International Journal of Innovative Computer Science and IT Research

Volume 01, Issue 04 – Jul-Aug 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

Network Traffic Analysis for Early Identification of Cybersecurity Incidents

Prof. William Fletcher

Professor, University of Manchester, United Kingdom

Abstract

The increasing sophistication of cyberattacks has created a strong requirement for cybersecurity mechanisms capable of identifying suspicious activities before they develop into severe security incidents. Network traffic provides valuable information about communication patterns, connection behavior, protocol usage, packet characteristics, and interactions among hosts and services. However, the increasing volume, velocity, and complexity of network traffic make continuous manual monitoring impractical. Network traffic analysis supported by machine learning, anomaly detection, statistical modeling, and intelligent classification can improve the early identification of potentially malicious activities. This research examines a structured approach for analyzing network traffic to identify cybersecurity incidents at an early stage. The proposed framework integrates traffic collection, preprocessing, feature extraction, behavioral profiling, anomaly detection, intelligent classification, event correlation, and security alert generation.

The methodology emphasizes the identification of deviations from normal communication behavior while reducing unnecessary alerts through contextual analysis and multi-stage validation. Network-level indicators such as packet rates, connection duration, protocol distribution, source-destination relationships, flow characteristics, and temporal behavior are considered within the analytical process. A conceptual analysis is conducted to compare major traffic-analysis techniques and their potential contribution to early incident identification. Two structured tables summarize analytical techniques, traffic features, detection capabilities, and operational limitations. The study demonstrates that intelligent traffic analysis can support earlier recognition of suspicious network behavior, improve monitoring efficiency, and provide security teams with actionable information before incidents escalate. Nevertheless, encrypted traffic, high-speed networks, adversarial evasion, concept drift, imbalanced datasets, privacy requirements, and false positives remain important challenges. The research concludes that effective early detection requires a layered analytical architecture combining statistical techniques, machine learning, behavioral analysis, and human security expertise. Such an approach can strengthen cybersecurity monitoring by transforming raw network traffic into timely and interpretable indicators of emerging security incidents.

Keywords: Network Traffic Analysis, Cybersecurity, Intrusion Detection, Machine Learning, Anomaly Detection, Network Security, Early Incident Detection, Traffic Monitoring, Cyber Threat Detection, Security Analytics

International Journal of Innovative Computer Science and IT Research

Volume 01, Issue 04 – Jul-Aug 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

1. Introduction

Modern organizations depend extensively on interconnected networks to support communication, cloud computing, business applications, remote services, data exchange, and digital operations. This connectivity has also increased exposure to cybersecurity threats. Attackers can exploit vulnerable services, compromised credentials, malicious software, misconfigured systems, and unauthorized access mechanisms to infiltrate organizational environments. Because many attacks generate observable changes in network communication, traffic analysis has become an important component of cybersecurity monitoring and incident identification.

Network traffic contains information about how systems communicate with each other. Packet flows, connection attempts, protocol usage, source and destination relationships, traffic volumes, timing patterns, and session characteristics can provide indicators of abnormal activity. Sudden increases in connection attempts may indicate scanning, unusual outbound communication may suggest data exfiltration, and unexpected communication patterns may indicate command-and-control activity. Detecting these signals early can provide security teams with valuable time to investigate and contain potential incidents.

Traditional network monitoring approaches frequently depend on predefined rules, signatures, thresholds, and known attack patterns. These mechanisms are effective for detecting recognized threats but may struggle with previously unseen or rapidly evolving attacks. Attackers can modify payloads, communication patterns, infrastructure, and timing to evade static detection mechanisms. Consequently, behavioral and anomaly-based approaches have become increasingly important for identifying deviations from normal network activity.

Machine learning and advanced traffic-analysis techniques can process large volumes of network-flow information and identify complex relationships within communication data. Supervised models can classify known malicious traffic, while unsupervised and semi-supervised techniques can identify unusual patterns without requiring complete attack labels. Statistical analysis can provide rapid indicators of abnormal traffic, and temporal modeling can identify changes in communication behavior over time.

