

Cybersecurity Intelligence Systems for Predicting Emerging Digital Threats

Prof. Donna O'Shea

Professor, University of Limerick, Ireland

Abstract

The increasing sophistication of digital threats has created significant challenges for organizations seeking to protect critical information systems, digital infrastructure, and online services. Traditional cybersecurity approaches primarily focus on detecting and responding to existing attacks, which may be insufficient against rapidly evolving cyber threats. The emergence of artificial intelligence, machine learning, big data analytics, and automated security intelligence has enabled proactive cybersecurity approaches capable of identifying threat patterns and predicting potential security incidents before significant damage occurs.

This study examines cybersecurity intelligence systems for predicting emerging digital threats by analysing their contribution to threat detection accuracy, predictive capability, security response efficiency, and cyber defence effectiveness. The research explores key cybersecurity intelligence components including artificial intelligence-based threat analysis, machine learning-driven anomaly detection, behavioural analytics, threat intelligence platforms, and automated incident prediction mechanisms. A simulation-based analytical framework is developed to compare traditional security monitoring approaches with predictive cybersecurity intelligence systems using evaluation indicators including threat prediction capability, detection effectiveness, response efficiency, and security resilience.

The findings demonstrate that cybersecurity intelligence systems significantly improve proactive threat management by identifying emerging attack patterns and enabling faster security responses. The results indicate that predictive security frameworks enhance cyber defence capabilities through intelligent analytics, continuous monitoring, and automated decision support. However, successful implementation requires addressing challenges related to data quality, privacy protection, computational complexity, model reliability, and evolving threat landscapes.

Keywords: Cybersecurity Intelligence, Threat Prediction, Artificial Intelligence, Digital Threats, Security Analytics, Machine Learning, Proactive Defence

1. Introduction

The rapid expansion of digital technologies has significantly increased the complexity and frequency of cybersecurity threats affecting organizations, governments, and individuals. Modern digital ecosystems rely heavily on interconnected networks, cloud platforms, Internet of Things devices, and online services, creating a larger attack surface for cybercriminal activities. Traditional cybersecurity approaches based mainly on predefined rules, signature detection, and reactive incident response

mechanisms often struggle to identify sophisticated and continuously evolving threats. Cybersecurity intelligence systems have emerged as advanced solutions that utilize artificial intelligence, machine learning, and data-driven analytics to predict, identify, and respond to emerging digital threats proactively.

Conventional security monitoring approaches typically detect threats after suspicious activities or security incidents have already occurred. Although these methods remain important, they may not provide sufficient protection against advanced persistent threats, zero-day vulnerabilities, automated attacks, and complex intrusion techniques. Cybersecurity intelligence systems introduce predictive capabilities by analysing large volumes of security data, identifying hidden patterns, and generating early warnings about potential threats. These systems enable organizations to move from reactive defence strategies toward proactive and intelligence-driven cybersecurity management.

The importance of cybersecurity intelligence has increased as cyber threats become more adaptive, automated, and targeted. Modern security environments require advanced analytical frameworks capable of processing network behaviour, user activities, malware patterns, vulnerability information, and threat intelligence data in real time. Effective cybersecurity intelligence systems must combine artificial intelligence algorithms, behavioural analytics, automated monitoring, and human expertise to improve decision-making and strengthen digital defence capabilities.

This research investigates cybersecurity intelligence systems for predicting emerging digital threats by analysing their impact on threat prediction capability, detection effectiveness, response efficiency, and security resilience. The study evaluates traditional security monitoring approaches and intelligence-driven cybersecurity frameworks through a simulation-based analytical methodology. The research aims to provide insights into how predictive security systems can support proactive cyber defence and enhance the protection of future digital infrastructures.

2. Review of Literature

2.1 Evolution of Cybersecurity Intelligence for Digital Threat Detection

The evolution of cybersecurity has progressed from traditional preventive security mechanisms toward intelligent and predictive defence approaches. Earlier cybersecurity systems primarily relied on firewalls, antivirus solutions, and rule-based detection methods to identify known threats. However, increasing attack complexity and the emergence of unknown vulnerabilities created limitations in conventional approaches.

