A Targeted Approach for Building a Secure Air-Gapped System

Esmail Siahloui[1*], Seyed Reza Tabatabaei Manesh[2]

[1] PhD, Department of Computer Science, Science Campus, Faculty of Mathematics, Yazd University, Yazd, Iran
[2] PhD Student, Department of Cyberspace Strategic Management, National Defense University, Tehran, Iran

*** Corresponding author email address**: Siahlooei@gmail.com

Received: 2024-11-05 **Reviewed:** 2025-01-25 **Revised:** 2025-02-01 **Accepted:** 2025-02-09 **Published:** 2025-09-01

Abstract

This study aims to present a targeted strategy for developing a methodology that leads to the design and implementation of an air-gapped system. The research integrates existing technologies from the fields of physics, cybersecurity, data transmission, physical protection, cryptography, and encoding. This paper is based on studies conducted on attacks targeting air-gapped systems, identifying vulnerabilities in each system, and subsequently proposing a solution. To achieve this, over 150 reputable global research articles were reviewed. In air-gapped systems, networked computer communications—whether wired or wireless—between the internal and external environments do not exist. As a result, these systems offer a higher level of security. However, studies indicate that they may still be vulnerable. This paper attempts to introduce a method that results in the creation of a structured list of tasks. Following this list aligns with organizational objectives for establishing an air-gapped system and ultimately leads to the design and implementation of such a system.

Keywords: *security, cybersecurity, data transmission, air gap, intrusion.*

How to cite this article:

Siahloui, E., & Tabatabaei Manesh, S. R. (2025). A Targeted Approach for Building a Secure Air-Gapped System. Management Strategies and Engineering Sciences, 7(5), 1-8.

1. Introduction

Throughout history, the security of human assets has always been a major concern. Since the beginning of human civilization, individuals have been sensitive about their possessions and have constantly sought to keep their valuable assets out of the reach of unauthorized individuals. In ancient times, people used to hide their valuables or secrets in chests, keeping them away from untrustworthy persons, effectively severing external access to their belongings. In some cases, assets were packaged and sealed and entrusted to individuals renowned for their reliability. Likewise, people were highly cautious in safeguarding their confidential information, ensuring that their important secrets were not shared with anyone else [1].

In today's world, where a significant portion of individuals' assets and confidential information is stored digitally, the crucial question arises: how can these digital assets be protected? Many computer systems incorporate encryption and secure storage tools. These tools are also available on mobile phones, allowing widespread usage [2-4].

High-speed internet has only recently become widely accessible, enabling the effortless transfer of information from any system to the internet, making it accessible to everyone or a specific group of individuals. Large video files and other data can be disseminated at unprecedented speeds, exposing them to numerous viewers. In this digital landscape, neglecting data protection could result in the loss of valuable information or allow unauthorized third parties to exploit such data [5].

Moreover, the presence of malware has increasingly threatened both personal data security and financial security, putting individuals at risk of losing their assets. One prominent example of such malware is ransomware, which can compromise a system, take control of specific files or information, and demand a ransom from its victim. While security software installed on computers and mobile devices can counteract malware, newly developed malware often evades detection, rendering these security measures ineffective. Consequently, systems equipped with security tools may still suffer from cyber threats [6]. Additionally, sophisticated malware can bypass security software defenses and infect systems.

In large organizations, advanced security tools and hardware are deployed to mitigate such attacks, imposing significant financial costs. However, no organization is entirely immune to internet-based malware threats. Consequently, alternative strategies, such as disconnecting internet access from organizational networks, have been proposed as a defense mechanism against cyberattacks [7-9].

