Rahul Sharma (He/ Him)

WebSite: rvsharma.com   **Email**: me@rvsharma.com
Linkedin.com/in/rahulvinodsharma   **Mobile**: +91 9711-93-7092
Blog: medium.com/@rahulvinodsharma

Senior Cloud Security Professional

Summary

- ✔ Cloud Security Professional with over 10 years of experience in Cyber Security, with Cloud like in GCP, AWS and Azure.
- ✔ Exposure to Fortune 500 infrastructure led cloud security practices to achieve cloud automation with home grown tools, that helps getting compliances, asset discovery.
- ✔ Being a Cloud security expert involved in setting up compliance standards such as PCI, SOC/2, HIPAA, C.I.S., ISO, and N.I.S.T, expert checking and configuring threat alerting systems using GCP Audit logs, IAM, and DLP, S.I.E.M., C.S.P.M., C.I.E.M, and C.W.P.P and proven track record of success that involves designing and implementing manifests for toughening GCP Cloud, ensuring compliance with PCI, SOC/2, HIPAA, C.I.S., ISO, and N.I.S.T, configuring threat alerting systems using GCP Audit logs, IAM, and DLP, setting security measures such as S.I.E.M., C.S.P.M., C.I.E.M, and C.W.P.P. and highly competent consistently conducts security assessments and audits to identify vulnerabilities and risks in the company's cloud environment.
- ✔ Exclusive project experience with industry-leading tools and models like C.S.P.M., S.I.E.M., C.N.A.P.P., C.W.P.P., and Zero Trust, and extensive operational and project experience in designing, implementing, and maintaining secure cloud-based systems and environments. Specific sector experience includes Fintech and the Health Industry, including Identity and Access Management (IAM), Data Loss Prevention (DLP), Macie, and Azure Information Protection.
- ✔ Hands-on experience in automating various aspects of IT operations, including configuration management, security, CI/CD build/release management, cloud resource utilization, and infrastructure automation.
- ✔ Strong communication skills and ability to collaborate with cross-functional teams to ensure the security of an organization's cloud-based systems and data. Works expansively for the organization's vision in delivering the project on time by planning and re-structuring to optimize performance
- ✔ Successfully reduced security alerts by 80% for a large Healthcare and financial services company by designing and implementing a comprehensive infrastructure security plan, including intrusion detection and prevention, access control, and incident response.
- ✔ Built and maintained secure cloud-based systems and environments on the Google Cloud Platform, including designing custom IAM roles and implementing zero-trust security principles.

Rahul Sharma (He/ Him)

WebSite: rvsharma.com   **Email**: me@rvsharma.com
Linkedin.com/in/rahulvinodsharma   **Mobile**: +91 9711-93-7092
Blog: medium.com/@rahulvinodsharma

✔ Led the automation of infrastructure provisioning using IACs and configuration management using Ansible, resulting in a 50% reduction in deployment time and improved system reliability.

✔ A learning enthusiast stays educated with technology trends, is dedicated, and works passionately. Has excellent interpersonal, communication, and analytical skills with demonstrated abilities in customer relationship management. Consistently exceeds expectations of end users and is an exceptional leader who directs the team to high productivity.

Academia

✔ Masters of Computer Application, Jaipur National University, 2017

Licenses & Certifications

✔ Professional Cloud Security Engineer, *24 Aug 2025*
✔ Certified in CloudSecurity, *July 31, 2026*
✔ Certified Kubernetes Security Specialist (CKS), *May 09, 2025*
✔ Certified Kubernetes Administrator (CKA), *November 10, 2023*
✔ Terraform Associate, *November 07, 2023*
✔ Professional Cloud Data Engineer, *6 Sep 2025*
✔ Professional Cloud DevOps Engineer, *26 Oct 2024*
✔ Cloud Digital Leader, *26 Oct 2025*
✔ Professional Cloud Developer, *26 Oct 2024*
✔ Professional Cloud Database Engineer, *26 Oct 2024*
✔ Professional Cloud Network Engineer, *26 Oct 2024*
✔ Professional Cloud Architect, *1 Aug 2024*
✔ Associate Cloud Engineer, *26 Jan 2025*
✔ Professional workspace Administrator, *27 Sep 2025*

Expertise

✔ Cloud Security Architect, Multi-Cloud Cloud Security Experience, Google Cloud Subject Matter Expert, Kubernetes & Docker Security, Identity Access Management, Risk and Threat Assessment, Incident Response, Data Security, Former Lead DevOps.

