RGPVNOTES.IN

Program : **B.E**

Subject Name: **Cloud Computing**

Subject Code: **CS-8002**

Semester: **8th**

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in

Downloaded from be.rgpvnotes.in

Subject Notes
CS 8002 - Cloud Computing

Unit-4

Cloud Security Fundamentals

Cloud evolution can be considered synonymous to banking system evolution. Earlier people used to keep all their money, movable assets (precious metals, stones etc.) in their personal possessions and even in underground lockers as they thought that depositing their hard earned money with bank can be disastrous. Banking system evolved over the period of time. Legal and security process compliances protected by Law played a big role in making banking and financial systems trustworthy. Now, people hardly keep any cash with them. Most of us carry plastic money and transact digitally. Cloud computing is also evolving the same way.

Robust cloud architecture with strong security implementation at all layers in the stack powered with legal compliances and government protection is the key to cloud security. As Banks didn't vanish despite frauds, thefts and malpractices, cloud security is going to get evolved but as much faster rate. Digital world has zero tolerance for waiting! Evolution is natural and is bound to happen.

Cloud is complex and hence security measures are not simple too. Cloud needs to be secured at all layers in its stack. Let's briefly look into major areas.

At infrastructure level: A sysadmin of the cloud provider can attack the systems since he/she has got all the admin rights. With root privileges at each machine, the sysadmin can install or execute all sorts of software to perform an attack. Furthermore, with physical access to the machine, a sysadmin can perform more sophisticated attacks like cold boot attacks and even tamper with the hardware.

Protection measures:

1. No single person should accumulate all these privileges.

2. Provider should deploy stringent security devices, restricted access control policies, and surveillance mechanisms to protect the physical integrity of the hardware.

3. Thus, we assume that, by enforcing a security processes, the provider itself can prevent attacks that require physical access to the machines.

4. The only way a sysadmin would be able to gain physical access to a node running a costumer's VM is by diverting this VM to a machine under his/her control, located outside the IaaS's security perimeter. Therefore, the cloud computing platform must be able to confine the VM execution inside the perimeter, and guarantee that at any point a sysadmin with root privileges remotely logged to a machine hosting a VM cannot access its memory.

5. TCG (trusted computing group), a consortium of industry leader to identify and implement security measures at infrastructure level proposes a set of hardware and software technologies to enable the construction of trusted platforms suggests use of "remote attestation" (a mechanism to detect changes to the user's computers by authorized parties).

At Platform level:

Security model at this level relies more on the provider to maintain data integrity and availability. Platform must take care of following security aspects:

1. Integrity
2. Confidentiality
3. Authentication
4. Defense against intrusion and DDoS attack
5. SLA

At Application level:

The following key security elements should be carefully considered as an integral part of the

SaaS application development and deployment process:

1. SaaS deployment model
2. Data security
3. Network security
4. Regulatory compliance
5. Data segregation
6. Availability
7. Backup/Recovery Procedure
8. Identity management and sign-on process

Most of the above are provided by PaaS and hence optimal utilization of PaaS in modeling SaaS

is very important.

Some of the steps which can be taken to make SaaS secured are:

- Secure Product Engineering
- Secure Deployment
- Governance and Regulatory Compliance Audits
- Third-Party SaaS Security Assessment

At Data level:

Apart from securing data from corruption and losses by implementing data protection mechanism at infrastructure level, one needs to also make sure that sensitive data is encrypted during transit and at rest.

Apart from all the above measures, stringent security process implementation should also be part of making cloud secure. Periodic audits should happen. Governing security laws should be amended with advent in technologies, ethical hacking and vulnerability testing should be performed to make sure the cloud is secure across all layers.

Cloud Security Devices

It doesn't matter what size you are when it comes to protecting your network. Big company, small company, and startup: Hackers will still want your information and they'll still stealthily poke holes in your network wherever they can.

You need to get security measures in place and fast.

That's why "security as a service" companies have become vital for anyone looking to deploy security for everything from documents to your entire business.

Security as a service can be loosely described as a "software as a service" security tool that doesn't require any on-premise hardware or software distribution. Unlike older security tools, like anti-virus software that needs to be installed on every single computer on your network, it's almost plugged and play — you click a button (and likely put in some credit card information) and suddenly you've got major security resources at your fingertips.

