Advancing Cybersecurity with LLMs: A Comprehensive Review of Intrusion Detection Systems and Emerging Applications

Hamouda Djallel[1], Mohamed Amine Ferrag[1], Benhamida Nadjette[1] and Seridi Hamid[1]

[1]Labstic Laboratory, Department of Computer Science, Guelma University, B.P. 401, 24000, Guelma, Algeria

Abstract

The rapid advancements in Transformers and Large Language Models (LLMs) have significantly transformed the landscape of cybersecurity, particularly in Intrusion Detection Systems (IDS). These models offer enhanced detection accuracy, scalability, and adaptability, surpassing traditional approaches in identifying and mitigating sophisticated cyber threats. This survey explores the integration of LLMs in IDS by addressing six key research dimensions: foundational methodologies, comparative performance with classical techniques, challenges in interpretability, practical applications, emerging trends, and directions for future research. By synthesizing the latest advancements, this work aims to provide a comprehensive framework for understanding the role of LLMs in strengthening cybersecurity and fostering innovation in network security and anomaly detection.

Keywords

Large Language Models, Transformers, Intrusion Detection Systems, Cybersecurity, Malware Detection

1. Introduction

The rapid digital transformation of industries and societies has significantly increased reliance on interconnected systems, making cybersecurity a critical concern [1]. With the increasing volume, diversity, and sophistication of cyber threats, traditional Intrusion Detection Systems (IDS), including those employing machine learning (ML) and deep learning (DL) techniques, face limitations in adaptability and resilience [2]. Although ML and DL-based IDS have enhanced detection accuracy and adaptability compared to static, signature-based systems, they often struggle with challenges such as handling high-dimensional data, evolving attack vectors, and adversarial inputs. These constraints underscore the need for more advanced and robust approaches to counter modern cyber threats [3].

Recent advancements in Artificial Intelligence (AI), particularly in Transformers [4] and Large Language Models (LLMs), have revolutionized numerous domains. Initially developed for natural language processing tasks, LLMs like BERT [5] and GPT [6] excel at identifying complex patterns and contextual relationships within extensive datasets. These attributes make LLMs a promising enhancement to existing IDS by addressing limitations in scalability, adaptability, and the detection of novel threats that traditional ML/DL-based approaches struggle to manage effectively [7].

This survey aims to explore the integration of LLMs into IDS, providing a comprehensive review of methodologies, applications, challenges, and future directions. Specifically, the paper addresses the following objectives:

- Examine the foundational methodologies enabling the deployment of LLMs in IDS.
- Compare the performance of LLM-based systems with traditional IDS approaches, highlighting their strengths and limitations.

Proceedings of the International IAM'24: International Conference on Informatics and Applied Mathematics, December 04–05, 2024, Guelma, Algeria

*Corresponding author.

†These authors contributed equally.

hamouda.djallel@univ-guelma.dz (H. Djallel); ferrag.mohamedamine@univ-guelma.dz (M. A. Ferrag); benhamida.nadjette@univ-guelma.dz (B. Nadjette); seridi.hamid@univ-guelma.dz (S. Hamid)

0000-0003-2168-4192 (H. Djallel); 0000-0002-0632-3172 (M. A. Ferrag); 0000-0002-5540-8594 (B. Nadjette); 0000-0002-0236-8541 (S. Hamid)

- Discuss key challenges, including computational complexity, dataset limitations, and interpretability concerns.
- Highlight practical applications of LLMs in cybersecurity, such as network security, malware detection, and phishing prevention.
- Propose future research directions to overcome current limitations and drive further advancements in the field.

By consolidating recent advancements and delivering a structured analysis, this study aims to equip researchers and practitioners with a roadmap for deploying LLMs to develop more efficient, adaptable, and comprehensive cybersecurity solutions

2. Background and Preliminaries

This section outlines foundational concepts, including LLMs, IDS, and their intersection, to set the stage for subsequent discussions

2.1. Large Language Models and Transformers

Transformers have reshaped artificial intelligence, with architectures such as BERT , GPT , and T5 achieving remarkable performance across diverse tasks [8]. Their foundational self-attention mechanism enables efficient modeling of relationships between input elements, allowing them to capture long-range dependencies effectively.

