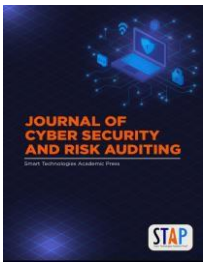
STAP
Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/



Applying risk analysis for determining threats and countermeasures in workstation domain

Rama Soliman Mousa[1], Rami Shehab[2]

[1] *King Abdullah the II IT School, University of Jordan, Amman 11942, Jordan*
[2] *Department of Computer Networks and Communications, King Faisal University, Al-Ahsa 31982, Saudi Arabia*

ARTICLE INFO

Article History
Received 05 Jan 2025
Accepted 22 Jan 2025
Published 25 Jan 2025

Academic Editor:
Mohammed Almaiah

Vol.2025, No.1

DOI:
https://doi.org/10.63180/jcsra.thestap.2025.1.2

ABSTRACT

The main purpose of this research is to perform a comprehensive analysis of cyber risks in workstation domain, including classifying threats, vulnerabilities, impacts, and countermeasures. This classification helps to identify suitable security controls to mitigate cyber risks for each type of attack. Additionally, this study aims to explore the main vulnerabilities based on the type of attack in workstation domain. This study employs the content analysis technique to collect, analyze, and classify data in terms of types of threats, vulnerabilities, and countermeasures. The methodology comprises four primary steps: (1) identifying key components, (2) threat identification, (3) vulnerability identification, and (4) countermeasure identification. The findings indicate that malware attacks and man in middle attacks were the most prevalent attacks in workstation domain, each accounting for 27% and 25% of incidents. The results found that unpatched software and weak access controls were classified as the most critical threats in the workstation domain, comprising 21% and 20% of incidents, respectively. The results also indicated that encryption methods, access controls mechanisms and firewall malware protection are the most significant and effective countermeasures for protecting the workstation domain environment. The findings of this study provides valuable recommendations for academic research in classifying the different types of cyber threats and understanding the significant security controls against cyber-attacks in workstation domain.

Keywords: Workstation Domain; Cyber threats; Vulnerabilities; Countermeasures; and Risk Management.

How to cite the article

Mousa, R. S., & Shehab, R. (2025). Applying risk analysis for determining threats and countermeasures in workstation domain. Journal of Cyber Security and Risk Auditing, 2025(1), 12–21. https://doi.org/10.63180/jcsra.thestap.2025.1.2

1. Introduction

Workstation security refers to the measures taken to ensure the protection of computer systems and data in workstations, especially in environments like lobby desks where the public is assisted [1]. It involves designing the workstation to be secure. Workstations may not be as prone to attack as networks or servers, but since they often contain sensitive data, such as credit card information, they are targeted by system crackers [2]. Workstations can also be co-opted without the user's knowledge and used by attackers as "slave" machines in coordinated attacks. For these reasons, knowing the vulnerabilities of a workstation can save users the headache of reinstalling the operating system, or worse, recovering from data theft [3].

Majority of enterprise security, a company's primary focus tends to be on the risk of an external cyberattack. While for workstations, it's also vital to consider vulnerabilities inside your organization. In workstations, employees represent the

*Corresponding author. Email: rshehab@kfu.edu.sa

most significant security threat to the business, all your other information technology security measures will be in vain if you fail to uphold workstation security. Where 95% of all cyberattacks can be traced directly to human error. Therefore, understanding these threats and risks will help security analysts better protect workstation domain assets [4].

Previous studies [5-10] have highlighted several security issues in workstation domain, including malware, social engineering attacks, outdated or unpatched software and misconfigured firewalls / operating systems. Malware such as Trojans, viruses, and worms that are installed on a user's machine or a host server. Social engineering attacks that fool users into giving up personal information such as a username or password. Outdated or unpatched software that exposes the systems running the application and potentially the entire network. Misconfigured firewalls / operating systems that allow or have default policies enabled. These vulnerabilities can lead to more advanced attacks such as a DDoS (distributed denial of services) attack, which can bring a network down to a crawl or prevent users from accessing it. Workstation vulnerabilities are always at threat of being compromised as malicious actors search to exploit and gain access into your business's system. For instance, the workstation's OS can have a known software vulnerability that allows a hacker to connect remotely and steal data. A workstation's browser can have a software vulnerability which allows unsigned scripts to silently install malicious software. A workstation's hard drive can fail causing lost date. [1] Investigated the effect of cyber-attack like phishing attack on the workstation domain and found that the success of this type of attack was almost 20% in any node in the workstation.

