Journal of Information Systems Engineering and Management
2025, 10(41s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Comparative Study of Cybersecurity Mechanisms

Dr. Nagaraju Kilari[1], Dr. Sumanth S[2], Dr. Nagamani H S[3], Ms. Apoorva A[4]

[1]Associate Professor & HoD, Department of BCA, New Horizon College, Marathalli, Bangalore, Karnataka – India.
[2]Associate Professor,Department of Computer Science and Applications,Government College for Women,Kolar, Karnataka – India.
[3]Associate Professor,Department of Computer Science,Smt VHD Central Institute of Home Science,(MCU) seshadri Road, Bengaluru, Karnataka,India ,
[4]Assistant Professor, Department of BCA, New Horizon College, Marathalli, Bangalore, Karnataka – India.

ARTICLE INFO

Received: 31 Dec 2024

Revised: 20 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

As our world becomes increasingly digital, the significance of cybersecurity is paramount. With the continuous evolution of cyber threats, the protective mechanisms must also advance. This paper presents a comparative study of various cybersecurity mechanisms, including firewalls, intrusion detection systems (IDS), encryption, multi-factor authentication (MFA), and security information and event management (SIEM) systems. By analyzing their functions, advantages, disadvantages, and suitability, this research aims to offer insights into the most effective strategies for protecting digital assets.

Keywords: IDS, SIEM, cybersecurity.

INTRODUCTION

The swift progression of technology has led to a rise in cyber threats, making cybersecurity a vital issue for both individuals and organizations. Cybersecurity mechanisms are crucial for ensuring the integrity, confidentiality, and availability of data. This paper investigates several key cybersecurity mechanisms, comparing their effectiveness, implementation challenges, and appropriateness for various environments.

CYBERSECURITY MECHANISMS

2.1 Firewalls

Functionality: Firewalls serve as a protective barrier between trusted internal networks and untrusted external networks, monitoring and regulating incoming and outgoing traffic based on established security rules.

Strengths:

- Acts as the initial defense against unauthorized access.
- Can be tailored to block specific traffic types.

Weaknesses:

- Ineffective against internal threats or attacks that circumvent the firewall.
- Requires ongoing updates to rules and configurations.

Applicability: Suitable for organizations of all sizes, especially those needing to protect a defined perimeter.

2.2 Intrusion Detection Systems (IDS)

Functionality: IDS monitor network traffic for suspicious activities and known threats, alerting administrators to potential security breaches.

Strengths:

- Capable of detecting a broad range of attacks, including those that bypass firewalls.

- Provides real-time monitoring and alerts.

Weaknesses:

- High rates of false positives can lead to alert fatigue.
- Requires skilled personnel to analyze alerts and respond effectively.

Applicability: Ideal for environments where real-time threat detection is essential, such as financial institutions and healthcare organizations.

2.3 Encryption

Functionality: Encryption converts data into a coded format that can only be accessed by authorized users with the correct decryption key.

Strengths:

- Safeguards data both at rest and in transit, ensuring confidentiality.
- Can lessen the impact of data breaches.

Weaknesses:

- Key management can be complex and challenging.
- May introduce performance overhead that affects system efficiency.

Applicability: Crucial for any organization dealing with sensitive data, including personal and financial information.

2.4 Multi-Factor Authentication (MFA)

Functionality: MFA requires users to provide two or more verification factors to access a system, enhancing security beyond just a password.

Strengths:

- Significantly lowers the risk of unauthorized access.
- Protects against credential theft.

Weaknesses:

- Can create user friction and complexity.
- Implementation may necessitate additional resources and training.

Applicability: Highly recommended for all organizations, particularly those with remote access or sensitive data.

2.5 Security Information and Event Management (SIEM)

Functionality: SIEM systems collect and analyze security data from across an organization's IT infrastructure, providing insights into potential security incidents.

Strengths:

- Delivers comprehensive visibility into security events.
- Aids in compliance reporting and incident response.

Weaknesses:

- Can be costly and resource-intensive to implement and maintain.
- Requires skilled personnel for effective analysis and response.

Applicability: Best suited for large organizations with complex IT environments and regulatory compliance needs.

COMPARATIVE ANALYSIS

Mechanism	Strengths	Weaknesses	Best Use Cases
Firewalls	Initial defense, traffic regulation	Cannot detect internal threats	Perimeter security for organizations
IDS	Real-time monitoring, broad attack detection	High false positives, requires skilled personnel	Environments needing real-time threat detection
Encryption	Data confidentiality, mitigates breach impact	Complex key management, performance overhead	Organizations handling sensitive data
MFA	Reduces unauthorized access risk	User friction, resource-intensive	All organizations, especially with remote access
SIEM	Comprehensive visibility, compliance support	Expensive, requires skilled personnel	Large organizations with complex IT environments

CONCLUSION

The cybersecurity landscape is intricate and constantly changing, necessitating a multi-layered approach to defend against various threats. Each cybersecurity mechanism has its own strengths and weaknesses, making it essential for organizations to evaluate their specific needs and risk profiles when choosing suitable solutions. A layered security strategy that integrates multiple mechanisms is often the most effective way to protect digital assets.

REFERENCES

[1] Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.

[2] AllahRakha, N. (2024). Cybersecurity Regulations for Protection and Safeguarding Digital Assets (Data) in Today's Worlds. Lex Scientia Law Review, 8(1), 405-432.

[3] Hani, N., & Amelia, O. (2024). Digital Transformation in Financial Services: Strategic Growth Through AI, Cyber Security, and Data Protection.

[4] Hasan, L., Hossain, M. Z., Johora, F. T., & Hasan, M. H. (2024). Cybersecurity in Accounting: Protecting Financial Data in the Digital Age. European Journal of Applied Science, Engineering and Technology, 2(6), 64-80.

[5] Chisty, N. M. A., Baddam, P. R., & Amin, R. (2022). Strategic approaches to safeguarding the digital future: insights into next-generation cybersecurity. Engineering International, 10(2), 69-84.

[6] Okoye, C. C., Nwankwo, E. E., Usman, F. O., Mhlongo, N. Z., Odeyemi, O., & Ike, C. U. (2024). Securing financial data storage: A review of cybersecurity challenges and solutions. International Journal of Science and Research Archive, 11(1), 1968-1983.

[7] Deep Neural Network based Malicious Network Activity Detection Under Adversarial Machine Learning Attacks