LLMs, built on these architectures, leverage extensive pre-training on large corpora followed by fine-tuning for specific tasks. Key advantages of LLMs include:

- **Pattern Recognition:** The ability to identify complex patterns within large and heterogeneous datasets [6].
- **Contextual Understanding:** Robust handling of sequential and contextual information [5].
- **Scalability:** High adaptability to diverse domains, including cybersecurity [8].

These properties make LLMs particularly suited for addressing the challenges posed by modern cyber threats.

2.2. Intrusion Detection Systems (IDS)

IDS are critical components of cybersecurity infrastructures, designed to monitor, detect, and respond to suspicious activities within networks or systems [2]. Broadly, IDS are categorized into:

- **Signature-Based IDS:** These systems rely on predefined rules and patterns to identify known threats. While efficient, they struggle with zero-day attacks and novel threats.
- **Anomaly-Based IDS:** These systems use statistical or machine learning techniques to detect deviations from normal behavior, making them more adaptable to new threats but prone to higher false positive rates.
- **Hybrid IDS:** Combining signature-based and anomaly-based approaches, hybrid IDS aim to balance accuracy and adaptability.

Despite advancements, traditional IDS often face challenges, including limited adaptability, high false positive rates, and computational inefficiency, particularly in handling large-scale or dynamic environments [2].

2.3. Intersection of LLMs and IDS

Integrating LLMs into IDS effectively addresses key limitations of traditional systems. Through their advanced pattern recognition and contextual analysis capabilities, LLMs enable IDS to:

- **Enhance Detection Accuracy:** Identify complex and evolving threats with greater precision [9].
- **Improve Adaptability:** Generalize effectively across diverse attack scenarios without extensive reconfiguration [7].
- **Reduce False Positives:** Provide more reliable threat detection, minimizing unnecessary alerts [9].

This synergy between LLMs and IDS represents a paradigm shift in cybersecurity, offering solutions that are both scalable and robust against sophisticated threats [10].

3. Current Methodologies

The integration of LLMs into IDS systems has led to the development of various methodologies aimed at enhancing detection capabilities. This section explores the primary approaches, including pre-trained model customization, fine-tuning strategies, integration into IDS pipelines, and key algorithms and models [11].

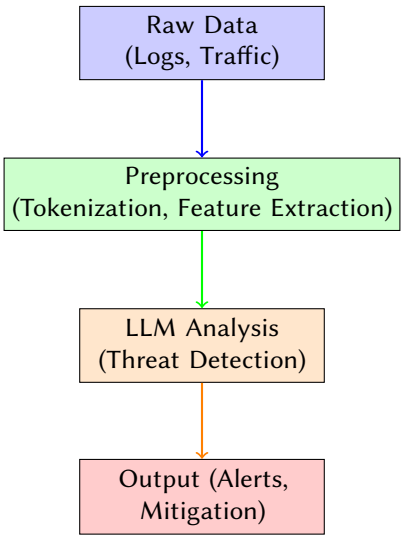

Figure 1: Workflow of an LLM-Based Intrusion Detection System

3.1. Pre-trained Models and Customization

Pre-trained LLMs, such as BERT and GPT, are trained on extensive corpora, capturing diverse linguistic patterns. Customization techniques are applied to adapt these models for cybersecurity applications:

- **Domain-Specific Pre-training:** Further training LLMs on cybersecurity-related datasets to imbue them with domain-specific knowledge [12].
- **Embedding Alignment:** Adjusting embeddings to align with cybersecurity terminologies and concepts, enhancing the model's contextual understanding [9].

3.2. Fine-tuning Strategies

Fine-tuning involves adapting pre-trained LLMs to specific tasks within IDS [13] :

- **Supervised Fine-Tuning:** Utilizing labeled datasets to train LLMs for tasks like anomaly detection and threat classification.
- **Transfer Learning:** Applying knowledge from related domains to improve performance on cybersecurity tasks, especially when labeled data is scarce [14].

3.3. Integration into IDS Pipelines

Incorporating LLMs into IDS involves designing workflows that leverage their capabilities [11]:

- **Data Preprocessing:** Converting network logs and alerts into formats suitable for LLM processing .
- **Real-Time Analysis:** Implementing LLMs to analyze data streams in real-time, enabling prompt detection and response.