Modern malware has evolved to employ new and sophisticated attack techniques, targeting general, global, or specialized systems. Many of these advanced malware programs are highly persistent and can evade conventional security measures. Some of these malware variants are designed for espionage and cyber sabotage, adapting over time to technological advancements and emerging threats (Nyholm et al., 2022). These malware programs operate stealthily, remaining undetected until they achieve their intended objectives. They often employ encrypted covert communications and advanced attack techniques, making detection increasingly challenging. Conventional security measures, such as antivirus and anti-malware systems, may be incapable of identifying new strains of such malware. Some of these advanced threats can bypass firewalls and infiltrate protected networks (Aboaoja et al., 2022).

The primary objectives of malware, along with its methods of propagation and transmission, have evolved over time due to changes in the technological landscape and environmental factors. For example, with the proliferation of high-speed internet, data-stealing malware became widespread. As web-based applications and mobile applications gained popularity, password theft malware became more common. The advent of cryptocurrencies led to the emergence of ransomware as a prevalent threat. Similarly, with the introduction of air-gapped systems, specialized malware was developed to target these systems, successfully compromising some organizations. Consequently, defensive strategies must be reinforced to counteract such threats. More importantly, air-gapped systems should be designed and implemented with the necessary resilience to withstand potential attacks.

This study proposes a solution for constructing secure systems, infrastructures, and organizations that must remain isolated from external networks. However, isolating a system from network communications presents significant challenges. These challenges become even more pronounced when cyberattacks target systems that have already been disconnected from the internet, compromising their security. Through an extensive review of previous cyberattacks and credible scientific research, this study introduces a structured approach tailored to organizational objectives and specific conditions. The proposed methodology provides a framework for designing, implementing, and operating an air-gapped system that remains resilient against cyber threats.

2. Methodology

The conducted research falls into the category of applied research, as its ultimate goal is to develop a practical method for establishing an organization with a high level of security. Furthermore, the current study is qualitative, meaning that the methods and techniques used for data collection and analysis were based on their qualitative nature. In terms of reasoning, a deductive and interpretative approach was adopted. Using an exploratory research method, the findings were formulated into a structured methodology and presented accordingly. The data foundation of this study comprises scientific and practical research articles related to cyberattacks on organizations, particularly air-gapped organizations.

3. Method for Constructing a Secure Air-Gapped System

This section presents a method for building an air-gapped system that is secure against specific attacks targeting such systems. Given that there is no network-based communication between this system and external networks, the proposed method ensures that any external interaction is regulated, making these communications controllable and traceable.

3.1. Examining Risky Inter-Organizational Communications

This section analyzes security risks, primarily those arising from uncontrolled interactions with external environments.

3.1.1. Organizational Responsibilities of Individuals

The security of an organization, particularly its cybersecurity, necessitates comprehensive knowledge and awareness across all organizational levels, including its members, employees, and other relevant personnel. Every individual within the organization holds a position where even a minor lapse in security protocols can severely compromise the overall security of the organization. Consequently, maintaining the security of an air-gapped organization requires seamless collaboration and coordination among all components of the system [10].

It is crucial to note that cyberattacks targeting air-gapped systems often begin with a single point of entry. Attackers exploit security gaps caused by negligence, lack of precaution, or an oversight by an employee within the organization. Once a weak point is identified, the attacker can infiltrate the system, gain the necessary access, and initiate an attack [11, 12].

3.1.2. The Relationship Between Organizational Security and Operational Procedures

One of the most critical aspects of air-gapped systems and external organizational communications is that no system can function effectively in complete isolation. In other words, the fundamental purpose of an organization is to interact with other organizations by exchanging data, resources, or personnel to fulfill its goals and benefit its stakeholders. Therefore, the notion that an organization can operate entirely independently, without any external interactions, is impractical.

External communication is essential for an efficient system. Hence, all entry and exit points for data, personnel, assets, and documents must be thoroughly monitored. Adequate security measures must be implemented, and a comprehensive document outlining these interactions should be prepared and communicated to employees [13].