Career Synopsis

✔ Lead Cloud Security Architect, NCR Corporation   Sep 2023 - Current

Rahul Sharma (He/ Him)

WebSite: **rvsharma.com**   **Email**: me@rvsharma.com
Linkedin.com/in/rahulvinodsharma   **Mobile**: +91 9711-93-7092
Blog: medium.com/@rahulvinodsharma

✔ Sr Cloud Consultant, Mysore 66 Degrees   Jan 2022 - Sep 2023
✔ Sr DevSecOps Engineer, Pune CloudCover.   Feb 2021 - Jan 2022
✔ Lead DevOps Engineer, Functionize Inc., Noida   Nov 2017 - Feb 2021
✔ Network Administrator, Delhi, CMI Pvt. Ltd.,   Aug 2015 - Oct 2017
✔ Penetration Tester, Sandrock eSecurities Pvt. Ltd., Delhi   Jan 2015 - July 2015

<u>PROJECTS IN DETAIL</u>

<u>PROJECT – 1</u>

Company Name: NCR Corporation   **Jan 2022 – Current**
Role: *<u>Lead info Security Consultant</u>*
Project Name: NCR
Location: Gurugram, India
Team Size: 5
<u>Responsibilities:</u>

Cloud Security:
✔ Design and enforce cloud security architectures across Azure and GCP, ensuring compliance with standards like PCI, SOC/2, HIPAA, and ISO. Conduct security code scanning and enhance Infrastructure as Code (IAC) practices organization-wide.

Infrastructure as Code (IAC) Security:
✔ Conducting regular security code scanning across the organization, enhancing security in Infrastructure as Code implementations. Helping Developers to achieve Best practices in the cloud.

Software Composition Analysis and Interactive Testing:
✔ Execute software composition analysis (SCA) and interactive application security testing (IAST) to proactively manage and mitigate software vulnerabilities.

Threat Alerting Systems:
✔ Develop and manage threat alerting systems using GCP Audit logs, IAM, and DLP tools. Collaborate with security teams to integrate advanced systems such as S.I.E.M., C.S.P.M., and C.W.P.P, Using Crowdstrike and Vmware Carbon Black.

Container and Application Security:
✔ Implement rigorous security protocols for containerized applications using GitHub Actions and conduct Docker and Azure image scans. Apply OWASP guidelines to enhance web application security.

Security Assessments and Incident Response
✔ Lead security assessments to identify vulnerabilities and oversee incident response strategies, ensuring rapid detection and management of security incidents in cloud environments.

Environment:
Azure Cloud, Google Cloud Platform, Terraform, Kubernetes Vanilla, GKE/AKS, Orca, Wiz, Snyk, Crowdstrike, Python, Containers, Continuous integrations with Github Actions.

Rahul Sharma (He/ Him)

WebSite: rvsharma.com   **Email**: me@rvsharma.com
Linkedin.com/in/rahulvinodsharma   **Mobile**: +91 9711-93-7092
Blog: medium.com/@rahulvinodsharma

PROJECT – 2

Company Name: 66Degress   **Jan 2022 – Sep 2023**
Role: *Senior Cloud Security Consultant*
Project Name: Davita
Location: Mysore, Karnataka, India
Team Size: 9
Responsibilities:

GCP Cloud Security:
✔ Adeptly designing and implementing manifests for hardening GCP Cloud, ensuring compliance with PCI, SOC/2, HIPAA, C.I.S., ISO, and N.I.S.T.

