

INFORMATION & CYBER SECURITY 800**ASSIGNMENT COVER SHEET****Name & Surname:****IT'S No:****Qualification:****Year:****Semester:****Assignment Due Date:****Date submitted:**

Table of Contents

QUESTION 1	3
Architectural Components and Strategies for the Security of a cloud-native Enterprise Environment	3
Runtime monitoring and vulnerability scanning for containers.	4
Approach to Authentication, Authorization, and Privilege Escalation Prevention:	5
Multi-Factor Authentication (MFA) in Enhancing Security:	6
Encryption mechanisms to protect data at rest and in transit	7
Strategies for key management and secure storage of cryptographic keys	8
QUESTION 2	9
Blockchain and Benefits of Blockchain to the Cybersecurity Ecosystem:	9
Blockchain applications in security	9
Types of software risks in the Fourth Industrial Revolution	10
Methods of Risk Mitigation	11
References	13



PITHYPAGE
 TOGETHER FOR EXCELLENCE

QUESTION 1

You have been asked to lead a cybersecurity team responsible for ensuring the security of a cloud-native enterprise environment that utilizes various cloud services emerging and disruptive technologies.

1.1 Describe the architectural components and strategies you would employ to secure the cloud-native environment. How would you address concerns related to network security, data protection, and access control? (10 marks)

Architectural components and strategies for the security of a cloud-native enterprise environment

To secure a cloud-native enterprise environment that employs numerous cloud services and emerging technologies, it is necessary to have a comprehensive approach that includes architectural components, strategies, and best practices. Following are the key components and strategies that I would utilize to ensure the security of such an environment, dealing with data protection, network security, as well as access control concerns:

1. Architectural Components:

- **Microservices Architecture:** Employ a microservices architecture to split the application into manageable and smaller components. This helps in isolation, scaling, as well as easier monitoring of every single service.
- **Containers and Orchestration:** Control containerization such as Docker and orchestration tools, for instance Kubernetes for constant use and scaling of applications (Rahaman *et al.*, 2023). Execute security actions, for instance network policies, image scanning, and pod security procedures.
- **Serverless Computing:** Integrate serverless computing for event-driven jobs. Serverless platforms can manage security features such as scaling and patching, lessening the attack surface.
- **Multi-Cloud Strategy:** It can help in avoiding vendor lock-in. Allocating jobs through several cloud providers can increase resistance and decrease single points of breakdown.
- **Zero Trust Architecture:** By adopting the zero-trust model, trust is certainly not assumed to be founded only on location (external or internal to the network). Authenticating identities and executing access controls despite device or user location.

2. Strategies for Network Security:

- Execute network segmentation to separate various application components, services, as well as data. Employ security groups and firewalls to control contact between segments.
- Employ micro-segmentation inside the cloud environment to restrict lateral movement of dangers. Practice network strategies to handle contact between each microservice.
- Apply Virtual Private Cloud to establish separate network environments inside the infrastructure of cloud providers (Subramanian and Gouda, 2015). Divide VPCs considering sensitivity levels and application tiers.

- Use intrusion prevention and detection systems (IPS/IDS) to check network traffic for doubtful patterns (Li *et al.*, 2015). Execute centralized logging and analysis to identify and react to irregularities.

3. Strategies for Data Protection:

- Execute encryption in transit and at rest. Utilize encrypted storage solutions for data at rest and TLS/SSL for data in transit. Control encryption keys strongly (Alqahtani and Gull, 2018).
- Categorize data based on regulatory needs and sensitivity. Employ suitable data protection methods created based on classification.
- Adopt Data Loss Prevention solutions to observe and avoid the unauthorized transfer of delicate data. This facilitates in preventing the leakage of data (Deepa *et al.*, 2012).
- Frequently back up data and application configurations on a daily basis. Examine backup and recovery procedures to ensure data integrity and accessibility in case of unpleasant incidents.