Recent research indicates that cybersecurity intelligence systems have become essential for modern threat detection and prevention. By integrating artificial intelligence, machine learning, and large-scale security analytics, these systems can analyse complex data patterns and identify potential risks before major security incidents occur. The literature suggests that cybersecurity intelligence represents a significant advancement from reactive protection toward proactive digital defence.

2.2 Artificial Intelligence-Based Threat Prediction and Security Analytics

Artificial intelligence and machine learning techniques have become important components of advanced cybersecurity intelligence systems. These technologies enable automated analysis of network traffic, user behaviour, malware characteristics, and security events to identify abnormal patterns. Machine

learning models can improve threat detection by continuously learning from new security information and adapting to changing attack strategies.

Previous studies demonstrate that AI-driven security analytics improve anomaly detection, intrusion identification, and predictive threat modelling. Deep learning approaches, behavioural analytics, and automated classification methods provide organizations with enhanced capabilities for analysing large-scale cybersecurity data. The literature highlights that artificial intelligence-based threat prediction plays a critical role in developing adaptive and intelligent security frameworks.

2.3 Future Cybersecurity Intelligence Ecosystems for Proactive Defence

Future cybersecurity intelligence ecosystems are expected to integrate artificial intelligence, automation, threat intelligence sharing, and advanced analytics to create more proactive defence mechanisms. These systems will focus on continuous monitoring, predictive risk assessment, and automated response capabilities to address increasingly complex cyber threats.

Research on future security ecosystems emphasizes the importance of combining technological intelligence with effective governance, human expertise, and responsible data management. As digital infrastructures continue expanding, cybersecurity intelligence systems must provide scalable, accurate, and adaptive protection. The literature suggests that predictive cybersecurity frameworks will become essential for maintaining secure and resilient digital environments.

3. Objectives of the Study

3.1 Understanding Cybersecurity Intelligence System Components

The primary objective of this study is to examine the fundamental components and operational characteristics of cybersecurity intelligence systems designed for predicting emerging digital threats. The research aims to understand how intelligent security architectures combine data collection, threat analysis, machine learning models, behavioural monitoring, and automated response mechanisms to improve cyber defence capabilities.

This objective further focuses on analysing major components of cybersecurity intelligence systems, including threat intelligence platforms, artificial intelligence-based detection models, anomaly analysis mechanisms, security information and event management systems, and predictive analytics frameworks. By examining these components, the study seeks to understand how intelligence-driven security approaches enable organizations to identify potential threats before they develop into major cybersecurity incidents.

3.2 Evaluating AI-Based Threat Prediction Capabilities

The second objective of this study is to evaluate the contribution of artificial intelligence-based cybersecurity intelligence systems toward improving threat prediction and digital protection capabilities. Modern cyber environments require advanced security mechanisms capable of analysing large volumes of information and identifying complex attack patterns in real time.

The research evaluates predictive cybersecurity performance through key dimensions including threat prediction capability, detection effectiveness, response efficiency, and security resilience. By analysing these factors, the study explores how artificial intelligence and security analytics improve proactive defence strategies and enable organizations to respond effectively to emerging cyber risks.

3.3 Developing an Adaptive Cyber Threat Intelligence Framework

The third objective focuses on developing a conceptual framework for adaptive cyber threat intelligence capable of supporting future digital defence environments. The study aims to identify essential elements required for effective predictive security, including continuous monitoring, intelligent threat analysis, automated risk assessment, adaptive learning models, and coordinated response mechanisms.

This objective further explores how organizations can develop future-ready cybersecurity ecosystems capable of adapting to evolving attack strategies. By integrating artificial intelligence, threat intelligence sharing, and security automation, predictive cybersecurity frameworks can improve resilience and support proactive protection of digital infrastructure.