Threat Alerting Systems:
✔ Proactively and consistently implements threat alerting systems using GCP Audit logs, IAM, and DLP. Collaborating with S.I.E.M., C.S.P.M., C.I.E.M., and C.W.P.P. tools to enhance security measures.

Container Security:
✔ Implementing container vulnerability scanning in Gitlab CI, ensuring a robust security posture for containerised applications.

Infrastructure as Code (IAC) Security:
✔ Conducting regular security code scanning across the organization, enhancing security in Infrastructure as Code implementations.

Security Assessments:
✔ Conducting security assessments and audits to identify vulnerabilities and risks in the company's cloud environment.

Incident Response Planning:
✔ Participating in incident response planning and exercises, ensuring the company's preparedness to handle security incidents and monitoring the company's cloud environment for security incidents and breaches, responding promptly and effectively.

Environment:
Google Cloud Platform, Secure Landing Zone, GKE, Storage, VPC, VPN, IAM, KMS, Cloud Key Management, Serverless, Security Command Center, Cloud Armor, Cloud Data Loss Prevention, Event Threat Detection, Cloud Identity, Binary Authorization, Docker, Kubernetes, Monitoring, Pagerduty, Ansible, Terraform, Bash, Python, BitBucket CI/CD, GitHub Actions, Jenkins, Spinnaker, Apache, Nginx, Bigquery, Airflow, DLP, Dataflow, DataForm, DataPrep, DataProc, Cloud SQL, Cloud Audit Logs, VPC Service Controls, Cloud HSM, Secret Manager.

PROJECT – 3

Company Name: CloudCover Consultancy Pvt Ltd   **Feb 2021 – Jan 2022**
Role: *Senior DevSecOps Engineer*
Client: OVO Payments (PT Visionet International - Fintech)
Location: Pune, Maharashtra, India

Rahul Sharma (He/ Him)

WebSite: **rvsharma.com**
Linkedin.com/in/rahulvinodsharma
Blog: medium.com/@rahulvinodsharma

Email: me@rvsharma.com
Mobile: +91 9711-93-7092

Project Name: OVO Payments (PT Visionet International - Fintech)
Team Size: 12
Responsibilities:

Cloud Manifest Design:
✔ Involved in designing and implementing manifests for hardening multiple clouds, ensuring compliance with PCI, SOC/2, HIPAA, C.I.S., ISO, and N.I.S.T. standards across Google Cloud Platform, AWS, and Azure environments.

Threat Alerting Systems:
✔ Setting the chain of threat alerting systems using GCP Audit logs, CloudTrail, S.I.E.M. (Security Information and Event Management), C.S.P.M. (Cloud Security Posture Management), and C.W.P.P. (Cloud Workload Protection Platform). This enhanced security measures across Google Cloud Platform, AWS, and Azure, providing robust threat detection capabilities.

Security Controls and Policies:
✔ Involved in designing and implementing security controls and policies to safeguard the company's cloud-based assets and data across Google Cloud Platform, AWS, and Azure, consistent security assessments and audits, proactively identifying potential vulnerabilities and risks in the company's multi-cloud environment.

Cloud Platforms: Google Cloud Platform, Microsoft Azure, AWS.
Environment and Tools/Skills:
SNYK, WIZ.io, Gitlab DevOps, Docker, Kubernetes, C.S.P.M., C.I.E.M., C.W.P.P., S.I.E.M., Cloud Custodian, AquaSecurity, Bash, Python, S.A.S.T, D.A.S.T, Azure Security Center, Cloud Security Scanner, WAFs, Security Hub, AWS Guarduty, AWS Inspector, IAM Access Analyzer, AWS Security Hub, AWS WAF, AWS Shield, AWS Firewall Manager, AWS Well-Architected Framework, AWS Security Ref Architecture.

