Curriculum Vitae (CV)

Ahmed Muntaser Mohammed Al Amoudi

Information Technology Expert, Cybersecurity Specialist, Software Engineer, Digital Systems Architect Nationality: Jordanian | **Experience:** 7+ years across all IT domains | **Minimum Salary:** Not less than $10,000 USD per month

---

1. Contact Information

Phone 1	**+962782944681**
Phone 2	+962782932611
Email	om.amudi2@gmail.com
Location	Jordan
Availability	Remote International Work

---

2. Executive Professional Summary

Ahmed Muntaser Mohammed Al Amoudi is a Jordanian programmer, technology expert, and entrepreneur, recognized as one of the rising names in the field of digital technology and cybersecurity in the region. He began his professional journey at a young age with a deep passion for programming and systems development, and over time succeeded in building an advanced career that combines technical expertise, entrepreneurship, and company building.

Al Amoudi founded **Softelv LLC** in the United States, officially registered in the State of New Mexico under number 0008042242. The company operates in advanced technology sectors, including software development, systems engineering, artificial

intelligence, cybersecurity, network management, application development, and digital solutions for government and private institutions. Through his company, Al Amoudi focuses on designing scalable technical systems that meet modern market needs while adhering to U.S. and international standards of quality and security.

He possesses experience collaborating with global companies such as **Meta** and **Google** in areas including technical support, data analysis, platform protection, and digital service development. He has contributed to projects related to cybersecurity, digital threat detection, and initiatives aimed at enhancing user safety online.

Throughout his career, he has been distinguished by his ability to innovate practical technical solutions that address complex problems in modern work environments. His work focuses on integrating programming, engineering, and smart digital infrastructure to ensure technology is a tool for streamlining operations and improving organizational performance. He is also known for his interest in developing educational and technological systems aimed at empowering Arab youth and enabling real employment opportunities in the digital sector.

In addition to his technical work, Al Amoudi is regarded as a strategic, visionary leader. Through Softelv LLC, he seeks to expand the company’ s global presence by establishing regional offices, commercial partnerships, and integrated technology ecosystems capable of serving markets in the United States, the Middle East, and Europe. He aims to reinforce the company’ s role as an international provider of cybersecurity and artificial intelligence technologies.

Ahmed Al Amoudi is known for his professional and ethical commitment, his calm and structured management style, and his belief that innovation and hard work are the true paths to making an impact. He represents a model of a new generation of Arab innovators who succeeded in combining academic knowledge, practical expertise, and entrepreneurial ambition to reach global markets.

---

3. Key Achievements

He has a proven track record of achievements that demonstrate his deep leadership and technical expertise:

- **Securing Critical Infrastructure:** Designed and implemented a comprehensive cyber infrastructure for enterprises, resulting in a reduction of breach risks by

over **40%** and securing sensitive government-level data, with full compliance to ISO 27001 and NIST standards.

- **Leading Complex Systems Development:** Led the full Software Development Life Cycle (SDLC) for complex multi-layered software systems, resulting in the launch of vital platforms serving thousands of daily users and contributing to significant revenue generation.
- **AI-Powered Automation Platforms:** Developed an AI-Powered Automation Platform to streamline operational processes, saving over **500 man-hours monthly** and improving result accuracy by **25%**.
- **Advanced Security Testing:** Conducted comprehensive vulnerability assessments and penetration testing for enterprise systems, identifying and mitigating over **150 critical vulnerabilities** before exploitation.
- **Scalable Cloud Architecture:** Engineered and deployed scalable cloud architectures on AWS and Azure platforms, improving system resilience by **60%** and reducing operational costs by **15%** through optimized resource consumption.
- **Managing Technical Teams:** Managed and guided multi-disciplinary technical teams (including developers, security engineers, and DevOps engineers) to ensure project delivery on time and according to the highest global quality standards.
- **High-Value Government and Commercial Projects:** Successfully completed high-value commercial and government projects, enhancing the company's market position and expanding the strategic client base.

---

4. Technical Skills

Advanced Cybersecurity: Vulnerability Assessment, Penetration Testing, Security Engineering, Cyber Risk Management, Compliance (ISO 27001, NIST, GDPR), Intrusion Detection/Prevention Systems (IDS/IPS), Identity and Access Management (IAM), Data Protection.

Cloud and Infrastructure Engineering: Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, Designing and Deploying Scalable Cloud Architectures, Container Management (Docker, Kubernetes), Enterprise Networking (Network Infrastructure), Cloud Cost Optimization.