Internal communications within the network must also be strictly regulated. Clear instructions should be defined for interactions between different subunits of the system, ensuring that only authorized personnel have access to necessary information. Additionally, if two subunits within an organization have no functional relationship, their communication should be strictly prohibited, and any attempt to establish contact should be flagged as suspicious and documented accordingly [10].

3.1.3. Permanent Staff

Permanent employees are individuals who have received training to work within the organization and have a long-term association with it. Naturally, these individuals possess extensive knowledge of the organization's internal systems. If this information is disclosed to unauthorized persons, it could pose a significant security threat [6, 14].

For instance, if an attacker learns that most of the organization's printers belong to a specific brand, they may develop malware targeting those devices, using them as a gateway to infiltrate the system. Therefore, employees must be strictly prohibited from sharing even seemingly insignificant details about the organization's infrastructure [15-17].

Additionally, employees must be cautious when bringing external devices, such as USB drives, smartphones, or other peripherals, into the organization, as these could introduce malware into the system. The organization’s physical security team is responsible for monitoring and controlling the entry and exit of such items [18, 19].

3.1.4. Temporary Personnel

Certain individuals who temporarily access the system do not have direct involvement in the organization's core functions. This category includes HVAC technicians, emergency medical staff, janitorial service providers, and other third-party service personnel. These individuals may enter and exit the system without any long-term commitment to the organization, and they typically have limited knowledge of its operations. However, they may gain access to restricted areas that are generally intended only for internal personnel [1, 2, 20].

As a result, security personnel must exercise strict supervision over these individuals. Interns and new employees also fall into this category, requiring additional monitoring. Their supervisors should oversee their activities, ensuring that they do not receive unnecessary or excessive access privileges [11, 16, 21, 22].

3.1.5. Archiving System

Documents should be meticulously reviewed and archived with precise classification. The archiving system must ensure that access to documents is granted based on an individual's designated privileges [6, 23].

It is recommended that a special classification be applied to records concerning personnel and object entry and exit within the system. These records can serve as a crucial reference in the event of a security breach or incident, enabling investigators to identify the source of the problem [21, 24].

3.1.6. Surveillance System

Monitoring tools such as surveillance cameras and other security devices must be deployed exclusively for recording necessary information. Cameras should never be positioned to capture sensitive documents or computer screens, as their footage could be exploited to extract organizational data [25, 26].

It is recommended that surveillance cameras be categorized based on security levels, ensuring that access to their feeds is restricted to authorized personnel according to their responsibilities. For example, entry and exit surveillance footage should only be accessible to security personnel managing building access, while internal movement surveillance should be handled by the internal security team.

By implementing these measures, an organization can strengthen its defense mechanisms against potential security threats while maintaining a structured and controlled operational framework.

3.2. Method Explanation

This method follows a step-by-step approach, progressively moving toward the completion of system design. At each step, all relevant factors are reviewed, considering the specific environmental conditions of the organization. Then, based on the data collected and analyses performed in previous steps, the next step is taken, gradually leading to a complete design. Additionally, the proposed method focuses not only on system design but also on implementation and post-implementation measures.

3.2.1. Understanding the System and Identifying Existing Risks

The primary aspect to consider is how data can exit the system. Since network-based data transmission is not available in air-gapped systems, alternative media must be considered for data transfer. The table below outlines different data exfiltration methods, their transmission mechanisms, and preventive measures.