4. Strategies for Access Control:

- Apply strong Identity and Access Management strategies to manage application and user access (Alsaadoun, 2019). Apply the principle of least privilege (PoLP) to make sure that the users merely have the required permissions.
- Demand Multi-Factor Authentication for opening essential systems and resources. It assists in providing an additional level of security, even at times when PINs or passwords are compromised.
- Use Role-Based Access Control. It will help in defining permissions and roles depending on the job functions. Give permissions as per these roles to keep a sure separation of jobs.
- Execute continuous monitoring of user activity as well as access logs. Put up warnings for unauthorized or doubtful access attempts.

1.2 Explain how you would implement runtime monitoring and vulnerability scanning for containers to detect and mitigate potential threats. (10 marks)

Runtime monitoring and vulnerability scanning for containers.

It is necessary to implement runtime monitoring and vulnerability scanning for containers to ensure the security of the cloud-native environment.

1. Runtime Monitoring:

Runtime monitoring refers to dynamically observing the activities and actions of containers when they are running. It facilitates in detection of any unauthorized or unusual actions that may denote a security compromise or breach. I would employ the runtime monitoring for containers in the following ways.

- I would take benefit of the built-in monitoring structures that are provided by container orchestration platforms such as Kubernetes (Carrión, 2022). Kubernetes, such as, offers structures, for instance, Network Policies, Pod Security Policies, as well as admission controllers that can implement security procedures at runtime.

- I would use container security solutions that offer real-time monitoring. These tools can examine containers for abnormalities from normal behavior, discover attempts for unauthorized access, as well as detect irregular traffic patterns.
- I would use behavioral analytics to create a standard of normal container behavior. Nonconformities from this standard can activate warnings or actions, signifying possible security occurrences.
- Implement Intrusion Detection Systems constructed for containers. Such systems can evaluate container action for signs of unauthorized access, intrusion attempts, or doubtful traffic (Becker *et al.*, 2008).

2. Vulnerability Scanning:

Vulnerability scanning refers to actively detecting security vulnerabilities in container images prior to they are deployed, accompanied by constantly visualizing images for new vulnerabilities all through runtime.

- Before using a container image, I would use computerized tools to inspect it for known vulnerabilities, insecure configurations, and useless libraries (Berkovich, Kam, and Wurster, 2020). It can be incorporated into the CI/CD pipeline to make sure that merely secure images are used.
- I would apply continuous vulnerability scanning throughout the runtime. It encompasses scanning containers at regular intervals, specifically after changes or updates, to make sure that new vulnerabilities haven't occurred.
- I would incorporate Common Vulnerabilities and Exposures (CVE) databases to remain informed about the latest vulnerabilities. Container images can be cross-referenced by scanning tools against these records to recognize vulnerabilities.
- I would outline security standards for container images, indicating standard configurations and libraries. Deviations can be identified through scanning tools by comparing images against these standards.
- I would fit in vulnerability scanning tools with a container registry or orchestration platform. This allows automated scanning of images when they are driven to the registry or used.
- I would act quickly on the results of the scan by updating container images to solve found vulnerabilities. Computerize the patching procedure to make sure of well-timed solutions.

1.3 Describe your approach to ensure strong authentication, authorization, and privilege escalation prevention? (10 marks) Provide arguments on multi-factor authentication (MFA) in enhancing the security of user access. (10 marks)

Approach to Authentication, Authorization, and Privilege Escalation Prevention:

I would include a combination of advanced technologies and best practices, as well as a continuous monitoring approach to ensure effective authentication, authorization, and privilege escalation prevention.

Authentication:

- Applying Multi-Factor Authentication for user access can be taken as a vital method to improve authentication (Ihalainen, 2016). It demands users to give numerous types of verification (for instance, biometrics, passwords, PINs, etc.) prior to allowing access. It helps in putting an additional level of security, even when one of them gets compromised.
- Employing Single Sign-On integrates user authentication as well as lessens the necessity for numerous passwords. It improves security by reducing the quantity of authentication places that can be damaged.
- Utilize risk-based authentication methods that review device information, user behavior, and location to clarify the level of authentication needed. Strange actions initiate further authentication steps.
- Execute strong password procedures containing systematic password changes, complex requirements, as well as blacklisting of ordinary passwords.