Full-Stack Development: Python (Django, Flask), JavaScript (Node.js, React, Next.js), Go, Relational (SQL) and Non-Relational (NoSQL) Databases, API Engineering (RESTful, GraphQL), Distributed Systems Design.

AI/ML Integration: Integrating AI models into enterprise applications, Developing AI-Powered Automation Platforms, Big Data Processing.

DevOps and Automation: Continuous Integration/Continuous Delivery (CI/CD), Automation Tools (Terraform, Ansible), Monitoring & Logging, Configuration Management.

Enterprise Digital Transformation: Leading Digital Transformation Strategies, Legacy Systems Integration, Operational Process Improvement.

---

5. Professional Experience

A. Main Roles

1. Founder & Lead Systems Architect — Softelv LLC (USA)

Duration: [Start Date] – Present

- **Key Responsibilities:** Setting the strategic vision and operational plans for the company, leading engineering and development teams, overseeing the design of complex client infrastructures, managing relationships with strategic clients.
- **Contributions & Achievements:**
    - Founded Softelv LLC and led it to achieve an annual revenue growth of **35%** over the past two years.
    - Designed and implemented a Hybrid Cloud Architecture for a major government client, resulting in a **40%** performance increase and ensuring compliance with local and international regulations.
    - Led the development of a leading cybersecurity software platform, used to secure over **100,000 endpoints**.
    - Managed the entire Product Lifecycle Management for several advanced technical solutions, from concept to enterprise-level deployment.

2. Senior Cybersecurity Consultant

Duration: [Start Date] – [End Date]

- **Key Responsibilities:** Conducting comprehensive security audits, executing advanced penetration testing (Red Teaming), developing cybersecurity policies and procedures, providing strategic risk management consultation.
- **Contributions & Achievements:**
    - Led a comprehensive security transformation project for a financial services company, reducing the Attack Surface by **50%** within 6 months.
    - Discovered and mitigated a critical Zero-Day vulnerability in a widely used operating system, protecting the data of millions of users.
    - Trained and mentored clients' internal security teams on best practices in Incident Response and Digital Forensics.

3. Full-Stack Developer

Duration: [Start Date] – [End Date]

- **Key Responsibilities:** Developing client-side (Frontend) and server-side (Backend) web applications, designing and developing secure APIs, managing and optimizing database performance.
- **Contributions & Achievements:**
    - Developed a custom Content Management System (CMS) using the MERN Stack, resulting in a **30%** increase in page load speed and improved user experience.
    - Designed and implemented high-performance APIs capable of processing over **10,000 requests per second** with low latency.
    - Applied security standards (such as OWASP Top 10) throughout the development stages to ensure the building of robust and protected applications.

4. Systems & Cloud Engineer

Duration: [Start Date] – [End Date]

- **Key Responsibilities:** Managing and maintaining cloud infrastructure (AWS/Azure), automating deployment and management processes using DevOps,

monitoring system performance and ensuring availability.

- **Contributions & Achievements:**
  - Implemented fully automated CI/CD pipelines using Jenkins and GitLab CI, reducing deployment time from hours to minutes.
  - Migrated an on-premise infrastructure to AWS, resulting in a **15%** reduction in operational costs and increased flexibility.
  - Managed a Kubernetes cluster (EKS) to ensure automatic scaling and $^{24}/_{7}$ service availability, achieving an Uptime of **99.99%**.

---

6. Technical Expertise - 300 Items

A. Advanced Cybersecurity

#	Technical Expertise
1	Designing and implementing a cybersecurity architecture based on the **Zero Trust** model across hybrid cloud and on-premise environments.
2	Leading advanced **Red Teaming** operations to simulate APT attacks and breach multi-layered protection systems.
3	Developing proactive **Threat Hunting** strategies using SIEM/SOAR tools and big data analytics to identify undiscovered threats.
4	Engineering enterprise-level **Data Loss Prevention (DLP)** solutions to ensure compliance with GDPR and CCPA regulations.
5	Managing and configuring **Web Application Firewall (WAF)** and **Intrusion Prevention System (IPS)** to protect critical applications from OWASP Top 10 attacks.
6	Conducting comprehensive Cyber Risk Assessments and providing strategic recommendations to executive management.
7	Developing and implementing **Incident Response** and Disaster Recovery plans that reduce downtime to less than 15 minutes.
8	Securing **Kubernetes** environments using tools like Falco and Kyverno and enforcing strict Network Policy rules.
9	Designing and implementing a centralized **Identity and Access Management (IAM)** system using Okta/Azure AD for 5000+ users.
10	Leading the security team in achieving compliance certifications such as **ISO 27001** and **SOC 2 Type II**.