Table 1. Data Transmission Risk Checklist

Data Exit Medium	Example of Transmission	Prevention Measures
Physical Devices	Data transfer via storage devices, mobile phones, or printed documents. Sender and receiver: human agents.	All items must be inspected by the security team upon exit.
Heat and Temperature	Data encoded into thermal pulses—caused by fluctuations in processor load or cooling system alterations. A sensor (or mobile phone) placed nearby can capture these changes. Sender: computer processor, cooling system.	Thermal insulation of computing systems, restriction of mobile phone access, monitoring anomalous power consumption patterns.
Sound	Data conversion into auditory or ultrasonic signals. Sender: microphone, speaker. Receiver: microphone, speaker, human agent.	Restrict unnecessary audio devices, soundproof relevant areas.
Visual Media	Encoding data into images, barcodes, or printed materials. Sender: monitor, printer, billboard. Receiver: human agent, camera.	Strengthen physical security, prevent monitor placement near windows, restrict billboards connected to internal networks, identify surveillance camera locations.
Electromagnetic Signals	Encoding data into electromagnetic pulses via electric current manipulation. Sender: graphics card, monitor cables. Receiver: radio devices, radio antennas.	Shielding systems, scanning for radio antennas near systems.
Electricity	Data converted into electrical pulse variations. Sender: power control units, electrical generators. Receiver: blinking lights, electrical sensors, power modems.	Periodic inspection of electrical power systems, monitoring unusual blinking lights, auditing electrical flow control components in the facility.
Light Signals	Encoding data into light pulses (visible or invisible) or Morse code. Sender: light-equipped devices (computer case, printer, Wi-Fi devices, mouse, keyboard, USB flash drives with LED lights). Receiver: camera, human agent.	Prevent exposure of light-emitting devices to windows or cameras, restrict the use of LED-equipped USB devices.
Noise (Acoustic or Vibrational)	Unintentional noise can be exploited for covert data transmission. Examples include system fan noise or vibrations from computer cases. Sender: system fan, vibrations. Receiver: audio sensors, vibration sensors (e.g., mobile phone accelerometers).	Prohibit mobile devices, repair areas producing unusual noise or vibrations, implement acoustic insulation.

Based on the above table and reviewed literature on cyberattacks, designing and implementing air-gapped systems requires expertise across multiple disciplines. The following table summarizes the required expertise and their respective roles in system security.

Table 2. Required Experts for Air-Gapped System Implementation

Expertise	Reason for Requirement

Physics Expert	Comprehensive knowledge of transmission media, such as sound, light, electromagnetism, and thermal radiation.
Data Encoding Specialist	Ensures data is encoded before transmission or reception. Identifies potential risks in encoded data transmission.
Communications and Networking Expert	Ensures secure and controlled intra-organizational communications. Designs and monitors secure network infrastructure.
Physical Security Personnel	Trained security personnel enforce pre-established security protocols for employees, system users, and clients.
Industry-Specific Specialists	For example, a financial expert in a banking organization is required to design secure data storage and classification methods.
Training Specialist	Provides security training for personnel to maintain system integrity.
Remote Security Specialist	Manages security monitoring systems such as surveillance cameras and logs critical organizational activity.

3.2.2. Roadmap Development and System Design

Once the necessary expertise is assembled and based on the knowledge gained from the data transmission table, the following steps must be taken to develop the system design documentation and proceed with implementation.