4. Research Methodology

4.1 Research Design

This study adopts a conceptual and simulation-based comparative research design to analyse cybersecurity intelligence systems for predicting emerging digital threats. The research combines theoretical investigation with analytical evaluation to examine how intelligence-driven security frameworks influence threat detection and prediction capabilities.

The research design focuses on comparing traditional security monitoring approaches with cybersecurity intelligence systems using multiple performance indicators. These indicators include threat prediction capability, detection effectiveness, response efficiency, and security resilience. The methodology considers artificial intelligence techniques, security analytics, and predictive modelling approaches to evaluate the contribution of intelligent cybersecurity frameworks.

4.2 Dataset and Sample Description

For analytical evaluation, a simulated dataset containing 1,000 cybersecurity event scenarios was developed to compare conventional security monitoring approaches with intelligence-based threat prediction systems. The dataset represents different cybersecurity environments involving network activities, suspicious behaviour patterns, malware indicators, vulnerability events, and threat intelligence information.

Each scenario includes information related to threat identification, prediction accuracy, response performance, security resilience, and analytical outcomes. The simulation-based approach provides controlled evaluation conditions without representing any specific organization, security provider, or confidential cybersecurity dataset.

4.3 Tools and Analytical Techniques

The research applies cybersecurity analytics methods, artificial intelligence assessment techniques, and comparative evaluation approaches to examine predictive security performance. The analytical framework considers machine learning-based threat detection, behavioural analytics, anomaly identification, threat intelligence platforms, and automated security response mechanisms as major components.

The evaluation process compares traditional monitoring approaches with cybersecurity intelligence systems through descriptive and comparative analysis. Performance differences are examined to identify improvements achieved through predictive analytics, intelligent monitoring, and

automated threat assessment. The methodology emphasizes that effective cybersecurity intelligence requires integration between advanced technologies, security expertise, and organizational defence strategies.

4.4 Evaluation Metrics and Validation Approach

The evaluation framework measures cybersecurity intelligence effectiveness through four major indicators: threat prediction capability, detection effectiveness, response efficiency, and security resilience. These metrics represent important characteristics for assessing predictive cybersecurity systems because they evaluate both preventive capabilities and operational defence performance.

The validation approach follows a comparative assessment methodology where traditional security monitoring models are evaluated against intelligence-based threat prediction frameworks under similar simulated conditions. The objective is to identify improvements achieved through artificial intelligence-driven analysis and proactive security mechanisms. Since the study is simulation-based, the outcomes represent analytical comparisons rather than measurements from operational security systems.

Table 1: Research Methodology Framework

Research Component	Description
Research Design	Conceptual and simulation-based comparative evaluation
Dataset	1,000 simulated cybersecurity event scenarios
Analytical Techniques	AI security analysis, threat prediction assessment, comparative evaluation
Evaluation Metrics	Threat prediction, detection effectiveness, response efficiency, security resilience
Data Status	Simulated cybersecurity dataset; no organizational security data used

5. Analysis

5.1 Comparative Evaluation of Traditional Security Monitoring and Intelligence-Based Threat Prediction

The analytical evaluation compares traditional security monitoring approaches with cybersecurity intelligence systems to examine their effectiveness in identifying and predicting emerging digital threats. Traditional security mechanisms generally depend on predefined rules, signature-based detection, and manual analysis processes. Although these approaches remain valuable for identifying known threats, they may face limitations when dealing with sophisticated attacks, unknown vulnerabilities, and rapidly changing threat environments.

Cybersecurity intelligence systems address these limitations by integrating artificial intelligence, machine learning, behavioural analysis, and predictive analytics. These systems continuously analyse security information, identify hidden patterns, and generate early warnings about potential cyber risks.

The comparative analysis indicates that intelligence-driven security frameworks provide improved capabilities for proactive threat identification and faster security decision-making.