PROJECT – 4
Company Name: Functionize Inc.   **Nov 2017 – Feb 2021**
Role: *Lead DevOps Engineer*
Client: Functionize (Own Product)
Location: Noida, Uttar Pradesh, India
Project Name: U.I. Test Automation On Cloud (Product Based)
Team Size: 5
Responsibilities:

GCP Expertise:
✔ Demonstrated leadership as a Cloud Operations Lead, managing operations on Google Cloud Platform (GCP)

Successful Migration:
✔ Oversaw the migration of a 3-tier application from on-premises to GCP, handling more than USD 50K GCP resources monthly.

Cloud Solution Architect:
✔ Designed and implemented cloud-based solutions aligned with organizational business needs, utilizing automation tools like Terraform for infrastructure provisioning

Rahul Sharma (He/ Him)

WebSite: rvsharma.com   **Email**: me@rvsharma.com
Linkedin.com/in/rahulvinodsharma   **Mobile**: +91 9711-93-7092
Blog: medium.com/@rahulvinodsharma

Cross-Functional Collaboration:
- ✔ Collaborated with developers, architects, and stakeholders to optimize the software delivery process for efficiency and effectiveness.

Security-Focused Development:
- ✔ Worked closely with development teams to ensure applications and systems were designed and implemented, emphasizing security.

Environment and Tools/Skills:
GCP, GKE, Storage, VPC, VPN, IAM, Serverless, Docker, Kubernetes, Monitoring, Pagerduty, Ansible, Terraform, Bash, Python, BitBucket CI/CD, GitHub Actions, Jenkins, Spinnaker, Apache, Nginx, Bigquery, Airflow, DLP, Dataflow, DataForm, Cloud SQL.

PROJECT – 5
Company Name: CMI Pvt. Ltd.   **Aug 2015 - Oct 2017**
Role: _Network Administrator_
Location: Delhi, India
Project Name: Capital One
Team Size: 4
Responsibilities:

Responsible for various tasks to ensure the optimal performance and security of Linux-based systems. Includes installing and configuring Linux operating systems, software, and drivers, focusing on system optimisation. Managed user accounts and permissions, maintaining access control and authorisation, all with a security-first approach. Proactive system performance monitoring has allowed for promptly resolving any security-related issues to maintain high availability. Data management and backup procedures to safeguard critical data, emphasizing data security. Furthermore, I have fortified network security by deploying firewalls and intrusion detection systems, ensuring a robust defense against potential threats and unauthorized access, thus contributing to the organization's overall cybersecurity posture.

Environment and Tools/Skills:

Linux, Ubuntu, R.H.E.L., Git, Zabbix, Nagios, Pagerduty, Bash, Python, Apache, Nginx, Mysql Databases.

PROJECT – 6
Company Name: Sandrock eSecurities Pvt. Ltd   **Jan 2015 - July 2015**
Location: Delhi India
Role: _Junior Penetration Tester_

Rahul Sharma (He/ Him)

WebSite: **rvsharma.com**   **Email**: me@rvsharma.com
Linkedin.com/in/rahulvinodsharma   **Mobile**: +91 9711-93-7092
Blog: **medium.com/**@rahulvinodsharma

Responsibilities:

Conducted thorough Vulnerability Assessments, employing a combination of automated and manual Penetration Tests to proactively identify and address vulnerabilities such as SQL injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and more. Threat Modeling has allowed me to proactively identify potential application threats and evaluate associated risks, ensuring a proactive security stance against emerging challenges. My role also includes meticulously documenting assessment findings and delivering comprehensive reports to stakeholders, offering detailed insights into vulnerabilities, data exposure risks, and actionable mitigation strategies for informed decision-making. Remediation Verification by re-testing applications after addressing vulnerabilities, ensuring the effectiveness of remediation efforts and the application's resilience against potential threats.

Environment and Tools/Skills:

Linux, Ubuntu, CentOS, Git OpenVas, O.W.A.S.P, BurpSuite, Automated Scanners, Bash, Python.