Authorization:

- Use Role-Based Access Control to explain and implement access permissions centered on user responsibilities and roles (Carruthers, 2022). Consistently assess and revise responsibilities to fit organizational changes.
- Balance RBAC with Attribute-Based Access Control, which employs attributes such as resource attributes, user attributes, and context for making access decisions. It assists in offering fine-grained control.
- Implement the principle of least privilege, making sure that users have simply the least access needed for their jobs. This restricts the possible effect of compromised accounts.
- Execute active authorization methods that assess access requests immediately founded on existing policies and conditions.

Privilege Escalation Prevention:

- Employ Just-In-Time access to permit temporary elevated privileges merely at the time of need. It reduces the exposure window for possible privilege escalation.
- Continuous monitoring can be executed for privilege escalations (Jaafar, Nicolescu, and Richard, 2016). Strange patterns of privilege changes activate warnings for additional analysis.
- Allow detailed logging and auditing of access attempts and privilege changes. It offers insights into possible unauthorized activities.

Multi-Factor Authentication (MFA) in Enhancing Security:

Multi-factor authentication (MFA) plays an important part in improving the security of user access by including several layers of authentication (Sekar *et al.*, 2021). While conventional authentication techniques such as passwords can be compromised via numerous ways, for instance, brute-force attacks or phishing, MFA moderates these risks by involving some further types of verification that merely the real user owns.

Firstly, MFA substantially decreases the efficiency of stolen credentials (Otta *et al.*, 2023). In case the password of a user is compromised, MFA still assists in preventing unauthorized access without the knowledge of the second factor, such as a smartphone application, a physical token,

a biometric scan, or a distinctive code sent through email or SMS. It makes it extremely challenging for attackers to break into an account with simply one factor.

Secondly, MFA gives strong security against account takeover attacks (McElroy, 2021). While intruders generally don't have access to the second factor of the user, getting unauthorized access happens to be extremely impossible. It is specifically vital for essential accounts that have high-level privileges or hold sensitive data.

Thirdly, MFA supports the principle of defense fully. By demanding several factors for verification, the attack surface is considerably decreased. Even when one security factor gets compromised, the intruder still encounters extra obstacles to access (Mughal, 2018).

Therefore, all these points show that MFA is an important element in modern cybersecurity approaches.

1.4 Explain how you would apply encryption mechanisms to protect data both at rest and in transit within the cloud environment. (10 marks)

Encryption mechanisms to protect data at rest and in transit

In protecting data in the cloud environment, a complete approach to encryption is essential to secure data both in transit and at rest. To secure data at rest, a robust foundation is created on effective key management systems. Such systems generate, store, as well as rotate encryption keys strongly, frequently employing cloud provider Key Management Services (KMS) for integrated control. Employing server-side encryption (SSE), information is automatically encrypted prior to being saved in numerous cloud storage services, making sure its privacy continues to be unharmed even when present in storage. Transparent Data Encryption (TDE) can be employed for records, encompassing the whole database, containing snapshots and backups, in a layer of encryption. Furthermore, storage-level encryption is suggested for infrastructure as a Service (IaaS) settings to keep data protected.

At times it comes to data in transit, the focus turns to protecting transmission over networks. Transport Layer Security (TLS) protocols take center stage, encoding data throughout transmission. Executing strong TLS patterns containing durable encryption suites, increases the degree of security (E. Rescorla, 2018). By imposing HTTPS for web traffic, protected communication between web applications and users' browsers is kept. Virtual Private Networks (VPNs) build protected channels for data transfer throughout cloud components or between the cloud and on-premises infrastructure. For inter-service communication and APIs, safe API gateways accompanying TLS encryption assure confidentiality as well as data integrity.