3.4. Key Algorithms and Models

Several models and algorithms have been developed to enhance IDS using LLMs :

- **BertIDS:** A BERT-based model fine-tuned for identifying and classifying network attacks, demonstrating improved accuracy over traditional methods [15] [9].
- **HuntGPT:** An LLM-powered intrusion detection dashboard that integrates proactive threat hunting with explainable AI frameworks [16].
- **ChatIDS:** An approach leveraging LLMs to make IDS alerts understandable to non-experts, enhancing interpretability and response [17].

These methodologies represent the forefront of integrating LLMs into IDS, offering enhanced detection capabilities and adaptability to evolving cyber threats.

4. Comparative Analysis with Traditional Techniques

Integrating large language models (LLMs) into intrusion detection systems (IDS) marks a transformative shift from traditional methodologies. This section presents a comprehensive comparative analysis, highlighting the strengths and challenges of LLM-based IDS in relation to traditional approaches. The key differences are summarized in Table 1.

LLM-based IDS outperform traditional methods in critical metrics such as accuracy and F1-score, demonstrating superior capability in handling diverse and complex datasets [10] [7] [13] [11]. These systems offer several advantages over traditional IDSs:

- **Enhanced Scalability**: LLMs effectively process large-scale and dynamic datasets, overcoming the scalability limitations of traditional systems.
- **Improved Adaptability**: With robust generalization capabilities, LLMs are better suited to detect novel threats and zero-day attacks.
- **Contextual Analysis**: Leveraging natural language understanding, LLM-based IDS derive context from logs and alerts, reducing ambiguity in threat identification.
- **Reduced False Positives**: Advanced contextual comprehension allows for more accurate threat classification, leading to fewer unnecessary alerts.

These features are contrasted with traditional IDS approaches in Table 1:
Despite these advantages, LLM-based IDS face notable challenges:

Table 1
Comparison of Traditional IDS and LLM-Based IDS

Feature	Traditional IDS	LLM-Based IDS
Detection Method	Rule-based or anomaly-based	Contextual analysis using deep learning
Adaptability to New Threats	Limited	High
Scalability	Challenging for large datasets	Scalable with proper optimization
False Positives	High	Lower due to contextual understanding
Interpretability	High	Low (requires Explainable AI)
Computational Requirements	Low	High

- **Computational Complexity**: These systems demand substantial computational resources, which can be a barrier in resource-constrained environments [11].
- **Training Data Requirements** : High-quality, labeled datasets are essential for fine-tuning LLMs, yet such datasets are often difficult to obtain in cybersecurity domains [14].
- **Interpretability Issues**: The black-box nature of LLMs complicates understanding their decision-making processes, creating a need for advancements in Explainable AI (XAI) [17].

To bridge the gap between traditional and LLM-based approaches, researchers are exploring hybrid models that integrate the efficiency and interpretability of traditional methods with the adaptability and precision of LLMs. Additionally, ongoing developments in XAI and optimization techniques hold promise for addressing computational and interpretability challenges, paving the way for broader adoption of LLM-based IDS in real-world scenarios.

5. Applications in Cybersecurity

The integration of Large Language Models (LLMs) into cybersecurity has enabled significant advancements across various domains. This section explores key applications, highlighting the role of LLMs in network security, malware analysis, phishing detection, data leakage prevention, and software vulnerability detection.

5.1. Network Security

LLMs have been instrumental in enhancing network security by detecting anomalies and identifying potential intrusions. By analyzing log files [14] [7], network traffic [9], and user behaviors [18], LLMs can:

- **Detect Sophisticated Attacks:** Identify advanced persistent threats (APTs) and zero-day vulnerabilities through contextual pattern analysis.
- **Mitigate Distributed Denial of Service (DDoS) Attacks:** Recognize traffic anomalies indicative of DDoS attacks and trigger real-time mitigation strategies.
- **Enhance Threat Intelligence:** Integrate with threat intelligence feeds to provide contextual insights into potential vulnerabilities.