These security services aren't the same as an on-premise firewall that watches the network from a physical appliance attached in your data center. But these products promise to protect you from malware, help you keep track of who signs into your network, monitor all your other cloud applications such as Salesforce and Google Docs, and more.

RGPVNOTES.IN

Small businesses can benefit from this kind of distribution model because it doesn't require a big IT or security teams to get it up and running. Of course, you're trusting a lot of your security to another company, but in reality these security-focused third parties have more resources (read: time and money) to focus on security than you do.

So what are the best security-as-a-service products out there? We talked to experts in the security community to compile this initial list of the top-tier providers.

Here are our top 6 in no particular order:

- **VentureBeat**

It is researching cloud platforms and we're looking for your help. We're starting with marketing specifically marketing automation. Help us by filling out a survey, and you'll get the full report when it's complete.

- **Qualys**

Qualys secures your devices and web apps, while helping you remain compliant through its cloud-only solution — no hardware or software required. The company analyzes threat information to make sure nothing gets in your system. If some malware already happens to be there, it will give you the steps to fix the problem. Beyond that, Qualys will verify that the issue has been fixed. It scans any and all web apps you use for vulnerabilities as well, keeping your data safe while you head out in the wonderful world of SaaS, IaaS, and PaaS. In the future, Qualys plans to create a cloud-only firewall to even further protect your websites from harm.

- **Proofpoint**

When we talk about attack vectors — holes in the network where bad guys can get in — email pops out as one of the weakest links. Proofpoint focuses specifically on email, with cloud-only services tailored to both enterprises and small to medium sized businesses. Not only does it make sure none of the bad stuff gets in, but it also protects any outgoing data. Proofpoint further promises that while it stores that data to prevent data loss, it does not have the keys to decrypt any of the information.

- **Zscaler**

Zscaler calls its product the "Direct to Cloud Network," and like many of these products, boasts that it's much easier to deploy and can be much more cost efficient than traditional appliance security. The company's products protect you from advanced persistent threats by monitoring all the traffic that comes in and out of your network as a kind of "checkpost in the cloud." But you don't have to filter all that traffic in from one central point. You can monitor specific, local networks as well given the flexibility of the cloud. Zscaler also protects iOS and Android devices within your company, which can then be monitored through its special mobile online dashboard.

- **CipherCloud**

CipherCloud is here to secure all those other "as a service" products you use, such as Salesforce, Chatter, Box, Office 365, Gmail, Amazon Web Services, and more. It promises to protect that prized company data you're just giving away to these services, as well as your communications, and more. It does this through many of the means we've already seen including encryption, traffic monitoring, anti-virus scans, and more. It also provides mobile security support.

- **DocTrackr**

RGPVNOTES.IN

DocTrackr is a security layer that sits on top of file sharing services such as Box and Microsoft Sharepoint. It is built on the idea that once you send a document out of your system, it is truly out of your hands: People can save it, change it, send it, and more and you've lost control of it. DocTrackr aims to stop that from happening. It lets you set user privileges for each person you share a document with. It further tracks everyone who opens the file, so you know who's looking at your stuff — and you can even pull documents back, effectively "unsharing" them, if you want.

Secure Cloud Software Requirements

1. **Authentication**: The process of providing identity is called authentication. Most computer system uses a user ID and password combination for identity and authentication. You identity yourself using a user ID and authenticate your identity with a password. Let's look at some examples of authentication from everyday life: at an automatic bank machine, you identify yourself using bank card, when you use a credit card etc.

2. **Single sing on**:Single sing on (SSO) is a session/user authentication process that permits a user to enter one name and password in order to access multiple applications. The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session.

3. **Delegation**: If a computer user temporarily hands over his authorizations to another user then this process is called delegation. There are two classes of delegation.

Delegation at authentication level and delegation at access control level

4. **Confidentiality**: confidentiality assures you that cannot be viewed by unauthorized people. The confidentiality service protects system data and information from unauthorized disclosure. When data leave one extreme of a system such as client's computer in a network, it ventures out into a non-trusting environment. So, the recipient of data may not fully trust that no third party like a cryptanalysis or a man-in-the middle has eavesdropped on the data.