Therefore, understanding potential security risks is crucial in risk assessment and should be considered when developing a robust security strategy to prevent data breaches. Security risk assessment plays a vital role in identifying potential threats, implementing proactive security measures, and mitigating the likelihood of successful attacks. Cybersecurity risk assessment for workstation is an ongoing process rather than a one-time task. By identifying and classifying risks, implementing appropriate security controls, and evaluating their effectiveness, organizations can significantly reduce potential threats and risks in workstation. Consequently, the study purpose to achieve the following objectives:

(1) To analyze the critical cybersecurity threats in workstation domain.

(2) To analyze the critical cybersecurity vulnerabilities in workstation domain.
(3) To analyze the critical cybersecurity countermeasures in workstation domain.

1. Literature Review

2.1 Cybersecurity Attacks in Workstation domain

Previous studies have studied several cyber-attacks in workstation domain. For instance, Lerums et al. [1] investigated the effect of cyber-attack like phishing attack on the workstation domain and found that the success of this type of attack was almost 20% in any node in the workstation. Another attack happened in 2012 known as Shamoon attack on Saudi Arabia's Saudi Aramco and Qatar's RasGas [2]. Where, the attacker sent phishing email with attachment file contains malicious code. The attack impacted more than 30,000 workstations and caused down on the services and computers [2]. Previous studies have highlighted several types of security attacks in workstation domain, including:

(A) Malware

Malware is a malicious software that is unknowingly purchased, downloaded, or installed. Systems infected with malware will present with symptoms such as running slower, sending emails without user action, randomly rebooting, or starting unknown processes. The most common types of malware include: Viruses, Key-loggers, Worms, Trojans, Ransomware, Logic Bombs, Bots/Botnets, Adware & Spyware and Rootkits.

(B) Social Engineering Attacks

Social engineering attacks have become a popular method used by threat actors to easily bypass authentication and authorization security protocols and gain access to a network. These attacks have increased significantly in the last 5 years

becoming a lucrative business for hackers. Internal users pose the greatest security risk to an organization typically because they're uneducated or unaware of the threat. Accidentally downloading an attachment or clicking a link to a website with malicious code can cost thousands in damages. The most common types of social engineering attacks include Phishing emails, Spear phishing, Whaling, Vishing, Smishing, Spam, Pharming, Tailgating, Shoulder surfing and Dumpster diving.

(C) Outdated or Unpatched Software

Actually, software developers are constantly coming out with new patches to fix bugs and errors to reduce vulnerabilities. Some applications are millions of lines of code long making vulnerabilities an inevitable part of software deployment. As a result, developers deploy patches to software to remediate these vulnerabilities, although patches may also be performance or feature upgrades. Maintaining the security of software code is an ongoing battle, with major companies like Facebook, Apple, and Microsoft releasing patches daily to defend against new cyber threats.

(D) Misconfigured Firewalls

One of the most significant threats to an organization is exposing your internal network or servers to the internet. When exposed, threat actors are easily able to spy on your traffic, steal data, or compromise the network. Figure 1 represents the domain of workstation.

