JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

AUGMENTING NETWORK SECURITY: CHALLENGES, APPROACHES, AND RESOLUTIONS

MALVINDER SINGH

ASSISTANT PROFESSOR (COMP. SC.), MIRI PIRI KHALSA COLLEGE, BHADUR, PUNJAB, INDIA.

ABSTRACT

Network security plays a critical role in safeguarding the integrity, confidentiality, and availability of data and resources in modern computing environments. As organizations increasingly rely on interconnected networks to conduct business and exchange information, ensuring robust network security measures has become paramount. This research paper provides a comprehensive overview of the challenges faced by network security professionals, along with strategies and solutions to address these challenges effectively. The paper begins by examining the evolving threat landscape, which includes sophisticated cyber threats such as malware, phishing, ransomware, and advanced persistent threats (APTs). These threats target vulnerabilities in network infrastructure, applications, and human behavior, posing significant risks to organizations of all sizes and industries. Next, the paper explores the key challenges encountered in securing modern networks, including the increasing complexity of network environments, insider threats, shadow IT, and compliance requirements. The paper then discusses strategies and best practices for mitigating network security risks and enhancing resilience against cyber threats. These include implementing defense-in-depth strategies, leveraging next-generation firewalls and intrusion detection/prevention systems, deploying encryption and authentication mechanisms, and establishing robust incident response and recovery procedures. Furthermore, the paper examines emerging technologies and trends in network security, such as artificial intelligence (AI) and machine learning, zero trust architecture, and secure access service edge (SASE) solutions. These technologies offer innovative approaches to threat detection, adaptive authentication, and network segmentation, enabling organizations to stay ahead of evolving cyber threats. In conclusion, the paper emphasizes the importance of proactive and collaborative approaches to network security, involving continuous risk assessment, threat intelligence sharing, and security awareness training. By adopting a comprehensive and adaptive security posture, organizations can effectively mitigate risks, protect critical assets, and maintain the trust and confidence of their stakeholders in an increasingly interconnected digital world.

Keywords: Artificial Intelligence, cyber threats, Intrusion Detection System, Network security, SASE, ZTA.

I. INTRODUCTION

The process of preventing unwanted access, misuse, alteration, or destruction of computer networks and the data transferred across them is known as network security. It includes a collection of guidelines, practices, and technological tools intended to guarantee the privacy, availability, and integrity of network resources and data.

Important facets of network security consist of:

- Confidentiality: Maintaining the privacy of confidential information means making sure that only authorized individuals can access it and that it is shielded from prying eyes and hostile elements [1].
- Integrity: Ensuring that data doesn't change or undergo tampering while being sent or stored to avoid unwanted changes.
- Availability: Protecting against denial-of-service (DoS) attacks and other disturbances while guaranteeing that network services and resources are available to authorized users when needed.
- Authentication: Verifying the identification of people, things, and systems gaining access to a network is known as authentication. This is usually done via credentials like passwords, digital certificates, biometrics, or usernames [2].
- Authorization: Authorization is the process of granting users the right amount of access following their verified identities and roles and implementing access rules to stop illegal activity.
- Non-repudiation: Using methods like digital signatures and audit trails, non-repudiation ensures that actions taken by users or systems on the network cannot be subsequently disputed or repudiated.

To accomplish these goals, network security uses a range of technologies and tactics mentioned below and shown in Fig. 1.

Fig. 1 Tactics for network security

- Firewalls: Incoming and outgoing network traffic is monitored and controlled by firewalls—devices or software—according to pre-established security rules, preventing unwanted access and thwarting network-based attacks [3].
- Intrusion Detection and Prevention Systems (IDPS): Devices that keep an eye on network traffic to spot unusual activity or patterns of known attacks. When they do, they notify administrators and take appropriate precautions to lessen the threat.
- Virtual Private Networks (VPNs): Provide privacy and secrecy for remote users connecting to company networks by securely encrypting and tunneling network traffic over open or untrusted networks.
- Encryption: To prevent eavesdropping and unwanted access, data can be encrypted while it's in transit (using protocols like SSL/TLS) and while it's at rest (using disk encryption, for example).
- Access Control: To enforce the least privilege and prevent unwanted access, access control technologies including network segmentation, multi-factor authentication (MFA), and role-based access control (RBAC) are implemented.
- Security Guidelines and Instruction: To educate users about security threats and best practices, complete security policies, processes, and guidelines should be established.