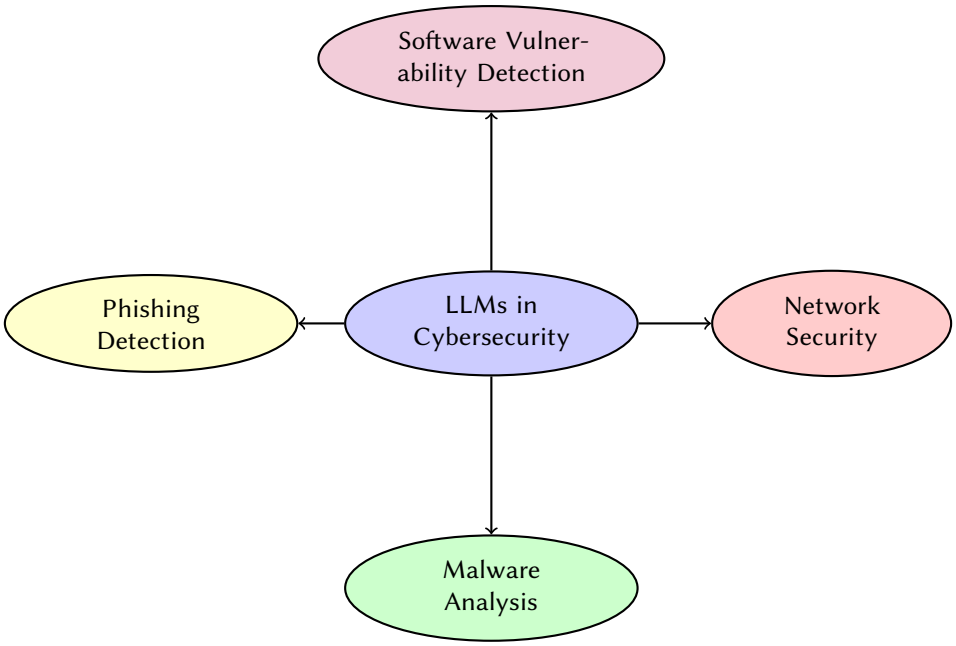

Figure 2: Applications of LLMs in Cybersecurity

5.2. Malware Analysis

Malware detection and classification have greatly benefited from LLMs' ability to analyze code and behavioral patterns [19] [20] [21]:

- **Behavioral Analysis:** Analyze system logs and executable behaviors to detect malicious activities without relying solely on static signatures.
- **Code Analysis:** Evaluate and classify obfuscated or polymorphic malware by understanding code structures and relationships.
- **Threat Categorization:** Facilitate automated categorization of malware families based on contextual and structural similarities.

5.3. Phishing and Social Engineering Detection

LLMs have shown exceptional capabilities in detecting phishing attempts and social engineering attacks [22] [23] [24]:

- **Email and Text Analysis:** Identify linguistic patterns and anomalies indicative of phishing attempts.
- **Preventing Deceptive Communications:** Detect impersonation and spoofing by comparing sender identities with behavioral baselines.
- **Proactive Awareness:** Generate simulated phishing attempts to train and assess user awareness .

5.4. Software Vulnerability Detection

Identifying vulnerabilities in software is a critical application of LLMs in cybersecurity [25] [26] [27] [28]. By analyzing source code, dependency graphs, and software configurations, LLMs can:

- **Detect Known Vulnerabilities:** Automatically identify and flag vulnerabilities from databases such as CVE or NVD by recognizing patterns in software code and configurations.
- **Identify Code Smells:** Spot potentially risky coding practices that could lead to future vulnerabilities, such as improper input sanitization or outdated dependencies.

- **Enhance Security Testing:** Generate test cases to validate software against common exploit scenarios, improving the overall robustness of applications.

These applications demonstrate the versatility of LLMs in addressing complex cybersecurity challenges, underscoring their value in building proactive and adaptive defense mechanisms.

6. Challenges and Interpretability

The adoption of Large Language Models (LLMs) in Intrusion Detection Systems (IDS) is transformative but introduces several challenges. Key issues include computational complexity, dataset limitations, interpretability concerns, ethical considerations, and privacy concerns. Table 2 summarizes these challenges and proposed solutions.