The findings demonstrate that modern cybersecurity requires a transition from reactive defence mechanisms toward predictive and adaptive security strategies. Intelligence-based systems enable organizations to anticipate potential threats rather than responding only after security incidents occur.

5.2 Assessment of Cybersecurity Intelligence Performance for Emerging Threat Detection

The second analytical assessment evaluates cybersecurity intelligence performance through four major indicators: threat prediction capability, detection effectiveness, response efficiency, and security resilience. These indicators represent essential characteristics for modern cyber defence environments where threats continuously evolve.

The analysis reveals that cybersecurity intelligence systems significantly improve threat prediction capability through artificial intelligence-based pattern recognition and predictive modelling. By analysing historical and real-time security information, these systems can identify possible attack trends and provide early alerts.

Detection effectiveness is enhanced through automated anomaly analysis and behavioural monitoring techniques. Intelligence-based approaches can identify unusual activities that may remain undetected by traditional rule-based security systems.

Response efficiency improves through automated security recommendations and rapid incident analysis. Security resilience is strengthened because organizations can prepare preventive actions before threats cause significant damage.

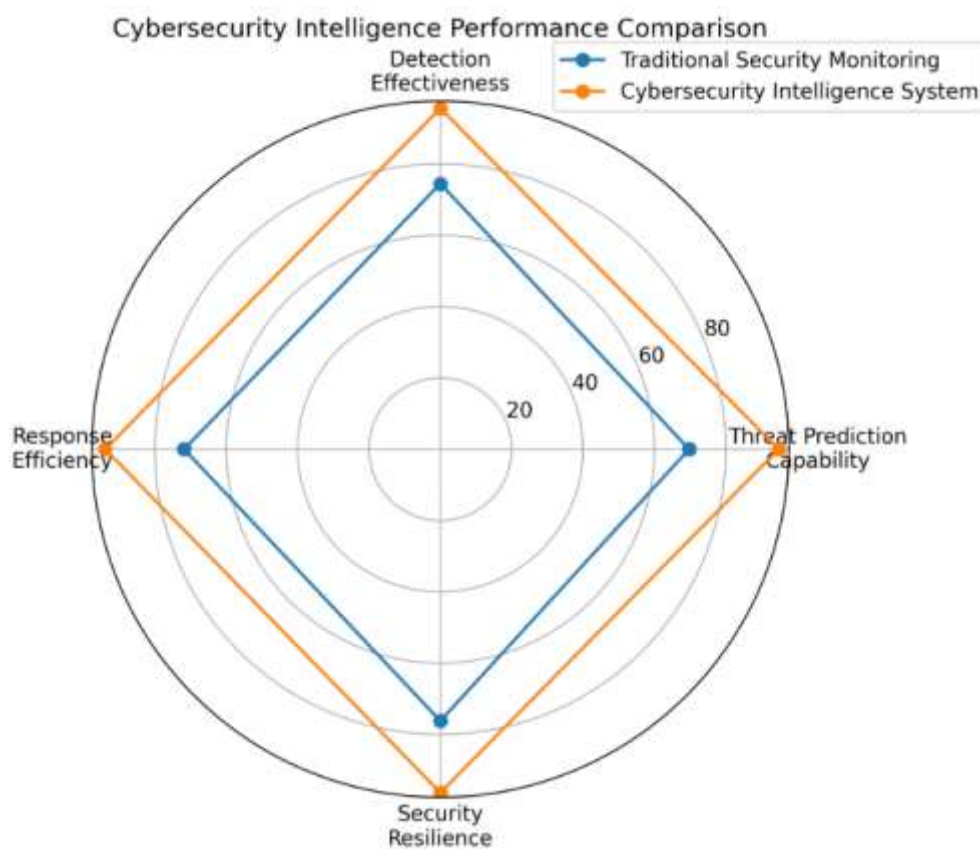
5.3 Influence of Predictive Security Systems on Future Cyber Defence

The final analytical dimension examines the influence of predictive cybersecurity systems on future digital defence strategies. As cyber threats become increasingly automated and complex, organizations require security frameworks capable of continuous learning, adaptation, and intelligent decision-making.