This research proposes a conceptual network traffic analysis framework for early identification of cybersecurity incidents. The framework integrates traffic acquisition, preprocessing, feature engineering, behavioral modeling, anomaly detection, classification, correlation, and alert prioritization. The objective is to create a layered approach that provides earlier and more reliable indications of suspicious activity while reducing unnecessary alerts and supporting security analysts in incident-response decision-making.

2. Objectives

Primary Objective

The primary objective of this research is to develop a structured network traffic analysis framework for identifying potential cybersecurity incidents at an early stage. The framework seeks to transform continuous network-flow information into meaningful security indicators by combining traffic preprocessing, feature extraction, behavioral analysis, anomaly detection, intelligent classification, and event correlation.

2.1 Identification of Abnormal Network Behavior

The first objective is to identify deviations from established patterns of legitimate network communication. Network environments typically exhibit recurring characteristics related to traffic volume, connection frequency, protocol distribution, destination patterns, and session duration.

Establishing behavioral baselines can enable analytical systems to recognize unusual activities. Early identification of such deviations can provide preliminary warnings of scanning, unauthorized access, malware communication, denial-of-service activity, or other potentially harmful events.

2.2 Intelligent Traffic Classification

The second objective is to investigate the use of machine learning and computational intelligence for classifying network traffic according to security relevance. Intelligent models can distinguish normal communication from suspicious or malicious patterns based on multiple traffic features.

Combining supervised classification with anomaly detection can improve coverage because known attack types can be recognized directly while unfamiliar behaviors can be flagged for further examination.

2.3 Early Incident Alerting and Response Support

The third objective is to establish an analytical mechanism that converts suspicious traffic observations into prioritized security alerts. Early alerts should provide sufficient contextual information to help analysts understand the affected systems, communication patterns, event timing, and potential severity.

Rather than generating alerts for every anomaly, the framework emphasizes correlation and prioritization to reduce alert fatigue and support timely incident-response activities.

3. Review of Literature

3.1 Network Traffic Analysis and Intrusion Detection

Network traffic analysis has traditionally been used to identify unauthorized activities by examining communication characteristics and comparing observed behavior with known security indicators. Intrusion detection systems commonly employ signature-based and anomaly-based approaches. Signature-based mechanisms are effective for known threats because they can identify recognizable patterns, whereas anomaly-based systems attempt to detect deviations from normal behavior.

The increasing complexity of modern networks has encouraged the development of automated traffic-analysis approaches. Network flow records can provide scalable representations of communication without requiring detailed inspection of every packet. These records can be analyzed to identify unusual connections, traffic bursts, protocol anomalies, and communication relationships. However, traffic diversity and changing workloads can make it difficult to define a universal baseline for normal behavior.

3.2 Machine Learning for Network Security

Machine learning has been widely explored for cybersecurity classification and anomaly detection. Supervised learning methods can identify previously labeled attack categories, while clustering and other unsupervised techniques can detect unusual patterns without requiring complete labels. Decision

Volume 01, Issue 04 – Jul-Aug 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

trees, support vector machines, ensemble learning, neural networks, and deep learning architectures have all been investigated for network security applications.

However, machine learning performance is highly dependent on dataset quality and environmental similarity. A model trained using one network environment may not perform equally well in another because network architectures, applications, traffic patterns, and user behaviors differ. Continuous model evaluation and environment-specific adaptation are therefore necessary for reliable deployment.

3.3 Early Detection Through Behavioral and Temporal Analysis

Early cybersecurity detection requires identifying weak indicators before they develop into major incidents. Behavioral analysis can examine changes in communication relationships, connection frequency, packet volume, destination diversity, and temporal activity. Temporal models can additionally examine event sequences to determine whether a series of activities represents a developing attack.

Combining multiple weak indicators can provide stronger evidence than relying on a single traffic anomaly. For example, an unusual outbound connection combined with abnormal authentication activity and increased data transfer may provide stronger evidence of compromise. Event correlation therefore plays an important role in transforming individual traffic anomalies into meaningful incident indicators.