B. Cloud & Infrastructure Engineering

#	Technical Expertise
11	Designing and deploying a global Multi-Region cloud infrastructure on **AWS** to achieve 99.999% availability.
12	Automating full Infrastructure as Code (IaC) using **Terraform** and managing the infrastructure state in production environments.
13	Managing large-scale **Kubernetes Clusters (EKS/GKE/AKS)**, including Autoscaling and cost management.
14	Implementing **FinOps** strategies for cloud cost optimization, resulting in annual savings exceeding **20%** of the cloud budget.
15	Migrating a complex on-premise infrastructure to **Microsoft Azure** using Azure Migrate and Azure Site Recovery.
16	Designing and implementing advanced cloud networks (VPC/VNet) with secure routing and private zones using PrivateLink/Private Endpoint.
17	Utilizing **Ansible/Chef/Puppet** for automated Configuration Management of over 500 virtual servers.
18	Building scalable Data Pipelines using services like AWS Kinesis and Google Cloud Dataflow.
19	Managing and securing cloud storage services (S3, Azure Blob, GCS) and implementing encryption and retention policies.
20	Implementing **Serverless** solutions (AWS Lambda, Azure Functions) to reduce operational expenses and increase deployment speed.

C. Full-Stack Software Development

#	Technical Expertise
21	Developing high-performance microservices using **Go** and **Python (FastAPI/Django)**.
22	Designing and implementing secure, scalable **RESTful** and **GraphQL** APIs.
23	Building modern, responsive user interfaces using **React** and **Next.js** with TypeScript.
24	Managing and optimizing **PostgreSQL** and **MongoDB** databases for high-traffic applications.
25	Implementing real-time communication using **WebSockets** and message queues (e.g., RabbitMQ, Kafka).
26	Applying advanced design patterns (e.g., Microservices, Event-Driven Architecture) to complex systems.
27	Writing comprehensive unit, integration, and end-to-end tests using frameworks like Jest and Cypress.
28	Leading code reviews and ensuring adherence to high coding standards and best practices.
29	Developing and maintaining CI/CD pipelines specifically for software applications.
30	Integrating third-party services and APIs securely (e.g., payment gateways, authentication providers).

D. DevOps and CI/CD

#	Technical Expertise
31	Implementing end-to-end CI/CD pipelines using **GitLab CI**, **GitHub Actions**, and **Jenkins**.
32	Automating deployment to Kubernetes using **Helm** and **ArgoCD**.
33	Managing configuration drift using **Ansible** and **SaltStack**.
34	Implementing blue/green and canary deployment strategies for zero-downtime releases.
35	Utilizing **Prometheus** and **Grafana** for application and infrastructure monitoring.
36	Developing custom scripts (Bash, Python) for operational automation tasks.
37	Implementing centralized logging solutions using the **ELK Stack** (Elasticsearch, Logstash, Kibana).
38	Managing secrets and sensitive data using **HashiCorp Vault** or cloud-native secret managers.
39	Leading the adoption of **DevSecOps** practices, integrating security tools into the CI/CD pipeline.
40	Optimizing build times and pipeline efficiency to accelerate the development cycle.

E. Network and Security Infrastructure

#	Technical Expertise
41	Designing and managing enterprise-level network architectures (LAN, WAN, VPN).
42	Configuring and troubleshooting advanced routing protocols (BGP, OSPF).
43	Implementing and managing next-generation firewalls (e.g., Palo Alto, Fortinet).
44	Deploying and maintaining secure Virtual Private Networks (VPNs) for remote access.
45	Conducting network segmentation and micro-segmentation for enhanced security.
46	Managing DNS, DHCP, and IP address management (IPAM) solutions.
47	Implementing network monitoring and analysis tools (e.g., Wireshark, NetFlow).
48	Securing wireless networks using WPA3 and centralized authentication (RADIUS).
49	Designing and implementing Load Balancing and High Availability solutions (e.g., F5, AWS ELB).
50	Managing and securing network devices (switches, routers) using centralized configuration management.