5. **Integrity**: It assures you that data has not changed without your knowledge (the information cannot be altered in storage or transit sender and receiver without the alteration being detected).The integrity can be used in reference to proper functioning of a network, system, or application.

6. **Non-repudiation**: Repudiation is the denial by one of the entities involved in a communication of having participated in all or part of the communication. Such denial can be prevented by non-repudiation. Non repudiation allows an exchange of data between two parties in such a way that the parties cannot subsequently deny their participation in the exchange.

7. **Privacy**: Internet privacy involves the desire or mandate of personal privacy concerning transaction or transmission of data via the internet. It also involves the exercise of control over the type and amount of information revealed about person on the internet and who mat access said information personal information should be managed as part of the data use organization. It should be manage from the time the information is conceived through to its final disposition.

8. **Trust**: Organization's belief in the reliability, truth, ability, or strength of someone or something. Trust revolves around 'assurance' and confidence that people, data entities, information or processes will function or behave in expected ways. Trust may be human to human, machine to machine, human to machine or machine to human. At a deeper level, trust might be regarded as a consequence of progress towards security or privacy objectives.

9. **Policy**: The term policy is high-level requirement that specify which access is managed and who, under what circumstances, may access what information. A security policy should fulfill many purposes. It should protect people and information, and set the rules for expected behavior by users, system administrators, management, and security personnel.

10. **Authorization**: Authorization is the act of checking to see if a user has the proper permission to access a particular file or perform a particular action. It enables us to determine exactly what a user is allowed to do. Authorization typically implemented through the use of access control. While determining what access will be provided to the parties to whom we have provided authorized access, there is an important concept we should consider, called the principle of least privilege.

11. **Accounting**: accounting services keep track of usage of services by other services/ users so that they can be charged accordingly.

12. **Audit**: Audit services keep track of security related events.

Cloud Computing Security Challenges

Clouds are everywhere these days. They are often cheaper, more powerful, compatible with single sign-on (SSO) and often accessible via a Web browser. There are four main types of clouds: on-premises, or clouds hosted by the customer; off-premises, or clouds hosted by a vendor; dedicated, which are clouds used only for a particular tenant; and shared, a cloud where resources are spread among many tenants.

These categories are more descriptive than public and private clouds. There are also virtual machine-based clouds where several separate computing environments can be used, versus bare-metal, where each compute node is a separate physical machine.

Threats to the Cloud

The first and most dangerous threat in any IT system is the insider threat. It’s especially hard to defend against because users, and particularly administrators, have usually been granted some degree of trust. Technological countermeasures can usually be circumvented if the user has the right level of access. This is why it is critical for organizations to have an efficient off boarding process so that disgruntled released employees do not have access to the systems.

Side-channel threats occur when an attacker has the ability to obtain information from another tenant’s node by measuring some side effect of the system’s use. These have been popularized in the research community but, to IBM X-Force’s knowledge; have not been seen in the real world.

Perhaps the most dangerous real-world threat is the loss of authority over the cloud control interface. We aren’t talking about the provisioning portal but rather the administrative interface of your enterprise’s cloud. Think of it as a control console for your cloud nodes.

In the right situation, this can lead to a complete loss of integrity, confidentiality and availability. Note that the attack here is against the interface’s Web server, or a cross-site scripting (XSS) or cross-site request forging (CSRF) attack against the administrator’s Web browser.

Make sure the interface’s Web server is up to date and that the interface does not have any XSS or CSRF vulnerabilities. These are just good security practices in general and are not unique to the cloud. If you use SSO, be sure your security assertion markup language (SAML) implementation follows the recommended specification.

Additionally, use two-factor authentication. Note that this is good practice for restricting access to any sensitive servers and data.

Additional Risks to Cloud Environments

There is a somewhat rare attack called virtual host confusion. It is often seen with content delivery networks and shared platform-as-a-service (PaaS) clouds. This attack can allow for server impersonation under the right circumstances. Once again, the X-Force team is not aware of this being exploited in the wild. For more information, read the paper “Network-based Origin Confusion Attacks against HTTPS Virtual Hosting.”