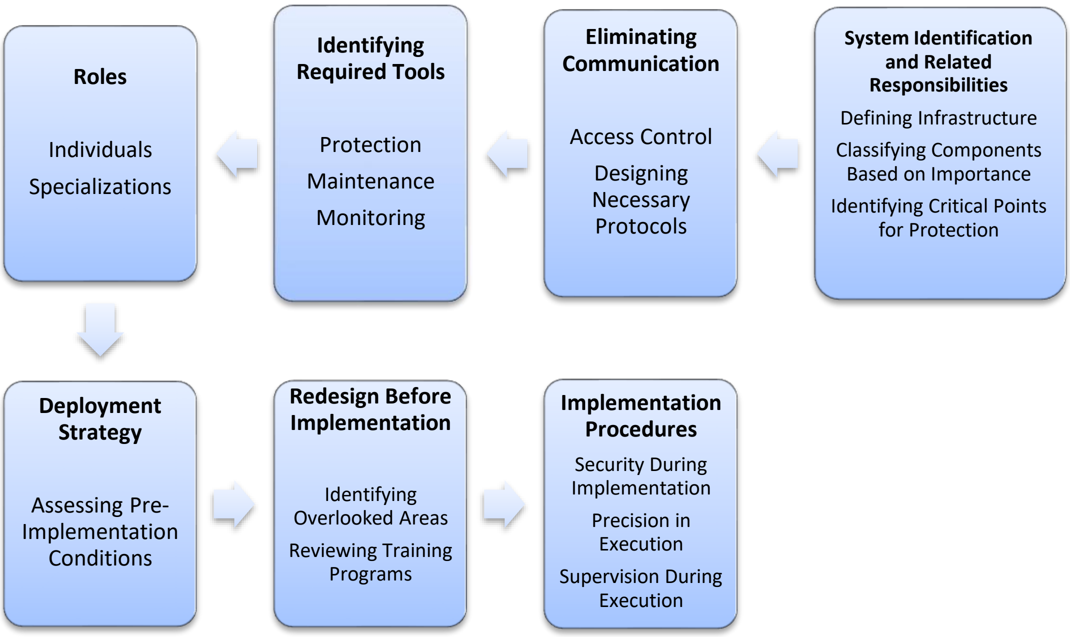
System Identification and Related Responsibilities
Defining Infrastructure
Classifying Components Based on Importance
Identifying Critical Points for Protection
Eliminating Communication
Access Control
Designing Necessary Protocols
Identifying Required Tools
Protection
Maintenance
Monitoring
Roles
Individuals
Specializations
Deployment Strategy
Assessing Pre-Implementation Conditions
Redesign Before Implementation
Identifying Overlooked Areas
Reviewing Training Programs
Implementation Procedures
Security During Implementation
Precision in Execution
Supervision During Execution

Figure 1. Steps for System Design and Documentation

1. **System Identification** – The first step in design involves defining the organization's objectives and thoroughly identifying its structural components. Data storage locations and infrastructure should be fully mapped and prioritized based on importance.
2. **Eliminating External Communications** – Before detailed design, all external communication channels should be severed. Necessary access permissions for each component must be determined, and communication protocols should be documented. For example, roles and access requirements for system components must be clearly outlined. External communication policies should also be established, ensuring the elimination of network-based connectivity.
3. **Identification of Monitoring and Maintenance Tools** – All software and hardware tools required for system oversight, maintenance, repair, cleaning, and security must be identified. Corresponding procedures should be documented.
4. **Personnel and Equipment Allocation** – Based on the previous steps, required specialists should be identified, their responsibilities documented, and a list compiled. Additionally, security sensors and monitoring devices should be planned and their installation sites determined. Detection mechanisms should be deployed for identifying attack behaviors, non-network communication attempts, and ongoing data transmission. Plans for component insulation should also be established.

5. **Component Deployment Strategy** – Each component's placement must follow predefined protocols and authorized internal communication guidelines. Security professionals should determine and document considerations such as environmental insulation, window placement, access control, cooling mechanisms, and surveillance devices. All system components should be reviewed together for consistency and alignment. Multiple iterations of this step may be necessary to refine the design.
6. **Simulated Attack Testing and Security Reinforcement** – Hypothetical attacks must be simulated on the system to identify vulnerabilities. Weak points or overlooked areas should be addressed and corrected. All previous documents may need revisions to strengthen security measures. Additionally, training documents related to personnel roles and system interactions should be compiled and distributed. Since a portion of training will focus on system maintenance and attack prevention, attack methodologies should be examined and included in educational materials.
7. **Implementation Procedures and Security Protocols** – At this stage, security protocols for the implementation phase should be finalized. For instance, sensitive areas must not be recorded during implementation, and no additional sensors should be installed within the organization's premises. Supervision methods for the implementation phase should be documented, and contractors must receive security training before commencing their work.

By following these steps, all documentation from the identification phase through implementation, maintenance, and training is consolidated within the overall system framework. These documents should be securely archived and referenced when necessary. Unauthorized access to these documents must be strictly prohibited.