4. Methodology

4.1 Research Design and Network Monitoring Framework

This study uses a conceptual and analytical research design to develop a layered framework for early cybersecurity incident identification through network traffic analysis. The framework begins with continuous traffic collection and proceeds through preprocessing, feature extraction, behavioral modeling, anomaly detection, traffic classification, event correlation, and alert generation. The design is intended for environments where network communication occurs across endpoints, servers, cloud resources, and external services. The methodology emphasizes scalable analysis because modern network environments may produce very large quantities of traffic information.

The proposed framework separates raw traffic acquisition from analytical processing to maintain reliable data handling. Network flows are collected and transformed into structured records containing temporal, statistical, protocol, and relational characteristics. Behavioral baselines are then constructed to represent expected communication patterns. Analytical models compare current observations against these baselines and generate anomaly indicators. Multiple indicators can subsequently be correlated to determine whether an event requires escalation. Security analysts remain responsible for final incident interpretation.

4.2 Traffic Collection and Preprocessing

Traffic collection focuses on obtaining network-flow information from appropriate monitoring points. Relevant information can include source and destination addresses, ports, protocols, timestamps, packet counts, byte counts, session duration, connection frequency, and flow direction. Depending on the monitoring architecture, packet-level information or summarized flow records can be analyzed.

Appropriate collection mechanisms should minimize unnecessary data retention and follow organizational security and privacy requirements.

Preprocessing converts heterogeneous traffic information into consistent analytical records. Missing values can be identified, duplicate records can be removed, timestamps can be standardized, and malformed observations can be isolated. Features with significantly different numerical scales can be normalized where required by the selected model. Preprocessing can also reduce irrelevant information to improve computational efficiency. The resulting dataset should preserve sufficient contextual information for later investigation while avoiding unnecessary exposure of sensitive network content.

4.3 Feature Engineering and Behavioral Modeling

Feature engineering transforms raw network information into variables capable of representing security-relevant behavior. Features can describe traffic volume, connection frequency, packet-size distribution, protocol diversity, destination concentration, session duration, temporal variation, and source-destination relationships. Combining multiple feature categories can provide a more comprehensive representation of network behavior than using isolated packet characteristics.

Key analytical features include:

- Packet and byte rates.
- Connection frequency.
- Flow duration.
- Source-destination relationships.
- Protocol distribution.
- Port activity.
- Destination diversity.
- Inbound and outbound traffic ratios.
- Temporal activity patterns.
- Repeated connection behavior.
- Unusual communication destinations.
- Sudden traffic-volume changes.

Behavioral models use these features to establish expected communication patterns for hosts, services, users, or network segments. Deviations can then be assigned anomaly scores according to their magnitude and contextual significance.

4.4 Anomaly Detection, Classification, and Validation

The detection stage combines anomaly detection with intelligent traffic classification. Statistical methods can identify significant deviations from historical behavior, while machine learning models can classify observations according to learned traffic patterns. Unsupervised approaches can provide additional support when labeled attack data are incomplete. Combining multiple analytical outputs can reduce dependence on a single detection mechanism and improve resilience against changing attack behavior.

Validation involves comparing model-generated alerts against additional evidence and historical patterns. An isolated anomaly may represent legitimate operational activity rather than an attack. Consequently, alerts should be correlated with host behavior, authentication events, endpoint indicators,

and other available security information. Model performance should be evaluated using precision, recall, false-positive rates, false-negative rates, detection latency, and computational requirements. Confirmed findings can then be prioritized for security-response teams.

5. Analysis

5.1 Network Features for Early Cybersecurity Detection

Network traffic contains several categories of information that can support early incident identification. Volume-based features can reveal unusual increases in traffic, while connection-based features can identify scanning or repeated connection attempts.

Relational features can expose unexpected communication between systems. Temporal features can additionally reveal changes in activity occurring over short or extended periods.