This attack is from the same group that identified Logjam, FREAK, SLOTH and others. To prevent this attack, never use certificates for more than one domain. Avoid using wildcard certificates and carefully configure TLS caching and ticketing parameters to be different for every Web server. Finally, make sure your domain fallback page is an error page.

RGPVNOTES.IN

Shared data and computations on shared (typically off-premises) clouds can be exposed in the right circumstances. This particularly applies to MapReduce operations. To prevent this leakage, consider dedicated clouds, where there is a lesser chance of malicious actors having a presence.

Never make the mistake of assuming that on-premises or dedicated clouds need not be secured according to industry best practices. These clouds are often considered a more valuable target by attackers.

Finally, there is shadow IT, or the inability of IT to monitor the activities of the user. This happens when the user's client is connected to a cloud with an encrypted connection. In that case, the user can interact with the cloud and perhaps perform unauthorized actions. To combat this, consider federating. Monitor your logs to see which applications are in use and use a proxy to intercept cloud traffic. You can also use an analytics engine and create relevant rules at your endpoint device.

Overcoming Challenges

In general, what can be done to improve cloud security? Always follow the best security practices whether you are a tenant or a provider, such as tracking new vulnerabilities and attacks against components of your cloud. If you are a cloud provider, do background research on entities that wish to join your environment.

If you are a tenant, always understand your cloud model and compensate for any weaknesses inherent in that type. Be sure to support TLS 1.2 access. This ensures stronger cryptography and is the latest secure protocol for connections to Web servers.

RGPVNOTES.IN

Both providers and tenants should institute regular vulnerability scanning as frequently as is feasible. They should also lock IP addresses so only authorized networks are able to access your cloud or site. If this is not possible as a provider, then be sure to employ strong authentication and access controls.

As a provider, make logs relevant to your tenants available. This complements the tenant's own logging.

As a tenant, make sure all software is up to date. PaaS providers need to do the same with their environments. In one of the most important measures, tenants must encrypt data. This is critical for data protection, but be sure to implement cryptography correctly. There are solutions available to minimize the ciphertext reduplication problem.

Virtualization Security in Cloud Computing

2011 ended with the popularization of an idea: Bringing VMs (virtual machines) onto the cloud. Recent years have seen great advancements in both cloud computing and virtualization On one hand there is the ability to pool various resources to provide software-as-a-service, infrastructure-as-a-service and platform-as-a-service. At its most basic, this is what describes cloud computing. On the other hand, we have virtual machines that provide agility, flexibility, and scalability to the cloud resources by allowing the vendors to copy, move, and manipulate their VMs at will. The term *virtual machine* essentially describes sharing the resources of one single physical computer into various computers within itself. *VMware* and *virtual box* are very commonly used virtual systems on desktops. Cloud computing effectively stands for many computers pretending to be one computing environment. Obviously, cloud computing would have many virtualized systems to maximize resources.

Keeping this information in mind, we can now look into the security issues that arise within a cloud-computing scenario. As more and more organizations follow the "Into the Cloud" concept, malicious hackers keep finding ways to get their hands on valuable information by manipulating safeguards and breaching the security layers (if any) of cloud environments. One issue is that the cloud-computing scenario is not as transparent as it claims to be. The service user has no clue about how his information is processed and stored. In addition, the service user cannot directly control the flow of data/information storage and processing. The service provider usually is not aware of the details of the service running on his or her environment. Thus, possible attacks on the cloud-computing environment can be classified in to:

1. **Resource attacks:**

   These kinds of attacks include manipulating the available resources into mounting a large-scale botnet attack. These kinds of attacks target either cloud providers or service providers.

2. **Data attacks**: These kinds of attacks include unauthorized modification of sensitive data at nodes, or performing configuration changes to enable a sniffing attack via a specific device etc. These attacks are focused on cloud providers, service providers, and also on service users.
3. **Denial of Service attacks**: The creation of a new virtual machine is not a difficult task, and thus, creating rogue VMs and allocating huge spaces for them can lead to a Denial of Service attack for service providers when they opt to create a new VM on the cloud. This kind of attack is generally called virtual machine sprawling.
4. **Backdoor:** Another threat on a virtual environment empowered by cloud computing is the use of backdoor VMs that leak sensitive information and can destroy data privacy.
5. Having virtual machines would indirectly allow anyone with access to the host disk files of the VM to take a snapshot or illegal copy of the whole System. This can lead to corporate espionage and piracy of legitimate products.