Regular training and awareness programs should also be offered. To protect users and organizations from a variety of cyber threats, network security is crucial for maintaining the availability, confidentiality, and integrity of vital data and resources in contemporary computer networks.

II. Malware, Phishing, and Ransomware

Malware, phishing, and ransomware are all types of cyber threats commonly used by attackers to compromise the security of computer systems and networks. Here's an overview of each:

- Malware:

A wide class of software applications intended to compromise, harm, or obtain unauthorized access to computer systems or networks is known as malware, or malicious software.

Malware can take many different forms, including worms, trojans, spyware, adware, and rootkits [4].

➢ Numerous channels, including malicious websites, external storage devices, contaminated email attachments, and software flaws, can spread malware.

➢ Malware can carry out a wide range of nefarious tasks after it is installed on a system, such as stealing confidential data, interfering with system functions, corrupting files or hardware, and giving attackers unauthorized access.

- Phishing:

Phishing is a type of cyberattack in which a person poses as a reliable source to fool people into disclosing sensitive information, including credit card numbers, usernames, passwords, and other personal information [5].

➢ Phishing assaults generally manifest as fraudulent emails, instant chat messages, or websites that impersonate reputable companies, banks, social media networks, or governmental bodies.

➢ Phishing attacks aim to trick victims into opening harmful attachments, clicking on dangerous links, or entering their login credentials into phony login forms. This gives attackers the ability to steal victims' personal information or access their accounts without authorization.

- Ransomware:

Malware known as ransomware encrypts data or locks down computer systems, making them unusable for users, and then demands a ransom to unlock the system.

➢ Usually, ransomware attacks start with malware being installed on the victim's computer, frequently via exploit kits or phishing emails that take advantage of software flaws.

➢ Once implemented, ransomware uses powerful encryption methods to encrypt files, rendering them unusable without the attacker's decryption key.

➢ The attackers then request payment, typically in cryptocurrency, in return for the decryption key needed to unlock the files or allow users to access the system again.

➢ Attacks using ransomware have the potential to cause serious harm to both people and businesses, including monetary losses, data breaches, business interruptions, and reputational harm.

Overall, malware, phishing, and ransomware are significant cybersecurity threats that require proactive measures, such as robust security controls, user education and awareness training, and regular software updates and patches, to mitigate their risks effectively.

III. Challenges in Network Security

The dynamic nature of cyber threats, the growing complexity of network infrastructures, and the quick uptake of new technologies provide several obstacles to network security. Among the principal difficulties are:

- Advanced Cyberthreats: Cybercriminals are always creating new and inventive ways to attack systems, such as malware, ransomware, phishing, and zero-day exploits. These methods can bypass conventional security measures and seriously harm networks and data [6].
- Advanced Persistent Threats (APTs): APTs are cunning, focused attacks executed by knowledgeable enemies with particular goals in mind. These adversaries frequently seek to obtain persistent access to confidential data or to interfere with vital activities. Proactive defense tactics and sophisticated threat intelligence are necessary for identifying and thwarting APTs.
- Insider Threats: Insider threats represent a serious risk to network security, regardless of their motivation. While careless insiders may unintentionally expose networks to vulnerabilities by casual acts, malicious insiders with privileged access may misuse their privileges to steal confidential information or disrupt operations.
- Increasing complexity of Networks: The proliferation of devices, applications, and cloud services in contemporary networks has increased network complexity and attack surface. For network security specialists, managing and safeguarding a variety of network environments—such as conventional on-premises networks, cloud infrastructures, and IoT devices—presents formidable obstacles [7].
- Bring-Your-Own-Device (BYOD) policies and shadow IT: Employees using unapproved or insecure devices and applications to access company networks run the risk of exposing sensitive data to unapproved access or leakage. Shadow IT refers to the unlawful use of applications and services.
- Mobile and Remote Workforce: As remote work and mobile computing become more popular, they present new security challenges. These include protecting data sent over open Wi-Fi networks, controlling the security of mobile devices, and making sure that security policies are followed outside of the company network perimeter.
- Data Privacy and Compliance: Organizations are subject to stringent obligations to safeguard the privacy and confidentiality of sensitive data, as a result of growing regulatory requirements and data privacy regulations (such as the CCPA and GDPR). It can be difficult and resource-intensive to comply with these laws while upholding strong network security procedures [8].
- Security of Internet of Things Devices: Since many IoT devices lack built-in security features and could be exploited by attackers, the proliferation of IoT devices creates new security risks. For enterprises, securing IoT devices and incorporating them into current network security frameworks pose serious issues.
- Cybersecurity Skills Gap: Organizations find it difficult to attract and retain individuals with experience in developing technologies, threat intelligence, and incident response. This makes network security teams' already difficult tasks even more difficult.

To meet these difficulties, network security must be approached comprehensively and proactively. This includes implementing strong security policies, having sophisticated threat detection and response capabilities, providing continuing security awareness training, and working with cybersecurity experts and peers in the industry.

IV. Mitigating Network Security Risks

A multi-layered strategy that incorporates organizational procedures and technical controls is needed to mitigate network security threats. To reduce the threats to network security, consider the following recommended practices:

- Use "Defense-in-Depth": Use several defensive strategies, such as firewalls, intrusion detection/prevention systems (IDPS), antivirus and antimalware software, access controls, and encryption, as part of a layered security approach [9]. This lessens the effect of possible security breaches and helps to erect several barriers against attackers.
- Update and patch systems frequently: Update all servers, apps, and network devices with the most recent security patches and upgrades. Patching software and firmware vulnerabilities on time is crucial to preventing exploitation since attackers frequently use them to obtain unauthorized access or run malicious code [10].
- Employ Multi-factor authentication (MFA) and Strong Authentication: Make use of multi-factor authentication (MFA) and other strong authentication technologies to confirm the identities of users and devices gaining access to the network. Make sure users only have access to the resources and rights they require to carry out their responsibilities to uphold the principle of least privilege.
- Secure Data While It's in Transit and at Rest: To secure data transferred over a network, particularly sensitive data like passwords, financial information, and personally identifiable information (PII), use encryption protocols (e.g., SSL/TLS). To prevent theft or data breaches, you should also encrypt data that is kept on servers, databases, and mobile devices [11].
- Monitor and Analyze Network Traffic: Use security information and event management (SIEM) systems and network monitoring tools to keep an eye out for any indications of questionable activity, such as malware infections, unauthorized access attempts, or data exfiltration. Examine logs and notifications to find and quickly address security incidents.
- Divide networks into segments and apply the least privilege: Depending on user responsibilities, departments, or the degree of data sensitivity, divide the network into distinct segments or zones. To prevent attackers from moving laterally within the network and lessen the effect of security breaches, implement network segmentation and access controls. Apply the least privilege concept to restrict user access to resources and systems to what is necessary [12].
- Educate and teach Staff: Regularly teach staff members in security awareness to increase their knowledge of common cyber threats, phishing scams, social engineering tactics, and best practices for preserving network security. Encourage staff members to swiftly report any suspicious activity or security incidents.
- Planning for Disaster Recovery and Backups: Establish routine backup methods to make offsite and onsite copies of vital systems and data. To guarantee the prompt restoration of services and data in the case of a network security breach, natural disaster, or other disruptive occurrences, develop and test a thorough disaster recovery strategy.