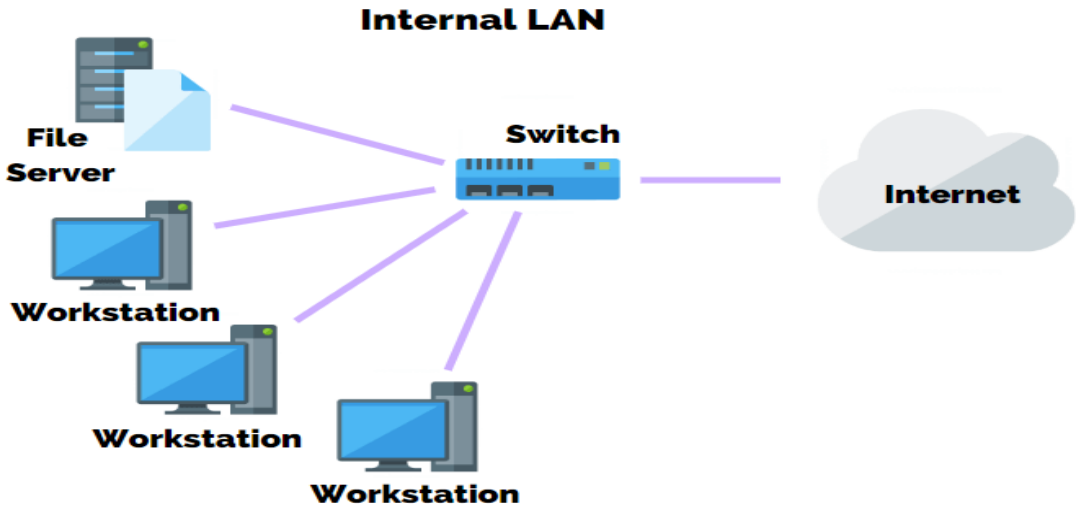


Figure 1. Workstation domain architecture.

3. Research Methodology

This section outlines the research design for proposing a risk assessment methodology for workstation domain. The methodology comprises four primary stages: (1) identifying key components, (2) threat identification, (3) vulnerability identification, and (4) countermeasure identification. Each stage is informed by the findings from the literature review. The primary objective of this risk assessment framework is to provide a robust and comprehensive approach for addressing all types of threats, vulnerabilities, and countermeasures in workstation domain. Figure 2 represents the main steps of the research methodology for this research.

3.1 Stage One: Identifying key components

The initial phase of the risk assessment framework involves compiling data from literature review findings to establish the dataset for this study. This process entails a comprehensive examination of existing studies, models, frameworks, and

literature in the field of workstation domain. The collected data encompasses threat types, vulnerability categories, and countermeasure methodologies. The information gathered during this stage will undergo analysis in subsequent phases.

3.2 Stage Two: Threats identification

Following data collection in the first stage, the subsequent phase involves analyzing the gathered information to identify and categorize existing cybersecurity threats in workstation domain. This stage encompasses a comprehensive and systematic process that identifies various types of threats with the potential to exploit vulnerabilities in database systems, potentially resulting in compromised systems.

3.3 Stage Three: Vulnerabilities identification

In the third stage, following data collection, an analysis is conducted to identify existing technical security vulnerabilities that could potentially compromise workstation domain. This stage of the risk assessment framework incorporates a comprehensive systematic review to determine critical vulnerability types that may be exploited to breach workstation domain.

3.4 Stage Four: Countermeasures identification

The final phase of the risk assessment framework involves identifying and categorizing effective countermeasures to address potential cybersecurity threats and vulnerabilities in workstation domain. The identification of these countermeasures is directly linked to all types of threats and vulnerabilities identified in the previous stages' findings. Consequently, this stage provides solutions to mitigate potential threats that could compromise the integrity of workstation domain.

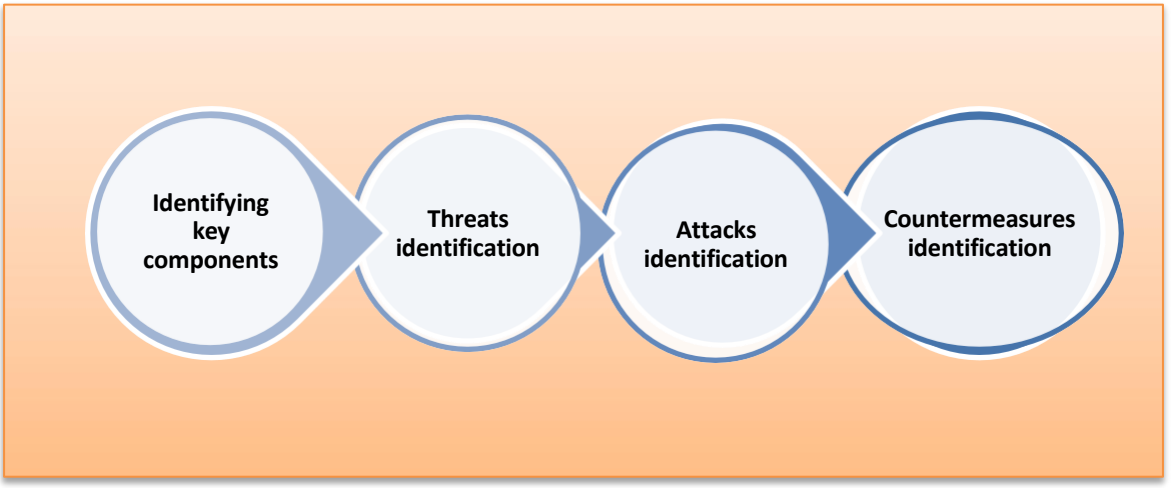


Figure 2. Steps of the research methodology.