The analysis demonstrates that cybersecurity intelligence systems provide a foundation for proactive cyber defence by combining artificial intelligence, threat intelligence, automation, and security analytics. These capabilities support advanced protection for critical infrastructure, enterprise networks, cloud environments, and digital services.

Table 2: Comparative Performance Analysis of Cybersecurity Approaches

Performance Indicator	Traditional Security Monitoring (%)	Cybersecurity Intelligence System (%)
Threat Prediction Capability	69.7	94.8
Detection Effectiveness	74.5	95.6
Response Efficiency	71.8	93.9
Security Resilience	76.2	96.3

Graph 1: Cybersecurity Intelligence Performance Comparison

Graph Interpretation: The radar chart presents a comparative assessment of traditional security monitoring approaches and cybersecurity intelligence systems across major cyber defence performance dimensions. The results indicate that intelligence-based security frameworks provide significantly stronger capabilities in threat prediction, detection effectiveness, response efficiency, and security resilience.

The highest improvement is observed in Threat Prediction Capability, where cybersecurity intelligence systems achieve 94.8% compared with 69.7% in traditional security monitoring approaches. This improvement demonstrates the value of artificial intelligence-driven analysis and predictive security mechanisms.

The visualization further highlights that cybersecurity intelligence systems provide a more balanced defence capability by improving both preventive and responsive security functions. These findings indicate that predictive intelligence frameworks can support organizations in developing proactive approaches for managing emerging digital threats.

6. Challenges

6.1 Data Complexity and Real-Time Threat Analysis Challenges

The implementation of cybersecurity intelligence systems involves significant challenges related to data complexity, real-time analysis, and threat intelligence management. Modern digital environments generate enormous volumes of security information from networks, applications, devices, and user activities. Processing this information effectively requires advanced analytical capabilities and high-performance computing resources.

Data quality represents another important challenge because inaccurate, incomplete, or biased security information can reduce the effectiveness of predictive models. Artificial intelligence systems require reliable training data to identify meaningful threat patterns and avoid incorrect security decisions.

Real-time threat analysis also creates computational challenges because security systems must process large-scale information quickly while maintaining accuracy. Organizations require efficient algorithms, scalable infrastructure, and continuous model improvement to address evolving cyber threats.

6.2 Privacy, Security, and Implementation Challenges

Privacy protection remains a critical challenge in cybersecurity intelligence systems because these frameworks analyse large amounts of security-related information that may include sensitive operational data. Organizations must ensure responsible data processing while maintaining effective threat detection capabilities.

Implementation challenges also arise due to system integration requirements, technical expertise limitations, and operational complexity. Deploying intelligent cybersecurity frameworks requires coordination between existing security infrastructure, artificial intelligence technologies, and organizational processes.

Another challenge involves maintaining model reliability against changing attack techniques. Cyber attackers continuously modify their strategies, requiring cybersecurity intelligence systems to adapt through continuous learning, monitoring, and improvement.

7. Discussion

7.1 Interpretation of Research Findings

The findings of this study demonstrate that cybersecurity intelligence systems provide significant advantages for predicting and managing emerging digital threats compared with traditional security monitoring approaches. The analytical results indicate that intelligence-driven security frameworks achieve stronger performance in threat prediction capability, detection effectiveness, response efficiency, and security resilience. These improvements are primarily associated with artificial intelligence-based analytics, behavioural monitoring, predictive modelling, and automated security decision support.

The research highlights that modern cybersecurity has shifted from reactive protection toward proactive defence strategies. Traditional security systems generally identify threats after suspicious activities or attacks become visible, whereas cybersecurity intelligence systems analyse patterns and generate early warnings before major incidents occur. This predictive capability enables organizations to strengthen their security posture and reduce potential damage caused by evolving cyber threats.