- Perform Frequent Penetration Testing and Security Assessments: To find and fix flaws in the network infrastructure and applications, conduct regular penetration testing, vulnerability scans, and security assessments. To make sure that security controls and incident response protocols are ready for any cyberattack, test their efficacy.
- Create protocols for responding to incidents: Create and record incident response protocols that specify what should be done in the case of a security breach or incident. Establish communication channels, assign roles and duties to incident response team members, and assess the efficacy of the response plan through routine drills and tabletop exercises [13].

V. EMERGING TECHNOLOGIES AND TRENDS IN NETWORK SECURITY

To handle new threats, strengthen detection and response capabilities, and improve overall security posture, emerging technologies and trends in network security are constantly changing. Notable new developments in network security trends and technologies include:

- ***Zero Trust Architecture (ZTA):***
  A method of network security known as "Zero Trust Architecture" operates under the premise that there is no reason to trust anyone, inside or outside the network boundary. Since ZTA places a strong emphasis on the idea of "never trust, always verify," all users, devices, and applications wanting to access network resources must undergo constant authentication, authorization, and encryption [14]. ZTA reduces the effect of security breaches and aids in preventing attackers from moving laterally across the network by introducing micro-segmentation and granular access controls.
  Implementing Zero Trust Architecture (ZTA) involves a strategic framework and set of principles rather than a specific algorithm. However, there are certain key components and steps involved in implementing ZTA principles within a network environment. Below mentioned is an outline of the algorithmic steps involved in implementing Zero Trust Architecture:
- Identify and Authenticate Users and Devices:
  - ➢ Algorithmically verify the identity of users and devices attempting to access network resources.
  - ➢ Implement strong authentication mechanisms, such as multi-factor authentication (MFA), to ensure the legitimacy of user/device identities.
- Establish Trust Based on Context:
  - ➢ Algorithmically assess contextual factors such as user/device behavior, location, time of access, and security posture to dynamically establish trust levels.
  - ➢ Utilize risk-based authentication algorithms to adjust access controls based on the assessed risk level associated with each access attempt.
- Implement Microsegmentation:
  - ➢ Algorithmically segment the network into smaller, logical segments based on user roles, applications, or data sensitivity levels.
  - ➢ Utilize network segmentation algorithms to enforce granular access controls and isolate network segments from each other, minimizing the attack surface.
- Enforce Least Privilege Access Controls:
  - ➢ Algorithmically enforce the principle of least privilege, granting users/devices access only to the resources and permissions necessary to perform their tasks.
  - ➢ Utilize access control algorithms to dynamically adjust access permissions based on user/device attributes, roles, and contextual factors.
- Monitor and Analyze Network Traffic:
  - ➢ Algorithmically monitor network traffic in real-time using advanced analytics and machine learning algorithms.
  - ➢ Utilize anomaly detection algorithms to identify suspicious activities, unauthorized access attempts, and deviations from normal behavior patterns.
- Enforce Security Policies Consistently:
  - ➢ Algorithmically enforce security policies consistently across all network resources, regardless of their location or access method.
  - ➢ Utilize policy enforcement algorithms to automatically apply security policies based on predefined rules and conditions.
- Implement Encryption and Secure Communications:
  - ➢ Algorithmically encrypt data in transit and at rest to protect it from eavesdropping and unauthorized access.
  - ➢ Utilize encryption algorithms and secure communication protocols (e.g., SSL/TLS) to ensure the confidentiality and integrity of data transmitted over the network.
- Continuous Monitoring and Adaptive Response:
  - ➢ Algorithmically monitor network and user/device behavior continuously, detecting and responding to security incidents in real time.
  - ➢ Utilize adaptive response algorithms to automatically mitigate threats, adjust access controls, and remediate security vulnerabilities as they are identified.
- Regular Auditing and Compliance Checks:
  - ➢ Algorithmically conduct regular audits and compliance checks to ensure adherence to security policies, regulations, and industry standards.
  - ➢ Utilize compliance assessment algorithms to identify non-compliant behavior and enforce remediation actions as necessary.
- Iterative Improvement and Optimization:
  - ➢ Algorithmically analyze security metrics and performance indicators to identify areas for improvement and optimization.