Along with data encryption best practices, data classification is essential. Vulnerable information gets prioritized encryption, and key rotation is implemented continually to decrease prospective risks originating from key compromises. Robust verification methods are created to control access to encryption keys and authorize people to be awarded restricted access. To assure clarity and active risk detection, complete logging and monitoring methods are established for encryption methods. Notably, backup encryption guarantees the protection of backups and snapshots encompassing encrypted data, protecting against not permitted access.

By accurately executing encryption methods for both data at rest and in transit, the cloud environment is protected with numerous levels of security (Alqahtani and Gull, 2018). This method strengthens the security posture, protecting sensitive data from possible unauthorized access and breaches.

1.5 Discuss strategies for key management and secure storage of cryptographic keys used for encryption.

Strategies for key management and secure storage of cryptographic keys

Key management refers to an essential aspect of keeping the safety and integrity of encrypted data. Suitable strategies for key management and secure storage of cryptographic keys are necessary to avoid unauthorized access, assure data secrecy, and reduce the chance of key compromise. Some of the strategies are as follows:

- Create cryptographic keys employing a reliable and consistent random number generator. The intensity of the keys clearly influences the encryption's security. Extended key lengths and extra complicated algorithms mostly provide bigger security.
- Execute an integrated key management system that grants a single point of control for creating, distributing, saving, and withdrawing cryptographic keys. It improves control and visibility over the major lifecycle.
- Frequently rotate encryption keys to reduce the possible effects of key compromise. It helps in reducing the time during which an intruder might employ a compromised key to get into encrypted data.
- Safely provide keys to authorized systems, users, or applications. Employ safe networks, for instance, secure key exchange protocols or secure file transfer protocols.
- Ponder upon employing Hardware Security Modules HSMs, specified hardware devices devised to safely store and supervise cryptographic keys. HSMs offer sound physical and logical security for keys as well as can endure numerous attacks (Boireau, 2018).
- Apply encryption at the application layer via frameworks and libraries that present built-in key management processes. It permits additional granular control over key use.
- Use split-key encryption, in which keys are split into parts held by several entities (Tang *et al.*, 2022). This blocks a single individual from having entire access to a key as well as making sure that cooperation is needed to recreate the key.
- Safely verify and allow users with access to encryption keys. MFA and sound access controls ensure that merely authorized people can control keys (Otta *et al.*, 2023).

QUESTION 2

2.1 In your own understanding, explain the concept of Blockchain? Discuss the benefits of Blockchain to the cyber security ecosystem (10 marks)

Blockchain and benefits of Blockchain to the Cybersecurity Ecosystem:

A Blockchain can be defined as a decentralized database system that is allocated amongst computer network nodes. Transactional data from several sources might be quickly gathered, included, and distributed via blockchain cloud services. Information is split into shared blocks connected with each other by employing cryptographic hashes as distinctive IDs.

Following are the benefits of Blockchain to the Cybersecurity Ecosystem:

- Due to the Blockchain's decentralized nature, once data is logged into the Blockchain, it gets practically impossible to modify, giving robust security against unauthorized access and data manipulation.
- Blockchain's resilient nature guarantees the data integrity (Kshetri, 2017). It is specifically important for cybersecurity since it permits the recording of important security incidents, transactions, as well as the logs in a manner that can be simply inspected and verified.
- The transparency of Blockchain in the cybersecurity setting can facilitate locating the origin of unauthorized access or security breaches, stimulating answerability among participants.
- Blockchain networks every so often depend on consensus mechanisms to authorize and establish transactions. This consensus makes sure that several participants approve the transactions' validity prior to they are included in the Blockchain, reducing the probability of false activities.
- Blockchain can increase identity management as well as is specifically beneficial in avoiding identity theft and unauthorized access.
- Blockchain can enable protected data sharing amongst various bodies with no need of a central authority. Members can distribute sensitive information with assurance, realizing that the data's reliability is maintained.
- Blockchain platforms such as Ethereum permit the formation of self-executing smart contracts, which are automatic scripts that impose predefined provisions. Smart contracts in the cybersecurity ecosystem can automate security-linked activities and decrease the necessity for intermediaries.
- Blockchain can improve supply chain security by offering a clear and tamper-proof verification of products' sources, movements, as well as transactions. It assists in tracking and validating the authenticity of goods.