Table 1: Network Traffic Features and Their Cybersecurity Relevance

Traffic Feature	Security Indicator	Potential Incident	Analytical Value
Connection Frequency	Abnormally high connection attempts	Scanning or brute-force activity	High
Packet/Byte Volume	Sudden traffic increase	DDoS or data transfer anomaly	High
Flow Duration	Unusual persistent sessions	Command-and-control activity	Medium-High
Destination Diversity	Unexpected external destinations	Malware or exfiltration	High
Port Distribution	Unusual service access	Reconnaissance or exploitation	High
Protocol Distribution	Unexpected protocol usage	Covert communication	Medium-High
Temporal Activity	Activity outside normal patterns	Account or host compromise	High
Source-Destination Relationships	Unexpected host interactions	Lateral movement	High

Interpretation: Table 1 demonstrates that multiple traffic characteristics can contribute to early detection. Connection frequency and destination diversity can provide useful indicators of reconnaissance or unauthorized communication, while temporal patterns can reveal activity inconsistent with established behavior.

International Journal of Innovative Computer Science and IT Research

Volume 01, Issue 04 – Jul-Aug 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

5.2 Analytical Techniques for Early Incident Identification

Different analytical approaches provide complementary detection capabilities. Statistical techniques can rapidly identify deviations, while supervised machine learning can classify known attack categories.

Unsupervised approaches can identify clusters or outliers that may represent unfamiliar behavior. Deep learning can model complex patterns in large datasets, although its computational requirements and explainability limitations must be considered.

Table 2: Network Traffic Analysis Techniques for Cybersecurity Incident Detection

Technique	Detection Capability	Early Detection Contribution	Limitation
Statistical Analysis	Traffic deviation detection	Rapid baseline comparison	Limited complex pattern recognition
Rule-Based Detection	Known suspicious behavior	Fast identification	Limited against novel attacks
Supervised ML	Known attack classification	Automated traffic categorization	Requires labeled data
Unsupervised ML	Unknown anomaly discovery	Supports novel-threat detection	Higher interpretation difficulty
Deep Learning	Complex traffic-pattern analysis	Detects sophisticated relationships	High computational cost
Behavioral Profiling	Host/user activity deviation	Identifies subtle changes	Requires reliable baselines
Event Correlation	Multi-source incident relationships	Improves alert confidence	Requires integrated data sources

Interpretation: Table 2 shows that early incident detection benefits from a combination of analytical methods. Rule-based systems provide rapid identification of established patterns, whereas machine learning can expand detection capabilities toward complex and previously unseen behaviors.

Behavioral profiling and event correlation are particularly valuable because they provide context for individual anomalies. A layered approach can therefore combine speed, adaptability, and contextual reasoning while reducing the limitations associated with dependence on a single analytical technique.

5.3 Early Alert Prioritization

Early identification is useful only when security teams can distinguish important alerts from routine anomalies. Alert prioritization should consider anomaly magnitude, affected assets, event frequency, communication direction, historical behavior, and relationships with other security events. An anomaly involving a critical server may require more immediate attention than an equivalent anomaly involving a low-risk endpoint.

International Journal of Innovative Computer Science and IT Research

Volume 01, Issue 04 – Jul-Aug 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

A contextual scoring mechanism can combine multiple indicators into an overall incident priority. Repeated anomalies can increase confidence, while known legitimate behavior can reduce unnecessary escalation. This approach can help minimize alert fatigue and ensure that security analysts focus on incidents with stronger evidence of malicious activity.

6. Discussion

6.1 Importance of Behavioral Network Monitoring

Behavioral network monitoring provides an opportunity to identify cybersecurity incidents before traditional signatures become available. Instead of searching exclusively for known malicious patterns, behavioral systems evaluate whether communication is consistent with expected activity. This capability is particularly useful when attackers employ modified tools, previously unseen infrastructure, or techniques that do not match established signatures.

However, behavioral monitoring must account for legitimate changes in network operations. New applications, software updates, remote workers, cloud migration, and seasonal business activity can alter traffic patterns. Consequently, baseline models should be adaptive while maintaining sufficient stability to avoid treating every operational change as suspicious.

6.2 Role of Machine Learning

Machine learning can increase the analytical capacity of network monitoring systems by examining large traffic datasets and identifying complex relationships. Classification models can automate the identification of recognized threat categories, while anomaly detection can identify potentially suspicious activities that fall outside established patterns. These capabilities can reduce the workload associated with continuous traffic monitoring.