  - ➢ Utilize feedback loop algorithms to iteratively refine ZTA implementation, adapt to evolving threats, and enhance overall security posture over time.

While there's no single algorithm that encompasses Zero Trust Architecture, the implementation of ZTA principles within a network environment involves a combination of algorithms, technologies, and processes aimed at dynamically assessing trust, enforcing access controls, and mitigating security risks in real time.

- ***Secure Access Service Edge (SASE):***
  Wide-area networking (WAN) capabilities are combined with network security features including firewalls as a service, secure web gateways, and secure access brokers in Secure Access Service Edge (SASE), a cloud-based security architecture. SASE offers safe and efficient access to apps and resources regardless of user location or device by combining networking and network security features into a single cloud-based solution. SASE helps enterprises lower complexity, increase scalability, and strengthen security posture while meeting the demands of distant and mobile users by moving networking and security services to the cloud [15]. Below mentioned is an outline of the key components and steps involved in implementing a Secure Access Service Edge:
- Identify User and Device:
  - ➢ Algorithmically authenticate users and devices attempting to access network resources.
  - ➢ Utilize identity verification algorithms, such as multi-factor authentication (MFA), to ensure the legitimacy of user/device identities.
- Determine Access Policy:
  - ➢ Algorithmically assess the context of access attempts, including user identity, device posture, location, and application being accessed.
  - ➢ Utilize policy-based access control algorithms to dynamically determine access permissions based on contextual factors and predefined security policies.
- Route Traffic to Security Services:
  - ➢ Algorithmically route network traffic to the appropriate security services based on security policies and traffic patterns.
  - ➢ Utilize traffic routing algorithms to direct traffic through security inspection points, such as secure web gateways, firewalls, and intrusion detection/prevention systems (IDPS), before reaching their destination.
- Inspect and Secure Traffic:
  - ➢ Algorithmically inspect network traffic for threats, vulnerabilities, and malicious activity using advanced security techniques.
  - ➢ Utilize security inspection algorithms, such as deep packet inspection (DPI), signature-based detection, and behavioral analysis, to identify and mitigate security risks in real time.
- Enforce Security Policies:
  - ➢ Algorithmically enforce security policies consistently across all network traffic, regardless of its origin or destination.
  - ➢ Utilize policy enforcement algorithms to apply security policies based on predefined rules and conditions, such as user roles, application types, and data sensitivity levels.
- Encrypt and Secure Communications:
  - ➢ Algorithmically encrypt data in transit to protect it from interception and unauthorized access.
  - ➢ Utilize encryption algorithms and secure communication protocols (e.g., SSL/TLS) to ensure the confidentiality and integrity of data transmitted over the network.
- Optimize Network Performance:
  - ➢ Algorithmically optimize network performance by dynamically adjusting traffic routing and prioritization based on application requirements and network conditions.
  - ➢ Utilize network optimization algorithms, such as traffic shaping, quality of service (QoS), and link aggregation, to ensure optimal performance and user experience.
- Provide Scalable and Resilient Infrastructure:
  - ➢ Algorithmically deploy scalable and resilient infrastructure to support dynamic workload demands and ensure high availability.
  - ➢ Utilize load balancing algorithms, fault tolerance mechanisms, and automated scaling techniques to distribute workloads efficiently and mitigate the impact of hardware failures or network outages.
- Continuous Monitoring and Adaptive Response:
  - ➢ Algorithmically monitor network traffic and security events in real-time, detecting and responding to security incidents promptly.
  - ➢ Utilize anomaly detection algorithms and machine learning techniques to identify suspicious behavior and automatically trigger response actions, such as blocking malicious traffic or quarantining compromised devices.
- Ensure Regulatory Compliance:
  - ➢ Algorithmically enforce compliance with regulatory requirements and industry standards, such as GDPR, HIPAA, and PCI DSS.
  - ➢ Utilize compliance assessment algorithms to audit security controls, track compliance status, and generate reports for regulatory purposes.