2.2 Mention and describe five (5) blockchain applications in security (10 marks).

Blockchain applications in security

1. Blockchain technology is used for decentralized and secure identity management (Song and Yu, 2022). Conventional identity systems frequently depend on centralized records, which are susceptible to data breaches. Blockchain, nonetheless, allows users to manage their personal digital identities via cryptographic keys saved on the Blockchain. It allows people to share merely required identity elements without showing confidential data.

Furthermore, it decreases the chances of identity theft and permits continuous cross-platform verification.

2. Blockchain improves supply chain security by offering a strong record of products' journey from source to the end point (Et al., 2021). Every stage in the supply chain is documented as a block, creating a final history. It assures authenticity, transparency, as well as the traceability of goods, lowering the probability of forged goods getting into the supply chain. Businesses can confirm the authenticity of goods, creating confidence among customers and partners.
3. **IP Protection:** Blockchain assists in safeguarding intellectual property rights by safely recording possession information of patents, creative works, as well as trademarks (Abeywardena *et al.*, 2021). It inhibits illegal use and creates a clear possession record. Smart contracts can automate royalty payments, assuring creators and artists get reasonable payment for their work with no intermediates.
4. Domain Name Systems solutions based on Blockchain remove centralized authorities, increasing defense and censorship resistance (Ravindra, 2018). Conventional DNS systems are susceptible to incidents, bringing unauthorized redirection or website takedowns. Decentralized DNS on the Blockchain assures ownership of the domain and protects domain resolution, reducing risks linked with essential points of control.
5. Blockchain permits corporations to safely share and work together on cyber threat intelligence data. Shared data is anonymized and encrypted, safeguarding the privacy of providers (Zhang, Bai and Feng, 2022). This collective method assists in detecting and reducing threats quicker, as members can mutually evaluate attack patterns as well as vulnerabilities without showing susceptible data.

2.3 Explain five (5) types of software risks in the Fourth Industrial Revolution (10 marks)

Types of software risks in the Fourth Industrial Revolution

The Fourth Industrial Revolution (4IR) has brought several transformative technologies that reform societies and industries, but it likewise brings new software risks (Jabbar, Mehmood and Malik, 2020). Following are the five types of software risks connected with the 4th Industrial Revolution:

1. **IoT Risks:** As the Internet of Things devices increased in the 4th Industrial Revolution, they turned into the prospective entry points for cyberattacks. Unsafe device firmware, absence of appropriate encryption, unpatched vulnerabilities, and ineffective verification can put in danger essential setups and personal data.
2. **Machine Learning and AI Risks:** Machine learning and AI tools are subject to confrontational attacks in which intruders influence input data to trick algorithms. Bias in Artificial Intelligence models can bring about unfair results, and the absence of interpretability can hamper the detecting of algorithmic errors. The wrong use of Artificial Intelligence software for creating realistic deepfakes or programmed phishing attacks causes substantial threats (Goel, Goel and Kumar, 2023).
3. **Independent Systems and Robotics Risks:** Self-sufficient systems, for instance, industrial robots and self-driving vehicles, encounter risks associated with software glitches, sensor

manipulation, or human mistakes in initial programming. A single software bug might result in dreadful results, emphasizing the necessity for thorough testing, redundancy, as well as fail-safe mechanisms.