3.2.3. Strengthening the System Against Attacks After Implementation

Given the critical role of surveillance systems, security mechanisms, and employee behavior in maintaining system security post-implementation, it is essential that personnel at all levels understand potential attack methods and implement necessary defensive measures. This section examines attack strategies from the perspective of an attacker and outlines corresponding defensive actions to reinforce system security.

Based on studies of real-world cyberattacks, most attacks follow a consistent pattern of intrusion and data exfiltration. The common steps in such attacks are outlined below:

Step 1: Acquiring System Knowledge – The attacker's first objective is to gather as much information as possible about the system. This can be achieved through various means, such as installing malware on employees' mobile devices for eavesdropping, engaging in conversations with employees to extract sensitive information, or monitoring the organization's physical environment.

Step 2: Injecting Malicious Code into the Organization – Once the attacker has obtained sufficient knowledge about the system, they will attempt to compromise at least one vulnerable component by introducing malware. The malware's primary function is to establish itself within the system, enabling data extraction or system sabotage. A vulnerable point is any location where software can be introduced into the system.

Step 3: Extracting Data from the System – Since the system is air-gapped and lacks network connectivity to external environments, data must be exfiltrated using alternative methods. As discussed in previous sections, attackers exploit various transmission media for this purpose. The key challenge for the attacker is establishing a connection between an internal sender and an external receiver.

Step 4: Delivering Data to the Sender – The malware's next task is to transmit collected data through an available medium. For example, if the system has an integrated speaker, the malware could take control of it to emit encoded signals containing sensitive information.

3.2.4. System Recovery Mechanisms

Another crucial aspect to consider during system design is the formulation of recovery procedures. System recovery is necessary when vulnerabilities are identified or an attack occurs. Although recovery is separate from the initial system design phase, it is essential for maintaining long-term system stability. The following steps contribute to a comprehensive recovery strategy:

- **Identifying responsible components, personnel, and roles** – This step involves reviewing surveillance reports and conducting inquiries to determine the source of the security breach.

- **Identifying vulnerable components or personnel** – Additional training and periodic refresher courses should be provided for individuals who demonstrate security weaknesses.
- **Analyzing and reinforcing the four key attack points** – This includes identifying and securing the points targeted by the attacker: (1) the information source within the system, (2) the malware entry point, (3) the malware's deployment location, (4) the internal transmission point, and (5) the external data reception point. New security protocols and detection sensors should be implemented to prevent future attacks.

3.2.5. Complementary Measures

During system operation, several key considerations must be upheld, particularly by security personnel and monitoring teams.

The first priority is continuous training. Employees should receive regular training to reinforce their understanding of permissible and prohibited behaviors. Periodic security training significantly enhances system resilience.

The second priority is behavioral monitoring. Unusual behavior must be identified at the earliest possible stage, and its potential negative impact should be assessed and mitigated. Steps should also be taken to prevent recurrence.

A critical aspect of security management is system maintenance and updates. Every software update and maintenance activity should be meticulously monitored, and the source of software updates must be verified. Additionally, maintenance personnel and technicians must possess appropriate security clearance and undergo thorough screening.

3.3. Outcomes and Results

Upon completing the outlined steps, a comprehensive design document will be produced, covering the following elements:

- System requirements and associated risks
- Design roadmap and finalized system architecture
- Operational guidelines for system utilization
- System recovery procedures
- Guidelines for training, monitoring, and system updates

4. Conclusion

Security, in any form, is beneficial for organizations. For organizations seeking protection against cyberattacks, disconnecting network communication with external environments is an effective strategy. However, this approach introduces its own set of challenges. The proposed method in this research demonstrates how to design and implement an air-gapped system or organization effectively.

Integrating air-gapped security measures within an organization necessitates the active participation of all employees and stakeholders. Every individual within the organization must acknowledge their role in maintaining system security.