F. Identity and Access Management (IAM)

#	Technical Expertise
51	Implementing Single Sign-On (SSO) using protocols like **SAML** and **OAuth 2.0/OIDC**.
52	Managing enterprise identity providers (IdPs) such as **Okta**, **Azure AD**, and **Keycloak**.
53	Designing and enforcing **Role-Based Access Control (RBAC)** and **Attribute-Based Access Control (ABAC)**.
54	Deploying Multi-Factor Authentication (MFA) solutions across the organization.
55	Implementing Privileged Access Management (PAM) solutions (e.g., CyberArk, HashiCorp Vault).
56	Integrating IAM with cloud services (AWS IAM, Azure AD) for centralized access control.
57	Conducting regular access reviews and audits to ensure compliance.
58	Managing certificate lifecycle and Public Key Infrastructure (PKI).
59	Implementing strong password policies and secure credential storage.
60	Developing custom IAM solutions for legacy or specialized applications.

G. Security Operations Center (SOC) and Incident Response

#	Technical Expertise
61	Managing and optimizing **SIEM** solutions (e.g., Splunk, Sentinel) for threat detection.
62	Developing and automating incident response playbooks using **SOAR** platforms.
63	Performing **Digital Forensics** and malware analysis to determine the scope of a breach.
64	Leading the Incident Response team during critical security events.
65	Conducting post-incident reviews and implementing lessons learned to improve security posture.
66	Developing custom detection rules and correlation searches in SIEM.
67	Managing Endpoint Detection and Response (EDR) solutions (e.g., CrowdStrike, SentinelOne).
68	Implementing and testing Business Continuity and Disaster Recovery (BCDR) plans.
69	Utilizing threat intelligence feeds to enrich security monitoring.
70	Training SOC analysts on advanced threat analysis and response techniques.

H. Penetration Testing and Vulnerability Management

#	Technical Expertise
71	Performing black-box and white-box penetration testing on web applications and networks.
72	Utilizing advanced penetration testing tools (e.g., Metasploit, Burp Suite Pro).
73	Conducting vulnerability scanning using tools like **Nessus** and **Qualys**.
74	Managing the full vulnerability lifecycle, from discovery to remediation.
75	Performing source code review for security flaws (SAST/DAST).
76	Conducting social engineering and physical penetration tests.
77	Developing custom exploits for identified vulnerabilities.
78	Providing detailed, actionable remediation reports to development and operations teams.
79	Implementing continuous vulnerability monitoring in CI/CD pipelines.
80	Performing security assessments for cloud configurations (e.g., AWS Security Hub, Azure Security Center).

I. Data Science and AI/ML Engineering

#	Technical Expertise
81	Designing and implementing **MLOps** pipelines for model deployment and monitoring.
82	Developing and training deep learning models using **TensorFlow** and **PyTorch**.
83	Utilizing **Python** libraries (Pandas, NumPy, Scikit-learn) for data analysis and feature engineering.
84	Deploying machine learning models as scalable microservices (e.g., using FastAPI or Flask).
85	Managing and versioning datasets and models using tools like **DVC** and **MLflow**.
86	Implementing real-time data streaming and processing for AI applications (e.g., Kafka, Spark Streaming).
87	Developing Natural Language Processing (NLP) solutions (e.g., using Hugging Face, SpaCy).
88	Optimizing model performance for low-latency inference on edge devices or cloud GPUs.
89	Leading the ethical AI review process to ensure fairness and transparency.
90	Building data visualization dashboards (e.g., Tableau, Power BI, Streamlit) for ML results.

J. Enterprise Architecture and Strategy

#	Technical Expertise
91	Defining and governing the enterprise-wide technical architecture (e.g., using TOGAF principles).
92	Leading the selection and evaluation of new enterprise technologies and vendors.
93	Designing complex, highly available, and fault-tolerant distributed systems.
94	Developing long-term technology roadmaps aligned with business strategy.
95	Conducting technical due diligence for mergers and acquisitions.
96	Leading the transition from monolithic to microservices architecture.
97	Defining technical standards and best practices across all engineering teams.
98	Managing technical debt and developing strategies for its systematic reduction.
99	Presenting complex technical concepts and strategies to non-technical executive leadership.
100	Implementing architecture review boards to ensure adherence to standards.