4. **Smart Contract Risks:** Although Blockchain gives security benefits, risks in smart contracts used on blockchain platforms can result in substantial monetary losses. Code exposures and coding mistakes in smart contracts can be used by intruders to draw off funds or interrupt transactions, highlighting the significance of code audits in addition to security best practices.
5. **Data Privacy Issues:** The massive data gathering and processing in the 4th Industrial Revolution brought issues associated with data security and privacy. Centralized data repositories turned into high-value points for cybercriminals. Ineffective data protection methods, for instance, improper access controls or weak encryption, can initiate breaches, revealing sensitive private and business data.

2.4 Discuss how the risks in 2.3 can be mitigated (10 marks).

Methods of Risk Mitigation

Mitigating the software risks linked with the Fourth Industrial Revolution needs a comprehensive approach that contains industry best practices technical solutions, besides an attentive cybersecurity attitude. To deal with risks regarding IoT, companies have to emphasize strong encryption for protected data transmission, implement robust authentication methods to avoid unauthorized access, as well as create a consistent system for consistent updates and patches. Executing network segmentation segregates IoT devices from essential systems, decreasing the prospective effect of violations.

For the risks associated with AI and machine learning, organizations should focus on combative training to sustain the models' strength against misuse. The implementation of understandable models increases accountability and transparency whilst continuous monitoring and bias detection assure honest and moral AI results. Establishing strategies for responsible AI use facilitates in mitigating unintentional and evil applications.

Risks associated with independent systems and robotics can be reduced by rigorous testing throughout different scenarios to uncover errors and software bugs. Establishing redundancy and fail-safe mechanisms assures operational security, even if software glitches are present. Keeping human administration and intervention skills remains fundamental to avoid mistakes and keep control over essential systems.

For dealing with smart contract risks, repeated code audits, besides adherence to protected coding practices, are important to distinguishing and fixing flaws in smart contract code. The inclusion of correct verification methods can statistically verify the accuracy of smart contract logic, additionally increasing security.

As far as the risks regarding data privacy and security are concerned, effective encryption techniques ought to be used to shield data at rest and in transit. Access controls have to be thoroughly employed to limit unauthorized access to sensitive information. A data minimization method, gathering and keeping merely critical data, reduces the prospective outcomes of breaches.

Fostering a cybersecurity-aware environment and adopting continuous training inside organizations is similarly vital. Applying a thorough and dynamic method, organizations can go through the era of the transformative technologies brought by the Fourth Industrial Revolution with resilience and confidence.



References

- Abeywardena, K. Y. *et al.* (2021) 'VANGUARD: A Blockchain-Based Solution to Digital Piracy,' *Global Journal of Computer Science and Technology*. Doi: 10.34257/gjcstevol20is4pg19.
- Alqahtani, A. and Gull, H. (2018) *Cloud Computing and Security Issues-A Review of Amazon Web Services, International Journal of Applied Engineering Research*. Available at: <http://www.ripublication.com> (Accessed: 5 April 2021).
- Alsaadoun, O. (2019) 'A cybersecurity prospective on industry 4.0: Enabler role of identity and access management', in *International Petroleum Technology Conference 2019, IPTC 2019*. doi: 10.2523/iptc-19072-ms.
- Becker, T. *et al.* (2008) 'Intrusion detection system for container security,' in *Proceedings of IEEE Sensors*. doi: 10.1109/ICSENS.2008.4716762.
- Berkovich, S., Kam, J. and Wurster, G. (2020) 'UBCIS: Ultimate benchmark for container image scanning,' in *CSET 2020 - 13th USENIX Workshop on Cyber Security Experimentation and Test, co-located with USENIX Security 2020*.
- Boireau, O. (2018) 'Securing the Blockchain against hackers', *Network Security*, 2018(1). doi: 10.1016/S1353-4858(18)30006-0.
- Carrión, C. (2022) 'Kubernetes as a Standard Container Orchestrator - A Bibliometric Analysis,' *Journal of Grid Computing*, 20(4). doi: 10.1007/s10723-022-09629-8.
- Carruthers, A. (2022) 'Role-Based Access Control (RBAC),' in *Building the Snowflake Data Cloud*. doi: 10.1007/978-1-4842-8593-0_5.
- Deepa, N. *et al.* (2012) 'Image based DLP security for risk professionals - A high impact strategy,' *International Review on Computers and Software*, 7(6).
- E. Rescorla (2018) 'RFC 8446 - The Transport Layer Security (TLS) Protocol Version 1.3', *Internet Engineering Task Force (IETF)*.
- Et. al., P. L. (2021) 'Block Chain Technology in Supply Chain Management Using Key Generation,' *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(1S). doi: 10.17762/turcomat.v12i1s.1765.
- Goel, A., Goel, A. K. and Kumar, A. (2023) 'The role of artificial neural network and machine learning in utilizing spatial information', *Spatial Information Research*. doi: 10.1007/s41324-022-00494-x.
- Ihalainen, P. (2016) 'What is Multi-Factor Authentication (MFA)?', *Globalsign*.
- Jaafar, F., Nicolescu, G. and Richard, C. (2016) 'A Systematic Approach for Privilege Escalation Prevention,' in *Proceedings - 2016 IEEE International Conference on Software Quality, Reliability and Security-Companion, QRS-C 2016*. doi: 10.1109/QRS-C.2016.17.
- Jabbar, J., Mehmood, H. and Malik, H. (2020) 'Security of cloud computing: belongings for the generations', *International Journal of Engineering & Technology*, 9(2). doi: 10.14419/ijet.v9i2.30396.

