FLEXMIND

Cloud Security 101

Sanjeev Kumar Jaiswal

Sanjeev Jaiswal (jassi)

- 14+ years of Experience
- Security Architect, Tesco
  - ➤ Security Head in Lifesight for 2.5 years
  - ➤ India Lead, AppSec Team in Epam
- Application Security and
- Cloud Security
- Programming: Perl, Python
- Areas of Interest: Learning and teaching concepts on DevSecOps, Cloud Security & Security Automation

FLEXMIND

What we will cover

- For whom this session is (awareness session)
- Brief of Cloud Computing
- Cloud Security Overview
- What covers under cloud security
- Job profile categories
- Learning references
- What’s Next

FLEXMIND

Key Audience

- College Students
- Freshers (0-2 years)
- Want to switch into Cloud Security
- Interested in Cloud Security
- Curious what’s there in Cloud Security

FLEXMIND

What we will cover

- Quick recap of Cloud Computing - 5 mins.
- Service model and Deployment model - 5 mins.
- Why we need Cloud Security - 5 mins.
- Cloud Security Fundamentals - 30 mins.
- What’s Next - 5 mins.
- Q&A - 10 min.

FLEXMIND

Cloud Computing is the use of computing services like servers, storage, databases, networking, software, analytics, intelligence and many more over the Internet (“the cloud”)

FLEXMIND

Why we need cloud computing at all?

- Better Availability
- Higher durability
- Secured?
- Economical
- Compliant
- Go live in a minute

FLEXMIND

Advantages of Cloud Computing

- Pay as you go
- Resilient
- Scalable
- Economical
- Enhance Productivity, Performance and
- Security

