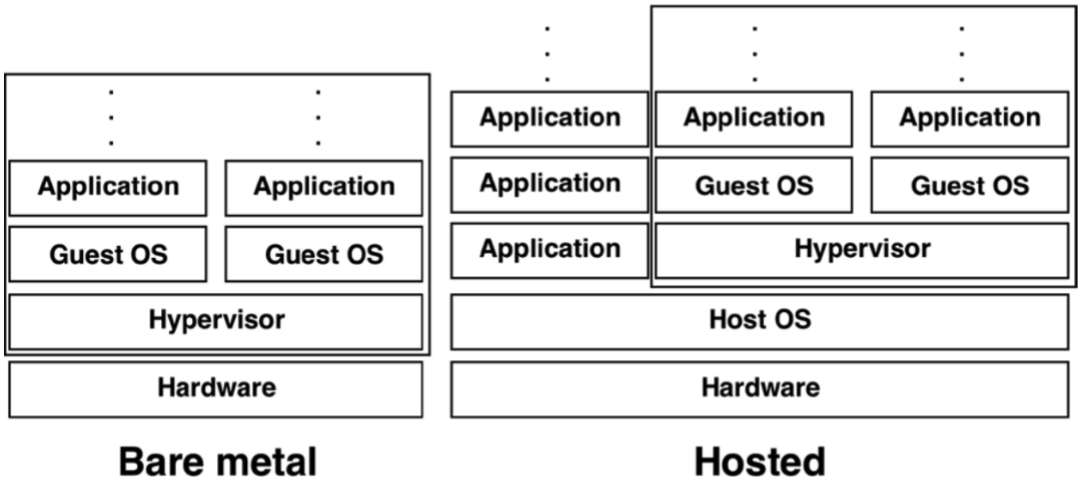


Figure 2-1. Full Virtualization Architectures

Virtualization in cloud computing allows the running of many VMs on a single physical server. The VMs function with their Private Operating Systems and Resources for Faster, Core, and Scalable Allocation, Configuration, and Management According to Workload Demands.

Types of Virtualizations

1. Application Virtualization

   Application virtualization simply runs individual applications or APIs from a remote server and makes them available to use on a local device. For example, the JVM allows a Java application to run on any device without modification, while online PDF converters do not require software to be installed locally to process files.

2. Operating System Virtualization

   Operating system virtualization simply means providing the operating systems virtually. It simply means that more than one independent OS instance can run on a physical machine. For example, tools like CompTIA's virtual environments allow you to run Linux on a Windows device, thereby giving the flexibility to switch over to the other whenever required.

3. Full Virtualization

   Full virtualization makes use of a hypervisor, which is the interface software layer between the physical hardware and the host operating system. With this, it enables the running of several OS instances independently on a single physical machine. Every operating system is made to run without insecurity and interference from the rest.

Types of Full Virtualization:

Bare Metal Virtualization: Here, the hypervisor is run directly on the physical hardware without any host OS. It is often integrated into the system firmware and provides an efficient robust virtualization environment.
Hosted Virtualization: In this case, the hypervisor runs on top of an existing conventional host operating system like Windows, Linux, or MacOS. With this configuration, a VM can run and be managed in conjunction with normal applications. This allows users to interact simultaneously with both virtual and non-virtual environments for ease of use.

Virtualization can further be classified based on computing environment architecture:

Single Server Virtualization: It will run multiple VMs on a single physical server efficiently, ensuring appropriate resource usage and flexibility for various applications and services.

Multi-Server Virtualization: This distribution of VMs over multiple physical servers would improve redundancy, load balancing, and overall resiliency.

In general, cloud virtualization increases resource efficiency by guaranteeing flexibility in managing workloads and enhancing security; it becomes part of the modern infrastructure in cloud computing.