- Kshetri, N. (2017) 'Blockchain's roles in strengthening cybersecurity and protecting privacy,' *Telecommunications Policy*, 41(10). doi: 10.1016/j.telpol.2017.09.003.
- Li, A. S. *et al.* (2015) 'Strategies for network security,' *Science China Information Sciences*, 58(1). doi: 10.1007/s11432-014-5182-9.
- McElroy, S. A. (2021) 'Learning from learning: detecting account takeovers by identifying forgetful users,' *Computer Fraud and Security*, 2021(6). doi: 10.1016/S1361-3723(21)00064-6.
- Mughal, A. A. (2018) 'The Art of Cybersecurity: Defense in Depth Strategy for Robust Protection,' *International Journal of Intelligent Automation and Computing*, 1(1).
- Otta, S. P. *et al.* (2023) 'A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure,' *Future Internet*, 15(4). doi: 10.3390/fi15040146.
- Rahaman, M. S. *et al.* (2023) 'Access Control Design Practice and Solutions in Cloud-Native Architecture: A Systematic Mapping Study,' *Sensors*. doi: 10.3390/s23073413.
- Ravindra, S. (2018) *Blockchain in Cybersecurity*, 18 January.
- Sekar, S. R. *et al.* (2021) 'FPGA Implementation of ECC Enabled Multi-factor Authentication (E-MFA) Protocol for IoT Based Applications', in *Communications in Computer and Information Science*. doi: 10.1007/978-981-16-5048-2_34.
- Song, Z. and Yu, Y. (2022) 'The Digital Identity Management System Model Based on Blockchain,' in *Proceedings - 2022 International Conference on Blockchain Technology and Information Security, ICBCTIS 2022*. doi: 10.1109/ICBCTIS55569.2022.00040.
- Subramanian, S. K. and Gouda, K. C. (2015) 'A Study on The Different Aspects Of Virtual Private Cloud,' *International Journal of Applied Engineering Research*, 10(86).
- Tang, H. *et al.* (2022) 'A Blockchain-Based Framework for Secure Storage and Sharing of Resumes,' *Computers, Materials and Continua*, 72(3). doi: 10.32604/cmc.2022.028284.
- Zhang, W., Bai, Y. and Feng, J. (2022) 'TIIA: A blockchain-enabled Threat Intelligence Integrity Audit scheme for IIoT,' *Future Generation Computer Systems*, 132. doi: 10.1016/j.future.2022.02.023.