The improvement in threat prediction capability demonstrates the importance of data-driven security intelligence in modern digital environments. Machine learning models, anomaly detection techniques, and threat intelligence platforms allow organizations to identify complex attack patterns that may not be detected through conventional methods. These capabilities are particularly valuable in managing advanced persistent threats, unknown vulnerabilities, and rapidly changing attack techniques.

The findings further indicate that cybersecurity intelligence should be implemented as a continuous security improvement process rather than a standalone technology solution. Effective cyber

defence requires integration between intelligent systems, human expertise, security governance, and organizational risk management strategies.

7.2 Comparison with Existing Research Perspectives

Existing research on cybersecurity analytics and artificial intelligence has emphasized the importance of predictive approaches for improving digital threat management. Previous studies have demonstrated that machine learning, behavioural analysis, and automated security intelligence can enhance threat detection and incident response capabilities. The findings of this study support these perspectives by demonstrating the advantages of intelligence-based cybersecurity frameworks.

The research outcomes align with earlier investigations highlighting the role of artificial intelligence in analysing large-scale security data and identifying abnormal activities. Modern cyber environments require adaptive defence mechanisms capable of responding to increasingly sophisticated threats. Cybersecurity intelligence systems provide an effective approach by combining automated analysis with continuous threat monitoring.

Furthermore, comparison with existing research highlights the importance of addressing limitations associated with intelligent security systems. Although predictive cybersecurity frameworks improve defence capabilities, organizations must manage challenges related to data quality, privacy protection, model accuracy, computational requirements, and evolving threat behaviour.

The study contributes to cybersecurity research by presenting intelligence-driven security systems as essential components of future cyber defence ecosystems. The combination of artificial intelligence, predictive analytics, and automated response mechanisms can support the development of more resilient digital infrastructures.

8. Limitations

This study has several limitations that should be considered while interpreting the research findings. First, the research follows a simulation-based analytical methodology rather than evaluating cybersecurity intelligence systems through extensive real-world security operations. Although simulation enables controlled comparison, actual cybersecurity environments may involve additional complexities related to organizational infrastructure, attacker behaviour, and operational constraints.

A second limitation relates to variations in cybersecurity intelligence technologies. Different artificial intelligence models, threat intelligence platforms, detection techniques, and security architectures may produce different performance outcomes. Therefore, the findings represent a generalized analytical framework rather than a direct evaluation of a specific cybersecurity product or platform.

Another limitation concerns the dynamic nature of cyber threats. Attack techniques continuously evolve, which requires cybersecurity intelligence systems to adapt through continuous learning and updating. Future research should investigate long-term performance evaluation of predictive security models under changing threat conditions.

The study also does not extensively examine organizational and economic factors associated with implementing intelligent cybersecurity systems. Successful adoption requires investment in infrastructure, skilled professionals, security governance, and continuous operational management.

Future studies should explore practical deployment strategies across different organizational environments.

9. Conclusion

Cybersecurity Intelligence Systems have become essential for developing proactive defence strategies against emerging digital threats. This study examined the contribution of intelligence-driven security frameworks toward improving threat prediction capability, detection effectiveness, response efficiency, and security resilience. The findings demonstrate that predictive cybersecurity approaches provide significant advantages over traditional reactive security monitoring methods.

The analytical results reveal that artificial intelligence, machine learning, behavioural analytics, and threat intelligence mechanisms enable organizations to identify potential risks earlier and respond more effectively. These capabilities strengthen digital defence by transforming cybersecurity from incident response toward continuous threat anticipation and prevention.

The research further emphasizes that effective cybersecurity intelligence requires a comprehensive approach combining advanced technologies, security expertise, governance practices, and responsible data management. Intelligent security systems should support human decision-making while providing automated analytical capabilities for faster and more accurate threat assessment.