Cloud Computing Deployment Model

FLEXMIND

Public Cloud

- Elasticity
- Utility Pricing
- Leverage Expertise

Private Cloud

- Total Control
- Regulation
- Flexibility

Community Cloud

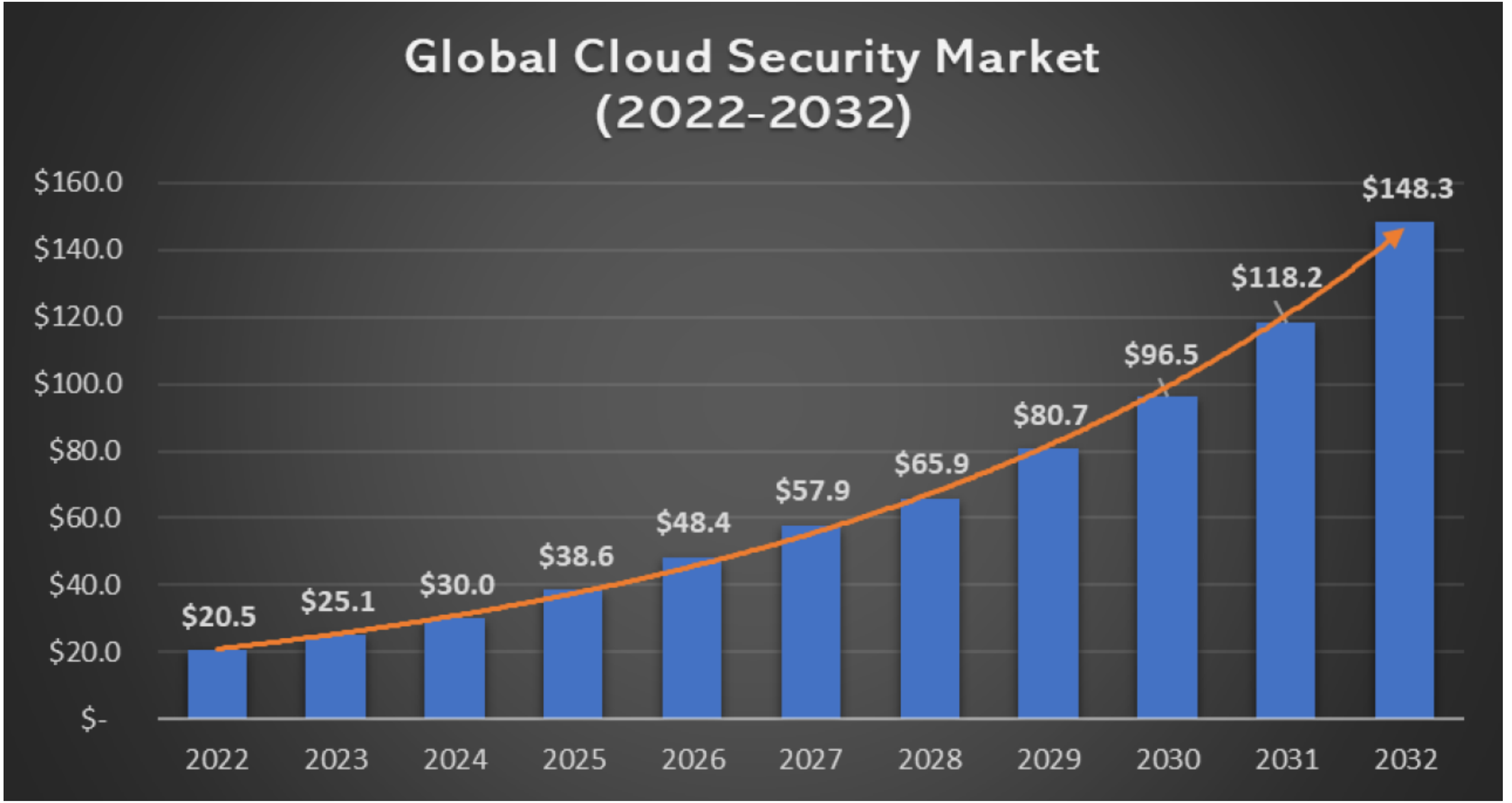
- Meets shared concerns

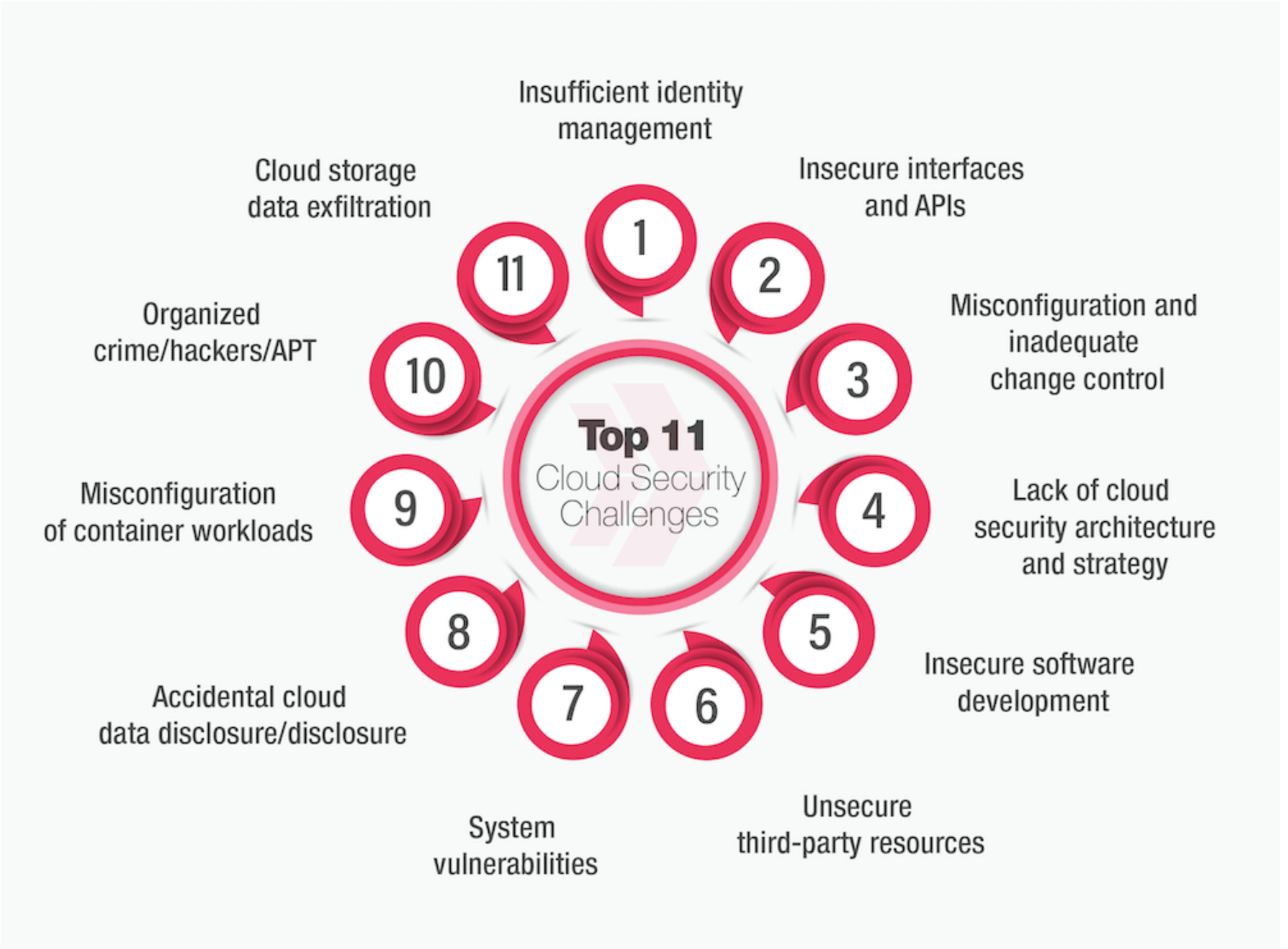
Hybrid Cloud

Cloud Computing Service Model

- IaaS - Digital Ocean, Rackspace, GCE, Amazon EC2
- PaaS - Beanstalk, Heroku, Google App Engine
- SaaS - Gmail, Facebook, Dropbox, Wordpress, Office365
- XaaS - Database as a Service, Security as a Service, Malware as a Service (VMware AppDefense)

Cloud Security Basics


Global Cloud Security Market
(2022-2032)
$160.0
$140.0
$120.0
$100.0
$80.0
$60.0
$40.0
$20.0
$-
$20.5
$25.1
$30.0
$38.6
$48.4
$57.9
$65.9
$80.7
$96.5
$118.2
$148.3
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032


Top 11
Cloud Security
Challenges
1
Insufficient identity management
2
Insecure interfaces and APIs
3
Misconfiguration and inadequate change control
4
Lack of cloud security architecture and strategy
5
Insecure software development
6
Unsecure third-party resources
7
System vulnerabilities
8
Accidental cloud data disclosure/disclosure
9
Misconfiguration of container workloads
10
Organized crime/hackers/APT
11
Cloud storage data exfiltration

Issue with PyTorch TorchServe - CVE-2024-35198 and CVE-2024-35199
AWS-2024-009, 07/18/2024

Issue with AWS Client VPN - CVE-2024-30164, CVE-2024-30165