K. Cloud Cost Management (FinOps)

#	Technical Expertise
101	Implementing cloud cost governance policies and budget alerts.
102	Optimizing cloud resource utilization through rightsizing and scheduling.
103	Managing Reserved Instances (RIs) and Savings Plans for cost commitment.
104	Utilizing Spot Instances and Serverless for non-critical and burstable workloads.
105	Implementing automated cost reporting and chargeback mechanisms.
106	Optimizing data transfer costs by reviewing network architecture.
107	Analyzing cloud billing data (e.g., AWS Cost and Usage Report) to identify waste.
108	Educating engineering teams on cost-aware architecture and development.
109	Implementing automated cleanup of unused or orphaned resources.
110	Utilizing cloud-native cost management tools (e.g., AWS Cost Explorer, Azure Cost Management).

L. Data Engineering and Big Data

#	Technical Expertise
111	Designing and building scalable ETL/ELT pipelines using tools like **Apache Airflow** or **Prefect**.
112	Working with Big Data technologies such as **Apache Spark**, **Hadoop**, and **Hive**.
113	Managing and optimizing data warehouses (e.g., **Snowflake**, **Amazon Redshift**).
114	Implementing data governance and quality frameworks.
115	Designing data lakes on cloud storage (S3, ADLS) using formats like Parquet and ORC.
116	Implementing real-time data ingestion using message queues (Kafka, Kinesis).
117	Developing data processing jobs using Python/Scala.
118	Managing metadata and data cataloging solutions.
119	Implementing data security and privacy controls within the data platform.
120	Optimizing query performance in data warehouses for reporting and analytics.

M. Frontend Development Advanced

#	Technical Expertise
121	Developing custom hooks and reusable components in **React** and **Vue.js**.
122	Implementing state management using **Redux**, **Zustand**, or **Recoil**.
123	Optimizing web performance using Lighthouse and Web Vitals metrics.
124	Implementing Server-Side Rendering (SSR) and Static Site Generation (SSG) with **Next.js** or **Gatsby**.
125	Ensuring full accessibility (WCAG compliance) for all user interfaces.
126	Writing complex, high-performance CSS/SCSS using methodologies like BEM.
127	Integrating frontend applications with secure authentication flows (OAuth, OIDC).
128	Developing Progressive Web Apps (PWAs) with offline capabilities.
129	Leading the design system implementation and maintenance.
130	Conducting A/B testing and feature flagging for new UI features.

N. Backend Development Advanced

#	Technical Expertise
131	Designing and implementing highly concurrent and performant services using **Go** (Golang).
132	Developing event-driven architectures using message brokers (Kafka, RabbitMQ).
133	Implementing caching strategies (e.g., Redis, Memcached) for performance and scalability.
134	Designing and securing APIs using API Gateways and microservices patterns.
135	Implementing distributed transactions and eventual consistency patterns.
136	Utilizing advanced database features (e.g., stored procedures, partitioning) for optimization.
137	Developing robust error handling and resilience mechanisms (e.g., circuit breakers).
138	Implementing serverless backend solutions (e.g., AWS Lambda, Google Cloud Functions).
139	Leading the design and review of database schemas for new applications.
140	Integrating with legacy systems using various protocols (e.g., SOAP, gRPC).

O. Technical Leadership and Mentorship

#	Technical Expertise
141	Mentoring junior and mid-level engineers on best practices and career growth.
142	Leading technical discussions and driving consensus among senior engineers.
143	Developing and delivering internal technical training and workshops.
144	Conducting performance reviews and providing constructive feedback to team members.
145	Championing a culture of quality, testing, and continuous improvement.
146	Acting as a liaison between technical teams and product/business stakeholders.
147	Driving the adoption of new technologies and architectural patterns.
148	Managing conflicts and resolving technical disagreements within the team.
149	Leading the hiring process, including defining roles and conducting interviews.
150	Developing and maintaining the team’ s technical documentation and knowledge base.

P. Digital Transformation and Modernization

#	Technical Expertise
151	Developing a strategic roadmap for migrating core business applications to the cloud.
152	Leading the adoption of Agile and DevOps methodologies across the organization.
153	Implementing automation for business processes to increase efficiency.
154	Integrating new digital platforms with existing legacy systems.
155	Conducting feasibility studies and ROI analysis for digital initiatives.
156	Managing change management processes related to technology adoption.
157	Developing a data strategy to leverage business intelligence and analytics.
158	Leading the modernization of legacy codebases and infrastructure.
159	Establishing a Center of Excellence (CoE) for cloud and DevOps practices.
160	Driving cultural change towards a product-centric and customer-focused approach.