The effectiveness of machine learning depends on reliable data and continuous evaluation. Models can become outdated when network behavior changes or attackers adopt new techniques. Security teams should therefore monitor model performance and periodically reassess training data, features, thresholds, and detection outcomes.

6.3 Integration with Incident Response

Network traffic analysis should not operate as an isolated security function. Early traffic indicators become more valuable when correlated with endpoint alerts, authentication records, vulnerability information, application logs, and threat intelligence. Such integration can transform a network anomaly into a more complete incident hypothesis.

Automated alerting should also provide sufficient context for response teams. Instead of reporting only that traffic is anomalous, the system should identify the affected hosts, communication characteristics, timeline, severity indicators, and related events. This contextual information can reduce investigation time and support faster containment decisions.

7. Challenges

One major challenge is the increasing use of encrypted network communication. Encryption protects legitimate users but also limits direct inspection of payload content. Consequently, traffic-analysis systems increasingly depend on metadata, flow characteristics, timing, destination information, and

behavioral patterns. Developing reliable detection mechanisms without unnecessarily inspecting sensitive content remains an important technical and privacy challenge.

Another challenge is the changing nature of network environments. Cloud computing, distributed architectures, Internet of Things devices, remote work, and software-defined infrastructure create highly dynamic traffic patterns. Static baselines may become inaccurate as legitimate behavior changes. Adaptive models are therefore required, but excessive adaptation can allow malicious behavior to become incorporated into the definition of normal activity.

A further challenge is adversarial evasion and alert management. Attackers can deliberately manipulate communication timing, packet characteristics, destinations, and traffic volumes to avoid detection. At the same time, legitimate unusual activities can produce large numbers of false alerts. Effective systems must therefore combine robust detection, contextual correlation, alert prioritization, and human validation.

8. Future Research

Future research should investigate adaptive network traffic models capable of continuously learning legitimate behavioral changes while preventing malicious activities from contaminating established baselines. Continual learning and online anomaly detection could provide more responsive monitoring for dynamic network environments. Research should also investigate methods for distinguishing genuine operational changes from gradual attack behavior.

Another important direction is privacy-preserving traffic analysis. Advanced techniques should allow security monitoring while minimizing the collection and exposure of sensitive communication information. Federated learning and privacy-preserving machine learning may support collaborative model development across distributed environments without requiring centralized access to all raw traffic data.

Future studies should also explore multimodal cybersecurity analytics in which network traffic is combined with endpoint telemetry, authentication events, DNS activity, cloud logs, and threat intelligence. Such integration can improve incident-context reconstruction and reduce false positives. Research should evaluate these systems using realistic datasets and metrics that include detection latency, precision, recall, scalability, explainability, and analyst workload.

9. Conclusion

Network traffic analysis provides a valuable foundation for the early identification of cybersecurity incidents because network communication frequently contains observable indicators of abnormal system and user behavior. Increasing attack sophistication, distributed infrastructure, cloud services, and large-scale connectivity make early detection increasingly important for organizational security. The framework presented in this study combines traffic acquisition, preprocessing, feature engineering, behavioral modeling, anomaly detection, intelligent classification, event correlation, and alert prioritization to transform raw network observations into actionable security indicators. Traffic features such as connection frequency, destination diversity, protocol usage, flow duration, temporal activity, and source-destination relationships can collectively provide meaningful evidence of emerging suspicious behavior. The analytical framework emphasizes that early detection should be based on multiple contextual indicators rather than isolated anomalies.

Machine learning and behavioral analysis can significantly extend traditional network monitoring by enabling automated examination of large traffic volumes and identification of complex patterns. Supervised learning can support recognition of known attack categories, while unsupervised techniques can assist in discovering unfamiliar deviations. Statistical analysis can provide rapid baseline comparisons, and event correlation can connect individual anomalies into broader incident patterns. Nevertheless, automated detection remains subject to limitations including false positives, incomplete training datasets, concept drift, encrypted communication, changing network architectures, and adversarial evasion. Therefore, AI and machine learning should be incorporated as components of a layered cybersecurity monitoring architecture rather than treated as independent solutions. Human analysts remain essential for validating significant findings, understanding organizational context, and making final incident-response decisions.