With so many obvious security issues (and a lot more can be added to the list), we need to enumerate some steps that can be used to secure virtualization in cloud computing.

The most neglected aspect of any organization is its physical security. An advanced social engineer can take advantage of weak physical-security policies an organization has put in place. Thus, it's important to have a consistent, context-aware security policy when it comes to controlling access to a data center. Traffic between the virtual machines needs to be monitored closely by using at least a few standard monitoring tools.

After thoroughly enhancing physical security, it's time to check security on the inside. A well-configured gateway should be able to enforce security when any virtual machine is reconfigured, migrated, or added. This will help prevent VM sprawls and rogue VMs. Another approach that might help enhance internal security is the use of third-party validation checks, preformed in accordance with security standards.

Cloud Security Architecture

Architecting appropriate security controls that protect the CIA of information in the cloud can mitigate cloud security threats. Security controls can be delivered as a service (Security-as-a-Service) by the provider or by the enterprise or by a 3rd party provider. Security architectural patterns are typically expressed from the point of security controls (safeguards) – technology and processes. These security controls and the service location (enterprise, cloud provider, 3rd party) should be highlighted in the security patterns.

Security architecture patterns serve as the North Star and can accelerate application migration to clouds while managing the security risks. In addition, cloud security architecture patterns should highlight the trust boundary between various services and components deployed at cloud services. These patterns should also point out standard interfaces, security protocols (SSL, TLS, IPSEC, LDAPS, SFTP, SSH, SCP, SAML, OAuth, Tacacs, OCSP, etc.) and mechanisms available for authentication, token management, authorization, encryption methods (hash, symmetric, asymmetric), encryption algorithms (Triple DES, 128-bit AES, Blowfish, RSA, etc.), security event logging, source-of-truth for policies and user attributes and coupling models (tight or loose).Finally the patterns should be leveraged to create security checklists that need to be automated by configuration management tools like puppet.

In general, patterns should highlight the following attributes (but not limited to) for each of the security services consumed by the cloud application figure 4.1:

Logical location – Native to cloud service, in-house, third party cloud. The location may have an implication on the performance, availability, firewall policy as well as governance of the service.

Protocol – What protocol(s) are used to invoke the service? For example REST with X.509 certificates for service requests.

Service function – What is the function of the service? For example encryption of the artifact, logging, authentication and machine finger printing.

Input/Output – What are the inputs, including methods to the controls, and outputs from the security service? For example, Input = XML doc and Output =XML doc with encrypted attributes.

Control description – What security control does the security service offer? For example, protection of information confidentiality at rest, authentication of user and authentication of application.

Actor – Who are the users of this service? For example, End point, End user, Enterprise administrator, IT auditor and Architect.