6.1. Challenges and Proposed Solutions

Table 2
Challenges and Solutions for LLM-Based IDS

Challenge	Proposed Solution
Computational Complexity	Model optimization techniques like quantization and pruning
Data Scarcity	Data augmentation, synthetic data generation, and federated learning
Interpretability Issues	Integration of Explainable AI methods such as attention visualization
Adversarial Vulnerabilities	Robust loss functions, adversarial training, and ensemble methods

- **Computational Complexity**: LLMs demand high computational resources, presenting barriers for real-time detection in resource-constrained environments. Optimization techniques like quantization, pruning, and distillation are promising solutions to reduce model size, latency, and energy consumption [11].
- **Dataset Limitations**: Cybersecurity datasets often suffer from imbalance, scarcity, and privacy concerns. These limitations affect model performance, particularly in detecting rare or zero-day threats. Techniques such as data augmentation, synthetic data generation, and federated learning address these issues while preserving privacy [11].
- **Interpretability Concerns**: The ”black-box” nature of LLMs complicates understanding their decisions, which is critical for trust and accountability in high-stakes cybersecurity environments. Explainable AI (XAI) methods, including attention visualization, feature importance ranking, and counterfactual analysis, are being developed to improve transparency [17].
- **Ethical Concerns**: LLMs may be vulnerable to adversarial attacks or misuse, such as generating phishing emails or automating sophisticated attacks. Countermeasures like adversarial training, robust loss functions, and clear policy frameworks are essential to mitigate these risks [29].
- **Privacy Concerns**: Training LLMs for cybersecurity often requires sensitive data, which poses risks related to data leakage and regulatory non-compliance. Privacy-preserving techniques, such as federated learning, differential privacy, and secure multiparty computation, can mitigate these risks while allowing the development of effective IDS solutions [29].

Table 3
Emerging Trends in LLM-Based Cybersecurity Solutions

Trend	Description
Real-Time Intrusion Detection	The use of LLMs for real-time intrusion detection is gaining traction. Techniques such as streaming transformers and lightweight model architectures are being developed to enable real-time processing of network traffic and alerts.
Federated Learning for Cybersecurity	Federated learning frameworks are emerging as a solution to privacy and data-sharing concerns in cybersecurity. By enabling decentralized model training, federated learning allows organizations to collaborate without exposing sensitive data.
Graph-Based Learning Integration	Graph-based models are being combined with LLMs to capture relationships between entities, such as users, IP addresses, and file hashes. This integration enhances the detection of sophisticated attacks, including supply chain attacks and APTs.
Explainable AI for Security	Explainable AI (XAI) tools are increasingly being adopted to address the interpretability challenges of LLMs. Visualization techniques, such as attention maps and saliency scores, are being integrated into cybersecurity workflows to build trust and transparency.

6.2. Future Directions

To overcome these challenges, researchers are focusing on:

1. **Lightweight Model Development**: Creating resource-efficient LLMs for edge device deployment.
2. **Dataset Expansion**: Building diverse, representative datasets to improve training and generalization.
3. **Enhanced XAI**: Advancing interpretability to foster trust and transparency in LLM-based systems.
4. **Ethical Governance**: Establishing guidelines to ensure responsible use and prevent malicious exploitation.

By addressing these challenges and adopting innovative solutions, LLM-based IDS can evolve into scalable, interpretable, and ethically responsible tools for modern cybersecurity.

7. Emerging Trends and Future Directions

LLM advancements, along with AI and cybersecurity progress, are set to revolutionize threat detection and mitigation. Emerging trends in LLM-based cybersecurity, such as real-time intrusion detection, federated learning, graph-based learning, and XAI, are highlighted in Table 3. Future improvements, including energy-efficient models, better datasets, hybrid systems, and enhanced security measures, are outlined in Table 4.

8. Conclusion

Large Language Models (LLMs) have emerged as powerful tools in transforming cybersecurity, particularly in enhancing the capabilities of Intrusion Detection Systems (IDS). This paper has reviewed the methodologies, applications, challenges, and future directions associated with LLM-based IDS, highlighting their ability to address the limitations of traditional approaches and adapt to evolving cyber threats.