Future development should focus on adaptive, explainable, privacy-aware, and integrated traffic-analysis systems. Continual learning can improve resilience against changing network conditions, while privacy-preserving methods can support monitoring without excessive exposure of sensitive communication information. Integrating network traffic with endpoint, authentication, cloud, DNS, and threat-intelligence data can further improve incident-context reconstruction and alert confidence. Effective evaluation should extend beyond accuracy and include detection latency, scalability, false-positive reduction, robustness, interpretability, and analyst workload. Ultimately, the value of network traffic analysis lies in its ability to provide timely and contextual awareness of emerging threats. A layered combination of intelligent analytics, behavioral monitoring, contextual correlation, and expert validation can enable organizations to recognize cybersecurity incidents earlier and respond before suspicious activities develop into more damaging security events.

References

1. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. [1] 2010. IEEE Symposium on Security and Privacy, 305– [2] 316. https://doi.org/10.1109/SP.2010.25
2. Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). [3] 2015. Military Communications and Information Systems Conference (MilCIS), 1– [4] 6. https://doi.org/10.1109/MilCIS.2015.7348942
3. 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
4. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 108–116. https://doi.org/10.5220/0006639801080116
5. Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. *Computers & Security, 86*, 147–167. https://doi.org/10.1016/j.cose.2019.06.005
6. 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

7. Moustafa, N., Slay, J., & Creech, G. (2017). Novel geometric area analysis technique for anomaly detection using trapezoidal area estimation on large-scale networks. *IEEE Transactions on Big Data, 5*(4), 481–494. https://doi.org/10.1109/TBDATA.2017.2711020
8. Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: An ensemble of autoencoders for online network intrusion detection. *Network and Distributed System Security Symposium*. https://doi.org/10.14722/ndss.2018.23204
9. Ahmad, Z., Khan, A. S., Shiang, C. W., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies, 32*(1), e4150. https://doi.org/10.1002/ett.4150
10. Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., & Anwar, A. (2020). TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems. *IEEE Access, 8*, 165130–165150. https://doi.org/10.1109/ACCESS.2020.3022862
11. Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. *Future Generation Computer Systems, 100*, 779–796. https://doi.org/10.1016/j.future.2019.05.041
12. Sharafaldin, I., Lashkari, A. H., Hakak, S., & Ghorbani, A. A. (2019). Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. [5] 2019. International Carnahan Conference on Security Technology, 1– [6] 8. https://doi.org/10.1109/CCST.2019.8888419
13. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence, 2*(1), 41–50. https://doi.org/10.1109/TETCI.2017.2772792
14. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE Access, 7*, 41525–41550. https://doi.org/10.1109/ACCESS.2019.2895334
15. 2018. Journal of Big Data, 7, [7] 104. https://doi.org/10.1186/s40537-020-00382-x
16. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity, 2*, 20. https://doi.org/10.1186/s42400-019-0038-7
17. Ahmad, I., Basheri, M., Iqbal, M. J., & Rahim, A. (2018). Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection. *IEEE Access, 6*, 33789–33795. https://doi.org/10.1109/ACCESS.2018.2841987
18. Maseer, Z. K., Yusof, R., Hassan, R., & Afifi, A. (2024). Meta-analysis and systematic review for anomaly network intrusion detection systems: Detection methods, dataset, validation methodology, and challenges. *IET Networks, 13*(5–6), 339–376. https://doi.org/10.1049/ntw2.12128
19. Al-Rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security, 74*, 263–285. https://doi.org/10.1016/j.cose.2018.01.001
20. Ahmad, Z., Shahid Khan, A., Shiang, C. W., Abdullah, J., & Ahmad, F. (2024). A comprehensive survey of intrusion detection system using machine learning and deep learning approaches. *2024 10th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 1–6. https://doi.org/10.1109/ICACCS60874.2024.10717043