While this outline provides a high-level overview of the components and steps involved in implementing a Secure Access Service Edge, the actual implementation may vary depending on the specific requirements and technologies used by organizations. SASE is a flexible and scalable architecture that adapts to evolving network environments and security threats, making it an increasingly popular choice for organizations seeking to enhance their security posture and provide secure access to distributed users and resources.

- ***Machine learning (ML) and artificial intelligence (AI):***
  ML and AI technologies are being utilized more and more in network security for behavioral analysis, anomaly detection, and threat identification. Security solutions powered by AI can automatically respond to security issues, detect trends suggesting malicious behavior, and analyze enormous volumes of network data in real time. By learning from previous security events, machine learning algorithms can adjust and advance over time, facilitating more precise threat identification and proactive prevention against new threats [16].
- ***Network Detection and Response (NDR):***
  These solutions offer a thorough understanding of network traffic and enable the prompt detection and remediation of security issues. NDR systems use behavior-based detection, packet inspection, and advanced analytics to find malware infestations, unauthorized access attempts, and unusual activities on the network. Network traffic analysis (NDR) solutions enable businesses to quickly identify and address security problems before they become breaches by fusing automated response capabilities with network traffic analysis.
- ***Identity-Centric Security:***
  This type of network security centers on protecting user identities and devices as the main boundary. To stop unwanted access and privilege escalation, this strategy places a high emphasis on identity verification, robust authentication procedures, and ongoing user behavior monitoring. Identity-centric security systems combine network security controls and identity and access management (IAM) policies to enforce least privilege, identify unusual behavior, and instantly handle security issues [17].
- ***Software-Defined Perimeter (SDP):***
  This design isolates users, devices, and applications from the larger network until their identification and security posture are confirmed. It does this by dynamically creating unique perimeters around each of these entities. Regardless of the users' or devices' physical location or the network environment in which they are located, SDP solutions use cryptographic techniques to provide safe, encrypted connections between them and network resources. SDP, especially in cloud-based and hybrid contexts, helps enterprises avoid unwanted access and lower the attack surface by implementing stringent access controls and a zero-trust policy [18].

These cutting-edge developments in network security and technology offer novel ways to combat changing cyber threats and strengthen the defenses of enterprise networks against highly skilled intrusions. Organizations need to keep up with the latest advancements in the threat landscape and take proactive steps to improve their network security posture.

VI. Conclusion

Due to the ongoing evolution of cyber threats in terms of sophistication and frequency, network security continues to be a vital necessity for enterprises globally. To provide insights into how companies may increase their security posture in a constantly changing threat landscape, this research study has examined a variety of network security topics, including emerging technologies, present difficulties, and future directions. Using cutting-edge technologies like Zero Trust Architecture (ZTA), Secure Access Service Edge (SASE), Artificial Intelligence (AI), and Machine Learning (ML) to improve threat detection and response capabilities, the research have explored the importance of implementing a multi-layered defense strategy throughout this paper. To protect network environments from constantly evolving cyber threats, the conducted research have also emphasized the significance of identity-centric security, network detection and response (NDR), and software-defined perimeter (SDP) solutions.

I've also talked about the difficulties businesses have protecting their networks, such as the growing complexity of network environments, insider threats, regulatory compliance, and a lack of qualified cybersecurity specialists. To reduce network security risks, I have underlined the significance of proactive measures including frequent updates and patches, robust authentication and access controls, security awareness training, and incident response preparation.

Looking ahead, new trends and technologies like autonomous security operations, decentralized identification, and quantum-safe cryptography will influence network security in the future. To stay ahead of the curve and be innovative in the face of ever-changing dangers, organizations need to embrace a security-first mentality and integrate security into their digital transformation activities.