AWS-2024-008, 07/16/2024

Issue with DeepJavaLibrary - CVE-2024-37902
AWS-2024-007, 06/17/2024

Issue with Amazon EC2 VM Import Export Service
AWS-2024-006, 06/11/2024

Issue with AWS Deployment Framework - CVE-2024-37293
AWS-2024-005, 06/11/2024

CVE-2024-28056
AWS-2024-003, 04/15/2024

CVE-2024-3094
AWS-2024-002, 03/29/2024

CVE-2024-21626 - Runc container issue
AWS-2024-001, 01/31/2024

FetchBench - Issue with Prefetchers in Arm Processors
AWS-2023-014, 11/26/2023

CVE-2023-23583
AWS-2023-013, 11/14/2023

CVE-2023-5528
AWS-2023-012, 11/14/2023

Issue with Amazon WorkSpaces Windows Client Version 5.9 and 5.10
AWS-2023-010, 10/06/2023

Results for **Nallurhalli, Whitefield, Bengaluru** · Choose area

Jobs

Follow

Job postings | Saved jobs | Following

Cloud Security Engineer
S&P Global
Bengaluru, Karnataka • via S&P Global Apply
6 days ago · Full–time

Cloud Security
Tata Consultancy Services Limited
Bengaluru, Karnataka • via Foundit.in
Full–time

Cyber Security Analyst/ Researcher
CloudSEK
Bengaluru, Karnataka • via Greenhouse
Full–time

31 more jobs →

Feedback *Learn more*

Naukri.com
https://www.naukri.com › ... › Cloud Security jobs

2557 Cloud Security Job Vacancies In Bengaluru Bangalore

Apply To 2557 **Cloud Security Jobs** In Bengaluru Bangalore On Naukri.com, India's No.1 Job Portal. Explore **Cloud Security Job** Openings In Bengaluru ...

LinkedIn India
https://in.linkedin.com › jobs › cloud-security-jobs-beng...