Follow us on facebook to get real-time updates from RGPV

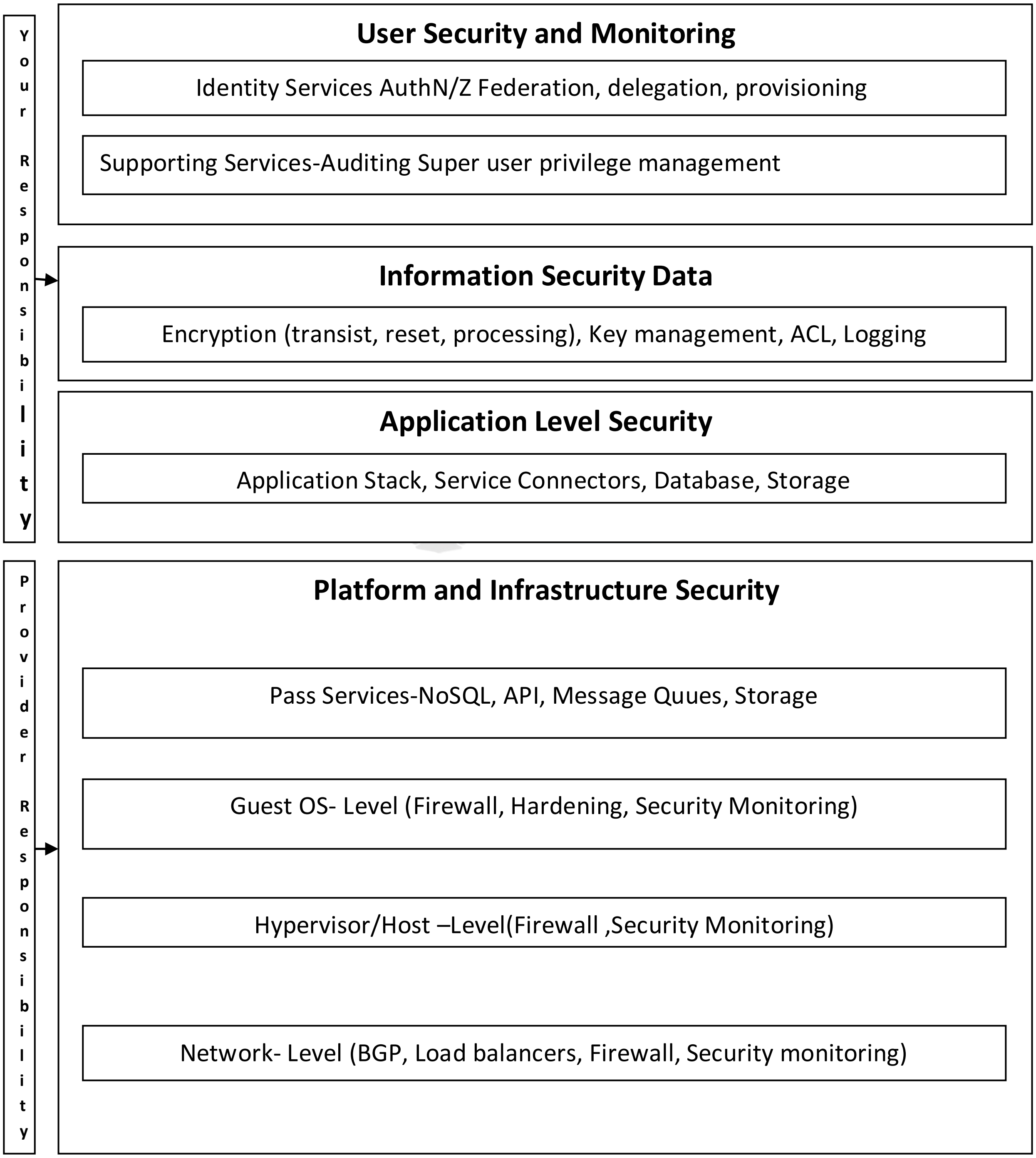
Your Responsibility
User Security and Monitoring
Identity Services AuthN/Z Federation, delegation, provisioning
Supporting Services-Auditing Super user privilege management
Information Security Data
Encryption (transist, reset, processing), Key management, ACL, Logging
Application Level Security
Application Stack, Service Connectors, Database, Storage
Provider Responsibility
Platform and Infrastructure Security
Pass Services-NoSQL, API, Message Quues, Storage
Guest OS- Level (Firewall, Hardening, Security Monitoring)
Hypervisor/Host –Level(Firewall ,Security Monitoring)
Network- Level (BGP, Load balancers, Firewall, Security monitoring)

Figure: 4.1 Cloud Security Architecture

Web Resources:

https://aws.amazon.com/security/introduction-to-cloud-security/

https://www.fortinet.com/solutions/enterprise-midsize-business/cloud-security.html

https://www.solutionary.com/managed-security-services/cloud-security/

http://www.csoonline.com/article/3053159/security/cloud-security-challenges.html

Follow us on facebook to get real-time updates from RGPV

RGPVNOTES.IN

We hope you find these notes useful.

You can get previous year question papers at https://qp.rgpvnotes.in .

If you have any queries or you want to submit your study notes please write us at rgpvnotes.in@gmail.com

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in