This paper presents a structured methodology for establishing an air-gapped system that, while fully aligned with organizational requirements, remains resilient to all known attack vectors targeting such systems. This alignment ensures that the system not only meets the logical and functional needs of the organization but also addresses essential physical security concerns.

Furthermore, the proposed framework includes operational procedures for system utilization, recovery, and attack response. This ensures that, in the event of security threats, appropriate countermeasures can be deployed effectively. Additionally, preventive measures for system hardening have been incorporated, guaranteeing a comprehensive and secure system from all perspectives.

Authors' Contributions

Authors equally contributed to this article.

Acknowledgments

Authors thank all participants who participate in this study.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

References

[1] C. Heath-Kelly and Š. Shanaáh, "The long history of prevention: Social Defence, security and anticipat ing future crimes in the era of 'penal welfarism'," (in en), *Theoretical Criminology,* vol. 26, no. 3, pp. 357-376, 2022/8// 2022, doi: 10.1177/13624806211056313.

[2] A. E. Hassanien, M. Elhoseny, and SpringerLink, *Cybersecurity and Secure Information Systems Challenges and Solutions in Smart Environments*. (in English), 2019.

[3] H. E. Amin, "An Integrated Approach to Cyber Risk Management With Cyber Threat Intelligence Framework to Secure Critical Infrastructure," *Journal of Cybersecurity and Privacy,* vol. 4, no. 2, pp. 357-381, 2024, doi: 10.3390/jcp4020018.

[4] O. O. Amoo, "GDPR's Impact on Cybersecurity: A Review Focusing on USA and European Practices," *International Journal of Science and Research Archive,* vol. 11, no. 1, pp. 1338-1347, 2024, doi: 10.30574/ijsra.2024.11.1.0220.

[5] M. Sauter, *From GSM to LTE-Advanced Pro and 5G: an introduction to mobile network s and mobile broadband*, Fourth edition ed. Hoboken, NJ: Wiley, 2021, p. 1.

[6] Z. A. Genç, G. Lenzini, and D. Sgandurra, "Cut-and-Mouse and Ghost Control: Exploiting Antivirus Software with Sy nthesized Inputs," (in en), *Digital Threats: Research and Practice,* vol. 2, no. 1, pp. 1-23, 2021/3/31/ 2021, doi: 10.1145/3431286.

[7] P. Katrakazas, "A Stakeholder Needs Analysis in Cybersecurity: A Systemic Approach to Enhancing Digital Infrastructure Resilience," *Businesses,* vol. 4, no. 2, pp. 225-240, 2024, doi: 10.3390/businesses4020015.

[8] O. C. Obi, "Comprehensive Review on Cybersecurity: Modern Threats and Advanced Defense Strategies," *Computer Science & It Research Journal,* vol. 5, no. 2, pp. 293-310, 2024, doi: 10.51594/csitrj.v5i2.758.

[9] E. S. Okafor, "Cybersecurity Analytics in Protecting Satellite Telecommunications Networks: A Conceptual Development of Current Trends, Challenges, and Strategic Responses," *International Journal of Applied Research in Social Sciences,* vol. 6, no. 3, pp. 254-266, 2024, doi: 10.51594/ijarss.v6i3.854.

[10] M. Guri, "AiR-ViBeR: Exfiltrating Data from Air-Gapped Computers via Covert Surf ace ViBrAtIoNs," *arXiv:2004.06195 [cs],* 2020/4/13/ 2020. [Online]. Available: http://arxiv.org/abs/2004.06195.

[11] M. Guri, Y. Solewicz, A. Daidakulov, and Y. Elovici, "Fansmitter: Acoustic data exfiltration from (speakerless) air-gapped c omputers," *arXiv preprint arXiv:1606.05915,* 2016 2016.

[12] M. Guri, Y. Solewicz, A. Daidakulov, and Y. Elovici, "DiskFiltration: Data Exfiltration from Speakerless Air-Gapped Computer s via Covert Hard Drive Noise," *arXiv preprint arXiv:1608.03431,* 2016 2016.