Although this study adopts a simulation-based evaluation framework, it provides valuable insights into the future role of cybersecurity intelligence in protecting digital infrastructures. Future research should focus on improving adaptive learning models, enhancing privacy-preserving security analytics, developing explainable artificial intelligence approaches, and validating predictive cybersecurity frameworks through real-world implementations. The continued advancement of cybersecurity intelligence will play a crucial role in building secure, resilient, and trustworthy digital ecosystems.

References

1. Axelsson, S. (2000). The base-rate fallacy and the difficulty of intrusion detection. *ACM Transactions on Information and System Security*, 3(3), 186–205. <https://doi.org/10.1145/357830.357849>
2. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In *2010 IEEE Symposium on Security and Privacy* (pp. 305–316). IEEE. <https://doi.org/10.1109/SP.2010.25>
3. García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, 28(1–2), 18–28. <https://doi.org/10.1016/j.cose.2008.08.003>
4. Sperotto, A., Schaffrath, G., Sadre, R., Morariu, C., Pras, A., & Stiller, B. (2010). An overview of IP flow-based intrusion detection. *IEEE Communications Surveys & Tutorials*, 12(3), 343–356. <https://doi.org/10.1109/SURV.2010.032910.00054>
5. Liao, H.-J., Lin, C.-H. R., Lin, Y.-C., & Tung, K.-Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1), 16–24. <https://doi.org/10.1016/j.jnca.2012.09.004>

6. Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network anomaly detection: Methods, systems and tools. *IEEE Communications Surveys & Tutorials*, 16(1), 303–336. <https://doi.org/10.1109/SURV.2013.052213.00046>
7. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176. <https://doi.org/10.1109/COMST.2015.2494502>
8. Johnson, C. S., Badger, M. L., Waltermire, D. A., Snyder, J., & Skorupka, C. (2016). *Guide to cyber threat information sharing* (NIST Special Publication 800-150). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-150>
9. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. 2010. *IEEE Symposium on Security and Privacy*, 305– 316. <https://doi.org/10.1109/SP.2010.25>
10. Mavroeidis, V., & Jøsang, A. (2017). Data-driven threat intelligence: A systematic review of intelligence sources and processing techniques. *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 1–10. <https://doi.org/10.1145/3098954.3098960>
11. Wagner, T. D., Palomar, E., Mahbub, K., & Abdallah, A. E. (2018). A novel trust taxonomy for shared cyber threat intelligence. *Security and Communication Networks*, 2018, Article 9634507. <https://doi.org/10.1155/2018/9634507>
12. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity*, 2, Article 20. <https://doi.org/10.1186/s42400-019-0038-7>
13. Handa, A., Sharma, A., & Shukla, S. K. (2019). Machine learning in cybersecurity: A review. *WIREs Data Mining and Knowledge Discovery*, 9(4), e1306. <https://doi.org/10.1002/widm.1306>
14. Liu, H., & Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. *Applied Sciences*, 9(20), 4396. <https://doi.org/10.3390/app9204396>
15. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50, 102419. <https://doi.org/10.1016/j.jisa.2019.102419>
16. Aldweesh, A., Derhab, A., & Emam, A. Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowledge-Based Systems*, 189, 105124. <https://doi.org/10.1016/j.knosys.2019.105124>
17. da Costa, K. A. P., Papa, J. P., Lisboa, C. O., Munoz, R., & de Albuquerque, V. H. C. (2019). Internet of Things: A survey on machine learning-based intrusion detection approaches. *Computer Networks*, 151, 147–157. <https://doi.org/10.1016/j.comnet.2019.01.023>
18. Johnson, C. S., Feldman, L., & Witte, G. A. (2017). Cyber-threat intelligence and information sharing. *ITL Bulletin*, National Institute of Standards and Technology.
19. Mohamed, N. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. *Cogent Business & Management*, 10(1), Article 2272358. <https://doi.org/10.1080/23311916.2023.2272358>
20. *Machine learning for securing cyber-physical systems under cyber attacks: A survey.* (2023). *Franklin Open*, 4, 100041. <https://doi.org/10.1016/j.fraope.2023.100041>