8000+ Cloud Security jobs in Bengaluru, Karnataka, India ...

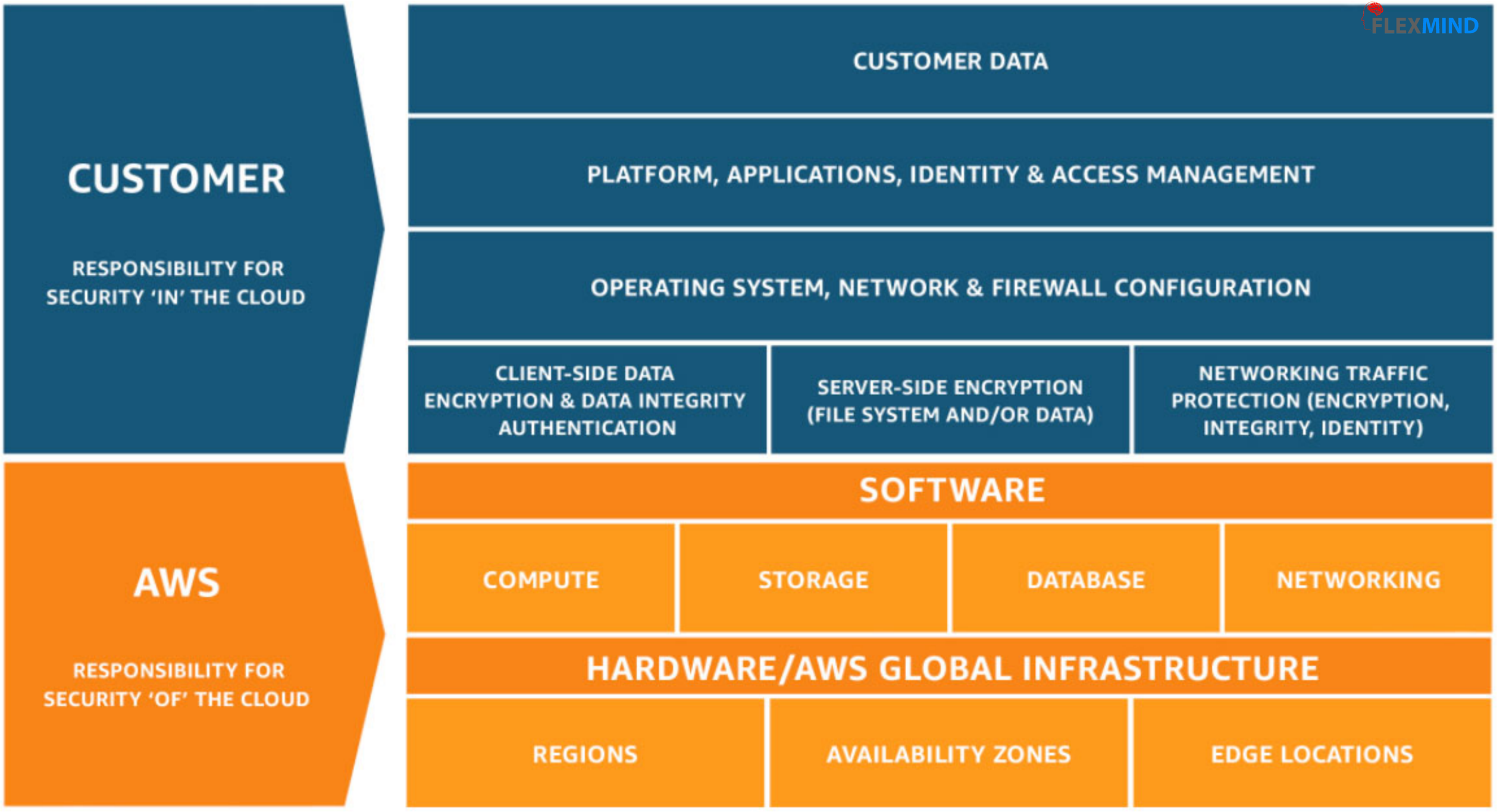
8,000+ **Cloud Security Jobs** in Bengaluru, Karnataka, India (581 new) · Manager, Information Security · Staff Engineer, Information Security · Cloud Security ...

FLEXMIND

Why we need cloud security

✳Cloud computing is being used for more than two decades.
Still, several businesses find **security** as a challenge to handle.