In conclusion, organizations can strengthen their resilience against cyber threats and protect their networks, data, and reputation in an increasingly digital and interconnected world by keeping up with emerging threats and trends, implementing best practices in network security, investing in robust security solutions, and developing talent.

References

[1]. Aghajani, G., Ghadimi, N., 2018. Multi-objective energy management in a micro-grid. Energy Rep. 4, 218–225.

[2]. Ahmed Jamal, A., et al., 2021. A review on security analysis of cyber physical systems using machine learning. Mater. Today: Proc.

[3]. Akhavan-Hejazi, H., Mohsenian-Rad, H., 2018. Power systems big data analytics: An assessment of paradigm shift barriers and prospects. Energy Rep. 4, 91–100.

[4]. Al-Ghamdi, M.I., 2021. Effects of knowledge of cyber security on prevention of attacks. Mater. Today: Proc.

[5]. Al Shaer, D., et al., 2020. Hydroxamate siderophores: Natural occurrence, chemical synthesis, iron binding affinity and use as Trojan horses against pathogens. Eur. J. Med. Chem. 208, 112791.

[6]. Alghamdi, M.I., 2021. Determining the impact of cyber security awareness on employee behaviour: A case of Saudi Arabia. Mater. Today: Proc.

[7]. Alghamdie, M.I., 2021. A novel study of preventing the cyber security threats. Mater. Today: Proc. Alhayani, B., et al., 2021. Best ways for computation intelligent of face cyber attacks. Mater. Today: Proc.

[8]. Alibasic, A., et al., 2016. Cybersecurity for smart cities: A brief review. In: International Workshop on Data Analytics for Renewable Energy Integration. Springer.

[9]. Alkatheiri, M.S., Chauhdary, S.H., Alqarni, M.A., 2021. Seamless security apprise method for improving the reliability of sustainable energy-based smart home applications. Sustain. Energy Technol. Assess. 45, 101219.

[10]. Alzubaidi, A., 2021. Cybercrime awareness among Saudi nationals: Dataset. Data Brief 36, 106965. Amir, M., Givargis, T., 2020. Pareto optimal design space exploration of cyber–physical systems. Internet Things 12, 100308.

[11]. Arend, I., et al., 2020. Passive- and not active-risk tendencies predict cyber security behavior. Comput. Secur. 97, 101964.

[12]. Ashraf, J., et al., 2021. IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities. Sustainable Cities Soc. 72, 103041.

[13]. Aziz, A.A., Amtul, Z., 2019. Developing Trojan horses to induce, diagnose and suppress Alzheimer's pathology. Pharmacol. Res. 149, 104471.

[14]. Baig, Z.A., et al., 2017. Future challenges for smart cities: Cyber-security and digital forensics. Digit. Investig. 22, 3–13.

[15]. Beechey, M., Kyriakopoulos, K.G., Lambotharan, S., 2021. Evidential classification and feature selection for cyber-threat hunting. Knowl.-Based Syst. 226, 107120.

[16]. Bullock, J.A., Haddow, G.D., Coppola, D.P., 2021. Cybersecurity and critical infrastructure protection. In: Bullock, J.A., Haddow, G.D., Coppola, D.P. (Eds.), Introduction to Homeland Security, sixth ed. Butterworth-Heinemann, pp. 425–497 (Chapter 8).

[17]. Cao, Y., et al., 2019. A topology-aware access control model for collaborative cyber-physical spaces: Specification and verification. Comput. Secur. 87, 101478.

[18]. Cao, J., et al., 2021. Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks. Inform. Sci. 548, 69–84.

About The Author

Mr. Malvinder Singh completed his Master of Computer Application from Maharishi Dayanand University, Rohtak in 2009. He is currently working in the capacity of an Assistant Professor in the Department of Computer Science, at Miri Piri Khalsa College, Bhadaur since 2009. He has published more than 4 research papers at National and International Conferences. His areas of interest are Network Security and Cloud Security.