4. Threats Identification

The threat classification was categorized based on the impact of attacks and threats in workstation domain. Workstation threats encompass malware types that exploit security weaknesses in the IT infrastructure of workstation domain, such as data breaches, outdated or unpatched software and social engineering. The classification analysis is based on multiple dimensions, including threat characteristics, behaviors, and their impacts. Each threat type is described with an explanation of its potential impact on workstation domain. The subsequent subsections provide a detailed threats classification on workstation domain. Table 1 represents the classification of cyber threats, attacks and their impacts.

(A) Malware Attacks:

Assets affected: OS, user Credentials, files and data. Malware Attacks have disastrous effects on an organization's workstation. They can lead to unauthorized access, data theft, system crashes, and significant downtime. Their effect can

even go beyond that to effect the organization's reputation and financial state. Furthermore, the cost of redemption after those attacks is considered very high.

(B) Man in the Middle:

Assets affected: Communication channels, Sensitive data, including login passwords, bank account information, and confidential company information, may be compromised by this kind of attack since the attacker can watch over and alter data while it is in transit without the parties' awareness. A MitM assault can have serious consequences, including unapproved access, data breaches, and a decline in partner and client trust.

(C) Advanced Persistent Threats (APTs):

Assets affected: User accounts, system logs, intellectual property. APTs have the ability to enter workstations through many techniques, such as phishing, malware, or using security flaws in the system. They frequently work on stealing confidential data, interfering with daily activities, or engaging in espionage. Because APTs are long lasting, attackers can create a lasting presence and cause a great amount of harm by stealing data, stealing intellectual property, and interfering with operations.

(D) Network Spoofing:

Assets affected: Network access points, network traffic. By tricking computers and users into engaging with phony or malicious network resources, network spoofing attacks on an organization's workstation domain can have detrimental influence. Attackers can eavesdrop on network traffic using methods like rogue access points or IP address spoofing. This can result in compromised communications, data breaches, or unwanted access to confidential data. The integrity of network operations may be compromised by these assaults, which could result in data loss, system failures, and sometimes monetary losses.

(E) Phishing Attacks:

Assets affected: Email accounts, financial information. This attack can result in unauthorized access to critical applications and data breaches. Using this attack hackers may be able to access company networks without authorization, breach user credentials, and steal confidential information.

(F) Social Engineering:
Assets affected: Internal Policies, Access Controls. This attack results in data breaches, illegal access, and manipulation of security measures; frequently, this is done by taking advantage of psychological flaws in people rather than technological ones.

(G) Physical Threats:
Assets affected: Office Infrastructure, Hardware, Workstations. These risks may lead to hardware damage or loss, the disclosure of private information kept on tangible devices, and even the possibility of an interruption in business operations.

Table 1. Classification of cyber threats, attacks and their impacts.

Type of attack or threat	Description
Malware [1][4][6] [23]	Malicious software used to poison software and take over OS
Man-in the Middle (MITM) [10]	An attacker secretly intercepting and potentially altering communications between two parties
Advanced Persistent Threats(APTs) [1][22][14]	Long-term cyberattack where adversaries gain and maintain unauthorized access to a network or system
Network Spoofing [23]	Creating fake network services or devices to deceive users and intercept, redirect, or manipulate network traffic for malicious purposes.
Phishing Attacks [1][4][22]	Attempts to obtain sensitive information by pretending to be a trustworthy entity, usually through email.
Social Engineering [1][4][22]	Gaining information by manipulating individuals
Physical Threats [1][4][19]	Unauthorized physical access to or damage of hardware, such as stealing or tampering with workstations.
BYOD Risks[9]	(Bring Your Own Device) risks, using personal devices to access company resources without proper security controls.

Brute Force Attacks *[4][21]*	trying all possible password combinations to gain unauthorized access to a system
DoS-DDoS [4][22][14]	Overloading a network, service, or server with excessive traffic to render it unavailable to legitimate users

5. Vulnerabilities Identification

The second step of the methodology aims to identify the technical security vulnerabilities that could be exploited to compromise the workstation domain ' assets. These vulnerabilities may be associated with either single or multiple operational or cyber security threats. Vulnerability scans and assessments are crucial steps in the risk assessment process to identify critical technical vulnerabilities. In this study, the classification of vulnerabilities is divided based on the type of attacks such as in malware attack, the main vulnerabilities related to this type of attack are Lack of antivirus and anti-malware software, unsecured download sources, software with security flaws. For man in middle attack, the vulnerabilities including: insecure Wi-Fi networks, unencrypted communications, lack of intrusion detection/prevention systems (IDS/IPS). Table 2 summarizes the main technical vulnerabilities in workstation domain.