- Everyone is in Cloud now a days
- It’s shared responsibility
- Still new, so more to explore
- Multi tenancy make things more attack prone
- Service Providers are not macho man
- Data Security is a big concern
- and many more …


CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

FLEXMIND

Cloud-Native Security vs Hybrid Cloud Security

- Door with built-in lock
- CCTV camera
- You need both for better security

FLEXMIND

Most Crucial aspects of Cloud Security

Security in the cloud consists of 4 areas:

- Data Protection
- Infrastructure Protection
- Privilege Management
- Detective Controls

FLEXMIND

Cloud Security Dissection

- It’s a shared responsibility
- IAM: Principle of Least Privilege
- Network Security
- Application Security
- Data Security
- Logging and Monitoring
- Cloud Security Automation
- Backup and Disaster Recovery
- Cloud Compliance and Governance
- Threat Detection and Response

FLEXMIND

Logging

- Whom to give log access
- What to Log
- Where to store
- Log Duration
- Secured Cloud Logging Service - sumologic, alertlogic
- Cloudtrail, Cloudwatch, VPC flow logs in AWS

FLEXMIND

Alert & Monitoring

- Trigger point
- What to monitor
- At what frequency
- How much possibility through Automation?
- Alert response mechanism
- IR Mechanism

FLEXMIND

AWS essential services

- AWS EC2
- AWS IAM
- Amazon S3
- VPC
- Lambda
- Route53
- Load Balancer
- API Gateway
- CloudTrail
- Amazon RDS
- Cloudfront

FLEXMIND

AWS Security services and tools

- AWS IAM
- KMS
- AWS CloudTrail
- AWS Config
- AWS GuardDuty
- AWS Macie
- Amazon Inspector
- AWS Shield
- AWS WAF
- Trusted Advisor
- AWS Security Hub
- Amazon Cognito
- Pacu, Prowler, Cloud Custodian, Cloudcheckr, Tenable, and so on…

Summary

- Understand basics of cloud computing
- Get familiar with linux commands, cli, computer networks
- Create a free tier account with AWS/GCP/Azure
- Make yourself comfortable with essential services
- Make a good grip on cloud native security services
- Hands-on is everything
- Read official documentation for better understanding

Technical And Professional Expertise:

- Strong familiarity with cloud provider ecosystems like Amazon AWS, MS Azure, GCP.
- Practical knowledge (desired) of Cloud Service provider's foundation services related to computing, network, storage, content delivery, administration and security, deployment and management, automation technologies. Understanding of microservices programming (AWS Lambda, Docker, etc.)
- Capability architecting highly available systems that utilize load balancing, horizontal scalability and high availability.
- Familiarity using native services on AWS such as (EC2, EKS, API Gateway, RDS, Lambda, CloudWatch, Route 53, etc.).
- GCP (Google Cloud Identity, Google Cloud EKM, Google Cloud Armor, Stack driver Monitoring, Google Kubernetes Engine(GKE).
- Azure (Azure Key Vault, Azure Information Protection, Azure Security Center, Web Application Firewall, etc).
- Understanding of complex enterprise environments and current technology areas like cloud and mobility.
- Familiarity with information security frameworks and standards such as PCI-DSS, HIPPA, NIST, GDPR, and CIS.
- Strong interest in cyber security technologies.
- Desire to work in a team environment with meticulous planning and reporting skills.

FLEXMIND

What's Next

- Advanced Network and Infra Security
- SIEM in Cloud
- CSPM vs CASB (also check CWPP) and now CNAPP
- Cloud Security Threats
- CSA and NIST standards
- Data Governance and Compliance
- Security Automation :
  - Cloudformation, Terraform, Pulumi etc.
  - Security in CI/CD -> DevSecOps (Hotshot)

References & Credits

- Basics of Cloud Security
- Cloud Services Explained by IBM
- Awesome AWS Security
- Cloud Computing Courses from Acloud.guru
- AWS Security Study Plan
- AWS Security Interview Questions
- Cybersecurity in the Cloud Specialization (Coursera)
- Secure Cloud Architecture

FLEXMIND

My Social Channels

cybercloud.guru

github.com/jassics

twitter.com/jassics

linkedin.com/in/jassics

For further queries, please feel free to contact me at jassics@gmail.com

WhatsApp Group (Cybercloud Learning):
https://chat.whatsapp.com/HYOMBR0edCm4L2ej3lcPmn