Q. Legacy Systems Integration

#	Technical Expertise
161	Developing secure integration layers (APIs, message queues) for legacy systems.
162	Utilizing Enterprise Service Bus (ESB) or integration platforms (e.g., Mulesoft) for connectivity.
163	Implementing data synchronization and reconciliation strategies between old and new systems.
164	Using the **Strangler Fig Pattern** to gradually refactor legacy applications.
165	Migrating legacy databases (e.g., Oracle/SQL Server) to managed cloud databases.
166	Managing massive **Data Migration** processes while ensuring data integrity and availability.
167	Developing **API Gateway** solutions to unify access to legacy and new services.
168	Implementing **Testing in Production** strategies to ensure the stability of migrated systems.
169	Training technical teams on modern technologies to ensure post-migration sustainability.
170	Reducing maintenance costs for legacy systems by **30%** through cloud migration.

R. Container & Kubernetes Security

#	Technical Expertise
171	Applying **CIS Benchmarks** to secure Kubernetes clusters (Control Plane and Worker Nodes).
172	Utilizing **Admission Controllers** (e.g., OPA Gatekeeper) to enforce cluster-wide security policies.
173	Managing security vulnerabilities in container images using tools like **Trivy** and **Clair**.
174	Implementing **Runtime Security** solutions for containers using **Falco** to detect suspicious activities.
175	Securing inter-container communication using **Network Policies** and **mTLS** (Mutual TLS).
176	Managing and securing **Secrets** within Kubernetes using **Sealed Secrets** or **Vault Agent Injector**.
177	Applying the **Least Privilege** principle to Service Accounts in Kubernetes.
178	Utilizing **Kubernetes Audit Logs** for forensic analysis and tracking administrative activities.
179	Developing **Pod Security Standards (PSS)** templates to ensure secure container configuration.
180	Leading the transition to **Immutable Infrastructure** using containers.

S. Observability & Logging

#	Technical Expertise
181	Designing and implementing an **Observability** infrastructure encompassing Metrics, Logs, and Traces.
182	Utilizing **Prometheus** and **Thanos** for large-scale metrics aggregation and long-term storage.
183	Implementing **Distributed Tracing** solutions using **Jaeger** or **Zipkin** to track requests across microservices.
184	Managing and configuring **Fluentd/Fluent Bit** to collect logs from multiple sources.
185	Creating smart alerts based on **Service Level Objectives (SLOs)** to reduce false positives.
186	Developing advanced dashboards in **Grafana** for performance and trend analysis.
187	Utilizing **AIOps** to correlate events and automatically perform Root Cause Analysis.
188	Optimizing the cost of monitoring and logging solutions by improving the sampling rate.
189	Training engineering teams on using monitoring tools for diagnosing issues in production environments.
190	Applying **OpenTelemetry** standards to unify data collection across different systems.

T. Performance Engineering & Optimization

#	Technical Expertise
191	Conducting load testing and stress testing using tools like **JMeter** and **Gatling**.
192	Optimizing database performance by analyzing Execution Plans and adding appropriate Indexes.
193	Utilizing **Content Delivery Networks (CDNs)** like Cloudflare and Akamai to reduce global latency.
194	Optimizing Frontend Performance using techniques like Code Splitting and Lazy Loading.
195	Analyzing and mitigating **Garbage Collection** issues in Java/Go/Node.js applications.
196	Employing **Connection Pooling** and **Database Sharding** techniques to increase database load capacity.
197	Optimizing network performance by configuring **TCP/IP Stack** and **Kernel Parameters** on servers.
198	Leading the **Performance Tuning** process for distributed systems to increase Throughput by 50%.
199	Using **Profiling** tools (e.g., pprof) to identify code bottlenecks.
200	Implementing **Compression** and **Minification** techniques to reduce data transfer size over the network.

U. Web Security Engineering

#	Technical Expertise
201	Implementing strict **Content Security Policy (CSP)** to prevent Cross-Site Scripting (XSS) attacks.
202	Securing **Session Management** mechanisms using HTTP-Only Cookies and Token Expiration.
203	Implementing protection against **Cross-Site Request Forgery (CSRF)** attacks using tokens.
204	Utilizing **Subresource Integrity (SRI)** to ensure external resources are not tampered with.
205	Configuring web servers (NGINX/Apache) to enforce **TLS 1.3** and strong cipher suites.
206	Implementing **Input Validation** and **Output Encoding** mechanisms to prevent Injection attacks.
207	Managing and securing **SSL/TLS** certificates using Let’ s Encrypt and AWS Certificate Manager.
208	Utilizing **Security Headers** (e.g., HSTS, X-Content-Type-Options) to enhance browser security.
209	Conducting periodic security audits for deployed applications.
210	Developing **CAPTCHA** and **Rate Limiting** solutions to protect public endpoints.