Table 2. Classification of the main technical vulnerabilities in workstation domain.

Type of attack or threat	Description
Malware	Lack of antivirus and anti-malware software, Unsecured download sources, software with security flaws.
Man-in the Middle(MITM)	Insecure Wi-Fi networks, Unencrypted communications, Lack of intrusion detection/prevention systems (IDS/IPS).
Advanced Persistent Threats(APTs)	Lack of employee security training, Weak access controls and user permissions.
Network Spoofing	Unsecured Wi-Fi networks, Weak encryption protocols.
Phishing Attacks	Lack of employee awareness and training, Weak or easily guessable passwords. Lack of multi-factor-authentication
Social Engineering	Weak security policies and procedures, Absence of a strong security culture.
Physical Threats	Weak policies for handling sensitive hardware. Weak physical security controls and guarding.
BYOD Risks	Weak security policies for personal devices, Lack of employee training on secure usage of personal devices.
Brute Force Attack	Reuse of passwords across multiple accounts and services, Lack of account lockout mechanisms after multiple failed login attempts.
DoS-DDoS	Lack of DDoS mitigation services and tools, Absence of rate limiting and traffic shaping controls.

6. Countermeasures Identification

In this phase, we conduct a comprehensive analysis of essential countermeasures aimed at reducing and mitigating the impact of vulnerabilities associated with cyber threats. Our study identified a range of security controls designed to enhance workstation domain system security against cyber-attacks. These measures include data encryption, access control, authentication, firewalls, data backup, IP blacklisting and filtering, and others. Security controls and countermeasures are mechanisms and tools developed to protect workstation domain from cyber threats and attacks. These countermeasures are crucial for maintaining data integrity and safeguarding workstation systems from unauthorized access. They can be categorized into several types based on the type attacks. For example, Table 3 to Table 11 include the main countermeasures for types of attacks including antivirus Software, user training, firewalls, backup and recovery solutions.

Table 3. Countermeasures for malware attack.

Countermeasure	Effectiveness
Antivirus Software	Generally effective at detecting known malware. Regular updates and scans are crucial for maintaining effectiveness.
User Education and Training	Can be very effective in reducing the risk of malware infections caused by user error. The results depend on the quality of training.
Firewalls	Effective at blocking unauthorized access and certain types of malware from entering the network. However, they may not prevent all forms of malware
Backup and Recovery Solutions	Highly effective in recovering from data loss due to malware attacks. Regular backups can minimize downtime and data loss.

Table 4. Countermeasures for man in middle attack.

Countermeasure	Effectiveness
Encryption	Highly effective in preventing MitM attacks by ensuring data confidentiality and integrity.
Two-Factor Authentication (2FA)	Enhances overall security by adding an extra layer of protection.
VPNs (Virtual Private Networks)	Very effective in securing data transmitted over untrusted networks, such as public Wi-Fi.
Network Segmentation and Monitoring	Effective in reducing the attack surface and detecting potential MitM attacks. While segmentation limits the impact of attacks, continuous monitoring helps in identifying and responding to suspicious activities.

Table 5. Countermeasures for Advanced Persistent Threats (APTs).

Countermeasure	Effectiveness
Incident Response Planning	Critical for minimizing the impact of an APT incident response plan ensures coordinated efficient response.
Advanced Threat Protection (ATP)	Highly effective by providing a multi-layered defense approach. Integrate various security technologies and intelligence to detect threats.
Red and Blue Team Exercises	Very effective in identifying gaps in security and improving incident response.

Table 6. Countermeasures for spoofing attack.

Countermeasure	Effectiveness
Regular Network Monitoring	Effective in detecting and responding to network spoofing attempts. The effectiveness depends on the accuracy of the monitoring tools
Encryption of Network Traffic	Very effective in protecting data in transit from being intercepted or altered.
IP Source Guard	Very effective in blocking IP spoofing attacks. Its effectiveness relies on accurate binding information.