[13] E. Byres, "The air gap: SCADA's enduring security myth," (in en), *Communications of the ACM,* vol. 56, no. 8, pp. 29-31, 2013/8// 2013, doi: 10.1145/2492007.2492018.

[14] D. Dumitriu and M. A.-M. Popescu, "Enterprise Architecture Framework Design in IT Management," (in en), *Procedia Manufacturing,* vol. 46, pp. 932-940, 2020 2020, doi: 10.1016/j.promfg.2020.05.011.

[15] M. Guri, Y. Solewicz, and Y. Elovici, "Fansmitter: Acoustic data exfiltration from air-Gapped computers via f ans noise," (in en), *Computers & Security,* vol. 91, p. 101721, 2020/4// 2020, doi: 10.1016/j.cose.2020.101721.

[16] M. Guri, B. Zadov, and Y. Elovici, "ODINI: Escaping Sensitive Data From Faraday-Caged, Air-Gapped Computer s via Magnetic Fields," *IEEE Transactions on Information Forensics and Security,* vol. 15, pp. 1190-1203, 2020 2020, doi: 10.1109/TIFS.2019.2938404.

[17] M. Hanspach and M. Goetz, "On Covert Acoustical Mesh Networks in Air," *arXiv:1406.1213 [cs],* 2014/6/4/ 2014. [Online]. Available: http://arxiv.org/abs/1406.1213.

[18] Q. Shan *et al.*, "Estimation of Impulsive Noise in an Electricity Substation," *IEEE Transactions on Electromagnetic Compatibility,* vol. 53, no. 3, pp. 653-663, 2011/8// 2011, doi: 10.1109/TEMC.2010.2092782.

[19] J. Szefer, "Survey of Microarchitectural Side and Covert Channels, Attacks, and De fenses," (in en), *Journal of Hardware and Systems Security,* vol. 3, no. 3, pp. 219-234, 2019/9// 2019, doi: 10.1007/s41635-018-0046-1.

[20] I. Hwang, J. Cho, and S. Oh, "VibeComm: Radio-Free Wireless Communication for Smart Devices Using Vi bration," (in en), *Sensors,* vol. 14, no. 11, pp. 21151-21173, 2014/11/10/ 2014, doi: 10.3390/s141121151.

[21] N. Mims, "Cyber-Attack Process," in *Computer and Information Security Handbook*: Elsevier, 2017, pp. 1105-1116.

[22] H. Nyholm *et al.*, "The Evolution of Volatile Memory Forensics," (in en), *Journal of Cybersecurity and Privacy,* vol. 2, no. 3, pp. 556-572, 2022/7/20/ 2022, doi: 10.3390/jcp2030028.

[23] M. Guri, "Optical air-gap exfiltration attack via invisible images," *Journal of Information Security and Applications,* vol. 46, pp. 222-230, 2019 2019.

[24] S. Sarkar, A. Chakraborty, A. Saha, A. Bannerjee, and A. Bose, "Securing Air-Gapped Systems," in *Proceedings of International Ethical Hacking Conference 2019*, vol. 1065, M. Chakraborty, S. Chakrabarti, and V. E. Balas Eds. Singapore: Springer Singapore, 2020, pp. 229-238.

[25] F. A. Aboaoja, A. Zainal, F. A. Ghaleb, B. A. S. Al-rimy, T. A. E. Eisa, and A. A. H. Elnour, "Malware Detection Issues, Challenges, and Future Directions: A Survey," (in en), *Applied Sciences,* vol. 12, no. 17, p. 8482, 2022/8/25/ 2022, doi: 10.3390/app12178482.

[26] J.-P. Aumasson and M. D. Green, *Serious cryptography: a practical introduction to modern encryption*. San Francisco: No Starch Press, 2017, p. 282.