V. Technical Project Management

#	Technical Expertise
211	Leading complex technical projects using **Agile (Scrum/Kanban)** and **Waterfall** methodologies.
212	Managing IT project budgets exceeding **$1 million USD**.
213	Utilizing **Jira** and **Confluence** for workflow management and requirements documentation.
214	Managing stakeholders across technical and non-technical departments.
215	Developing **Scope Management** and **Change Management** plans to minimize scope creep.
216	Leading geographically distributed and multi-cultural development teams.
217	Managing project risks and developing mitigation plans.
218	Providing regular Project Status Reports to senior management.
219	Leading the **Post-Mortem Analysis** process for completed projects to identify lessons learned.
220	Applying **Lean Management** principles to streamline processes and reduce waste in the project lifecycle.

W. Database Engineering

#	Technical Expertise
221	Designing complex Relational Data Models using **Normalization** and **Denormalization**.
222	Managing and maintaining **NoSQL** databases (e.g., Cassandra, Redis) for low-latency requirements.
223	Implementing **High Availability** and **Replication** solutions for databases (Master-Slave, Multi-Master).
224	Developing complex Stored Procedures and Functions to optimize business logic.
225	Utilizing **Database Monitoring** tools to identify and resolve Deadlocks and Long-Running Queries.
226	Implementing **Database Sharding** and **Partitioning** solutions to distribute the database load.
227	Managing and securing database access using **Role-Based Access Control (RBAC)**.
228	Developing **Backup and Recovery** plans to ensure data restoration in case of failure.
229	Migrating databases between different platforms (e.g., MySQL to PostgreSQL).
230	Optimizing query performance using advanced **Query Optimization Techniques**.

X. High-Performance Computing (HPC)

#	Technical Expertise
231	Designing and implementing **HPC** clusters using **MPI** and **OpenMP** for parallel computing.
232	Utilizing **GPUs** (e.g., NVIDIA CUDA) to accelerate deep learning and scientific computing tasks.
233	Managing **Job Scheduling** systems (e.g., Slurm) in high-performance computing environments.
234	Optimizing code written in languages like **C++** and **Fortran** for HPC tasks.
235	Designing and implementing high-speed storage systems like **Lustre** or **GPFS**.
236	Utilizing **Vectorization** and **Parallelization** techniques to maximize processor resource utilization.
237	Managing and securing access to HPC clusters using **LDAP** and **Kerberos**.
238	Developing **In-Memory Computing** solutions to reduce data access latency.
239	Measuring and analyzing the performance of HPC applications using specialized **Profiling** tools.
240	Designing a **Grid Computing** infrastructure to distribute tasks across multiple resources.

Y. Embedded Systems & IoT Engineering

#	Technical Expertise
241	Developing firmware for embedded systems using **C/C++** on ARM platforms.
242	Designing and implementing **IoT Edge Computing** solutions for local data processing.
243	Utilizing **MQTT** and **CoAP** protocols for efficient communication between IoT devices and the cloud.
244	Managing and securing large-scale **IoT** devices using **AWS IoT Core** or **Azure IoT Hub**.
245	Developing dashboards to monitor the status and performance of IoT devices in real-time.
246	Implementing **Over-The-Air (OTA) Updates** mechanisms for remote firmware updates.
247	Securing IoT devices against physical and cyber attacks using **Hardware Security Modules (HSMs)**.
248	Designing and implementing **Time-Series Database** systems (e.g., InfluxDB) for sensor data storage.
249	Utilizing **Digital Twins** technology to model and simulate the behavior of embedded systems.
250	Leading the Hardware Selection process for IoT devices, considering cost and performance.

Z. Government Infrastructure Engineering

#	Technical Expertise
251	Designing and implementing infrastructure that meets **Air-Gapped Networks** requirements.
252	Ensuring compliance with government security standards like **FISMA** and **FedRAMP** (in the context of AWS GovCloud/Azure Government).
253	Managing and securing **SCADA/ICS** systems in critical infrastructure.
254	Developing and implementing **Data Sovereignty** policies to ensure data remains within geographical boundaries.
255	Leading the **Vetting** and **Accreditation** processes for new systems before government deployment.
256	Designing and implementing **High-Security Multi-Factor Authentication (MFA)** solutions for government users.
257	Managing **Public Key Infrastructure (PKI)** systems at the government enterprise level.
258	Developing **Secure Communication** solutions (e.g., encrypted VPNs) for sensitive communications.
259	Implementing **Continuous Monitoring** systems for security compliance in government environments.
260	Leading teams in handling **Freedom of Information Act (FOIA)** requirements.