Table 7. Countermeasures for phishing attack

Countermeasure	Effectiveness
Email Filtering and Anti-Phishing Software	Very effective in blocking known phishing emails and malicious attachments.
Phishing Simulation and Testing	Highly effective in assessing and improving employees' ability to recognize and respond to phishing attacks.

Web Browser Security Extensions	Useful for providing additional warnings and protections against phishing websites while browsing.
Regular Security Audits and Penetration Testing	Very effective for identifying and addressing potential weaknesses in phishing defenses.

Table 8. Countermeasures for Social engineering attack

Countermeasure	Effectiveness
Access Controls and Least Privilege	Effective in limiting the damage from social engineering attacks by restricting access to sensitive information and systems.
Clear Desk and Screen Policies	Effective in reducing the risk of information leakage through casual social engineering techniques
Security Awareness Training	Highly effective in reducing the success rate of social engineering attacks by improving employees' ability to identify and respond to attempts.

Table 9. Countermeasures for physical attack

Countermeasure	Effectiveness
Security Guards	Highly effective in providing a physical presence and immediate response to security incidents.
Alarm Systems	Effective in detecting and responding to breaches in real-time.
Environmental Controls	Effective in protecting physical assets from environmental threats.

Table 10. Countermeasures for Brute force attack

Countermeasure	Effectiveness
Password Hashing	Highly effective in protecting stored passwords from being easily decrypted.
Strong Password Policies	Effective in making brute force attacks more time-consuming and difficult.
Account Monitoring and Alerting	Effective in providing early warning of potential brute force attacks

Table 11. Countermeasures for DDoS attack.

Countermeasure	Effectiveness
Rate Limiting	Effective in mitigating smaller-scale DoS attacks by controlling traffic flow and preventing abuse.
Web Application Firewalls	Effective in protecting web applications from a variety of attacks.
Load Balancing	Effective in managing traffic loads and improving resilience against DoS attacks.
IP Blacklisting and Filtering	Effective in preventing known malicious traffic from reaching the network.

7. Conclusion

Understanding potential security risks is crucial in risk assessment and should be considered when developing a robust security strategy to prevent data breaches. Security risk assessment plays a vital role in identifying potential threats, implementing proactive security measures, and mitigating the likelihood of successful attacks. Cybersecurity risk assessment for workstation is an ongoing process rather than a one-time task. By identifying and classifying risks, implementing appropriate security controls, and evaluating their effectiveness, organizations can significantly reduce potential threats and risks in workstation. Consequently, the study purpose to analyze the critical cybersecurity threats in workstation domain. The findings indicate that malware attacks and man in middle attacks were the most prevalent attacks in workstation domain, each accounting for 27% and 25% of incidents. The results found that unpatched software and weak access controls were classified as the most critical threats in the workstation domain, comprising 21% and 20% of incidents,

respectively. The results also indicated that encryption methods, access controls mechanisms and firewall malware protection are the most significant and effective countermeasures for protecting the workstation domain environment. The findings of this study provides valuable recommendations for academic research in classifying the different types of cyber threats and understanding the significant security controls against cyber-attacks in workstation domain.

Conflicts Of Interest

The authors declare no conflicts of interest.

Funding

No funding.

Acknowledgment

References

[1] Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., & Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*, *112*, 102494.

[2] Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of Things*, *11*, 100227.

[3] Rana, M., Mamun, Q., & Islam, R. (2022). Lightweight cryptography in IoT networks: A survey. *Future Generation Computer Systems*, *129*, 77-89.

[4] Ravi, N., & Shalinie, S. M. (2020). Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture. *IEEE Internet of Things Journal*, *7*(4), 3559-3570.

[5] Lee, E., Seo, Y. D., Oh, S. R., & Kim, Y. G. (2021). A Survey on Standards for Interoperability and Security in the Internet of Things. *IEEE Communications Surveys & Tutorials*, *23*(2), 1020-1047.

[6] Mohanta, B. K., Jena, D., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H. (2020). Addressing security and privacy issues of IoT using blockchain technology. *IEEE Internet of Things Journal*, *8*(2), 881-888.

[7] Grammatikis, P. I. R., Sarigiannidis, P. G., & Moscholios, I. D. (2019). Securing the Internet of Things: Challenges, threats and solutions. *Internet of Things*, *5*, 41-70.

[8] Kumar, R. L., Khan, F., Kadry, S., & Rho, S. (2022). A survey on blockchain for industrial internet of things. *Alexandria Engineering Journal*, *61*(8), 6001-6022.

[9] Rao, P. M., & Deebak, B. D. (2023). Security and privacy issues in smart cities/industries: technologies, applications, and challenges. *Journal of Ambient Intelligence and Humanized Computing*, *14*(8), 10517-10553.

[10] Sharma, P., Jain, S., Gupta, S., & Chamola, V. (2021). Role of machine learning and deep learning in securing 5G-driven industrial IoT applications. *Ad Hoc Networks*, *123*, 102685.

[11] Santhosh Kumar, S. V. N., Selvi, M., & Kannan, A. (2023). A Comprehensive Survey on Machine Learning-Based Intrusion Detection Systems for Secure Communication in Internet of Things. *Computational Intelligence and Neuroscience*, *2023*(1), 8981988.

[12] Younan, M., Houssein, E. H., Elhoseny, M., & Ali, A. A. (2020). Challenges and recommended technologies for the industrial internet of things: A comprehensive review. *Measurement*, *151*, 107198.

[13] Yugha, R., & Chithra, S. (2020). A survey on technologies and security protocols: Reference for future generation IoT. *Journal of Network and Computer Applications*, *169*, 102763.

[14] Nikou, S. (2019). Factors driving the adoption of smart home technology: An empirical assessment. *Telematics and Informatics*, *45*, 101283.

[15] Ande, R., Adebisi, B., Hammoudeh, M., & Saleem, J. (2020). Internet of Things: Evolution and technologies from a security perspective. *Sustainable Cities and Society*, *54*, 101728.

[16] Hajiheidari, S., Wakil, K., Badri, M., & Navimipour, N. J. (2019). Intrusion detection systems in the Internet of things: A comprehensive investigation. *Computer Networks*, *160*, 165-191.

[17] Manzoor, A., Braeken, A., Kanhere, S. S., Ylianttila, M., & Liyanage, M. (2021). Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain. *Journal of Network and Computer Applications*, *176*, 102917.

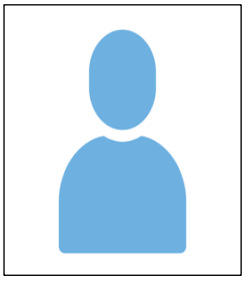
[18] Zhu, Q., Loke, S. W., Trujillo-Rasua, R., Jiang, F., & Xiang, Y. (2019). Applications of distributed ledger technologies to the internet of things: A survey. *ACM computing surveys (CSUR)*, *52*(6), 1-34.

[19] Haghi, M., Neubert, S., Geissler, A., Fleischer, H., Stoll, N., Stoll, R., & Thurow, K. (2020). A flexible and pervasive IoT-based healthcare platform for physiological and environmental parameters monitoring. *IEEE Internet of Things Journal*, *7*(6), 5628-5647.

[20] NV, R. K., & E, B. (2022). Detection and monitoring of the asymptotic COVID-19 patients using IoT devices and sensors. *International Journal of Pervasive Computing and Communications*, *18*(4), 407-418.

[21] Shahin, M., Maghanaki, M., Hosseinzadeh, A., & Chen, F. F. (2024). Advancing network security in industrial IoT: a deep dive into AI-enabled intrusion detection systems. *Advanced Engineering Informatics*, *62*, 102685.

[22] Zhang, J., Li, L., Lin, G., Fang, D., Tai, Y., & Huang, J. (2020). Cyber resilience in healthcare digital twin on lung cancer. *IEEE access*, *8*, 201900-201913.
[23] Shirvanimoghaddam, M., Shirvanimoghaddam, K., Abolhasani, M. M., Farhangi, M., Barsari, V. Z., Liu, H., ... & Naebe, M. (2019). Towards a green and self-powered Internet of Things using piezoelectric energy harvesting. *Ieee Access*, *7*, 94533-94556.
[24] Rao, P. M., & Deebak, B. D. (2023). A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions. *Ad Hoc Networks*, *146*, 103159.



Rama Soliman Mousa is studying a cybersecurity in the University of Jordan, Jordan. She has published several papers in well reputed journals and conferences. Her research interests include cybersecurity, cybersecurity risk assessment and cryptographic .

Rami Shehab is working as a lecturer at the College of Computer Sciences and Information Technology, King Faisal University (KFU), Saudi Arabia. He has published several papers in well reputed journals and conferences. His research interests include cybersecurity, cybersecurity risk assessment and cryptographic .