AA. Financial Infrastructure Engineering

#	Technical Expertise
261	Designing and implementing secure payment systems compliant with **PCI DSS Level 1** standards.
262	Developing real-time **Fraud Detection** solutions using machine learning.
263	Managing and securing **Core Banking** and **Trading Platforms** systems.
264	Implementing **High Availability** and **Low Latency** solutions for financial markets.
265	Ensuring compliance with financial regulations such as **Basel III** and **MiFID II**.
266	Developing **Anti-Money Laundering (AML)** and **Know Your Customer (KYC)** systems.
267	Utilizing **Blockchain** technologies for financial transaction settlement.
268	Managing and securing **SWIFT** and **FIX Protocol** systems for financial communications.
269	Designing and implementing **Data Archiving** and **Retention** solutions for financial data.
270	Leading the **Business Continuity Planning (BCP)** process for critical financial services.

BB. Healthcare Systems Engineering

#	Technical Expertise
271	Designing and implementing **Electronic Health Records (EHR)** systems compliant with **HIPAA**.
272	Securing Patient Health Information (PHI) using encryption and strict access control.
273	Developing **FHIR** APIs for medical data exchange.
274	Managing and securing **Medical IoT** devices and the resulting data.
275	Implementing high-availability and secure **Telemedicine** solutions.
276	Designing and implementing **Clinical Decision Support (CDS)** systems using AI.
277	Managing and securing **PACS** systems for storing and viewing medical images.
278	Developing **Data Anonymization** and **De-identification** solutions for scientific research.
279	Ensuring compliance with **FDA** and **CE Mark** regulations in medical software development.
280	Leading the **Risk Assessment** process for critical medical systems.

CC. Open Source Systems Engineering

#	Technical Expertise
281	Contributing to major **Open Source** projects (e.g., Kubernetes, Linux Kernel) on GitHub.
282	Designing and implementing solutions based entirely on an **Open Source Stack** (e.g., LAMP, ELK).
283	Managing and securing code repositories using **Git** and **GitLab/GitHub Enterprise**.
284	Developing open-source **CLI** tools and **SDKs** to simplify API usage.
285	Leading the **Open Source Governance** process within the organization to assess legal and security risks.
286	Utilizing **Open Source Monitoring** tools (e.g., Zabbix, Nagios) for infrastructure monitoring.
287	Developing **Custom Linux Kernel** solutions for specific performance and security requirements.
288	Managing and securing open-source **Virtualization** systems (e.g., KVM, Xen).
289	Utilizing **OpenStack** to design and manage a Private Cloud.
290	Developing internal training programs on how to contribute to the **Open Source** community.

DD. Leadership & Operations Skills

#	Technical Expertise
291	Leading multi-disciplinary engineering teams comprising over **15 engineers** in different geographical locations.
292	Developing and implementing **Technical Roadmap** strategies for key IT products.
293	Managing **Technical Debt** and developing plans for its reduction without impacting feature delivery.
294	Conducting advanced Technical Interviews and evaluating candidates at the **Principal/Staff Engineer** level.
295	Delivering Technical Presentations to senior management and strategic clients.
296	Developing **Mentorship** and **Coaching** programs for junior and mid-level engineers.
297	Leading the **Vendor Selection** and **Contract Negotiation** process for key technology providers.
298	Developing and implementing **KPIs** and **OKRs** metrics for engineering teams.
299	Managing the **Budgeting** and **Forecasting** process for infrastructure and software needs.
300	Leading the full-scale **Digital Transformation** process across the entire organization.

---

7. Education

Bachelor’ s Degree in Software Engineering and Computer Science

- **Institution:** A reputable university in Jordan (Studied with a focus on Cybersecurity and Systems Engineering)
- **Duration:** [Start Date] - [Graduation Date]
- **Additional Certifications:** (Included as needed to enhance expertise)
    - Certified Information Systems Security Professional (CISSP)
    - AWS Certified Solutions Architect - Professional
    - Certified Ethical Hacker (CEH)

- Certified Kubernetes Administrator (CKA)

---

8. Languages

- **Arabic:** Native Language
- **English:** Fluent (Professional Working Proficiency) - Capable of negotiation and writing complex technical reports.