Table 4
Future Directions for LLM-Based Cybersecurity Solutions

Direction	Description
Energy-Efficient LLMs	Developing energy-efficient LLMs is crucial for their sustainable deployment in cybersecurity. Techniques such as model compression, quantization, and distillation should be further explored to reduce energy consumption.
Comprehensive Cybersecurity Datasets	The creation of diverse and representative cybersecurity datasets is essential for training robust LLMs. Future efforts should focus on curating datasets that capture a wide range of attack scenarios, including zero-day vulnerabilities and emerging threats.
Hybrid Models	Hybrid systems that combine traditional IDS techniques with LLM capabilities offer a balanced approach. For instance, combining rule-based detection with LLM-powered anomaly detection can enhance both accuracy and efficiency.
Adversarial Robustness	Future research should prioritize developing LLMs that are resilient to adversarial attacks. Adversarial training, ensemble methods, and robust loss functions are promising techniques to enhance model security.
Ethical and Policy Frameworks	Establishing clear ethical guidelines and policy frameworks is critical to prevent the misuse of LLMs in cybersecurity. Future work should explore mechanisms to enforce responsible deployment and mitigate potential risks.
Interdisciplinary Collaboration	Collaboration between AI researchers, cybersecurity professionals, and policymakers is essential for driving innovation. Interdisciplinary research can help address complex challenges and unlock new opportunities for LLM-based cybersecurity solutions.

While LLMs offer significant advantages, such as improved detection accuracy, scalability, and contextual analysis, challenges related to computational demands, dataset limitations, and interpretability persist. Addressing these issues through advancements in model optimization, Explainable AI, and ethical frameworks will be essential for their sustainable deployment.

Looking ahead, interdisciplinary collaboration among AI researchers, cybersecurity professionals, and policymakers will be key to unlocking the full potential of LLMs. By fostering innovation and addressing critical challenges, LLMs can redefine the cybersecurity landscape, offering scalable and intelligent solutions for safeguarding digital infrastructures.

In summary, LLMs represent a promising step toward more adaptive and resilient cybersecurity systems, paving the way for intelligent, proactive, and scalable defense mechanisms.

Declaration on Generative AI

During the preparation of this work, the authors used ChatGPT, for rephrasing, grammar and spelling checks, and improving writing style. After using this tool/service, the authors reviewed and edited the content as needed and takes full responsibility for the publication's content.

References

[1] G. Culot, F. Fattori, M. Podrecca, M. Sartor, Addressing industry 4.0 cybersecurity challenges, IEEE Engineering Management Review 47 (2019) 79–86.

[2] D. Hamouda, M. A. Ferrag, N. Benhamida, H. Seridi, Intrusion detection systems for industrial internet of things: A survey, in: 2021 International Conference on Theoretical and Applicative Aspects of Computer Science (ICTAACS), IEEE, 2021, pp. 1–8.

[3] M. A. Bouke, A. Abdullah, N. I. Udzir, N. Samian, Overcoming the challenges of data lack,

leakage, and imensionality in intrusion detection systems: a comprehensive review, Journal of Communication and Information Systems 39 (2024).
[4] A. Vaswani, Attention is all you need, Advances in Neural Information Processing Systems (2017).
[5] J. Devlin, Bert: Pre-training of deep bidirectional transformers for language understanding, arXiv preprint arXiv:1810.04805 (2018).
[6] T. B. Brown, Language models are few-shot learners, arXiv preprint arXiv:2005.14165 (2020).
[7] O. G. Lira, A. Marroquin, M. A. To, Harnessing the advanced capabilities of llm for adaptive intrusion detection systems, in: International Conference on Advanced Information Networking and Applications, Springer, 2024, pp. 453–464.
[8] M. A. K. Raiaan, M. S. H. Mukta, K. Fatema, N. M. Fahad, S. Sakib, M. M. J. Mim, J. Ahmad, M. E. Ali, S. Azam, A review on large language models: Architectures, applications, taxonomies, open issues and challenges, IEEE Access (2024).
[9] M. A. Ferrag, M. Ndhlovu, N. Tihanyi, L. C. Cordeiro, M. Debbah, T. Lestable, N. S. Thandi, Revolutionizing cyber threat detection with large language models: A privacy-preserving bert-based lightweight model for iot/iiot devices, IEEE Access (2024).
[10] H. Xu, S. Wang, N. Li, K. Wang, Y. Zhao, K. Chen, T. Yu, Y. Liu, H. Wang, Large language models for cyber security: A systematic literature review, arXiv preprint arXiv:2405.04760 (2024).
[11] M. A. Ferrag, F. Alwahedi, A. Battah, B. Cherif, A. Mechri, N. Tihanyi, Generative ai and large language models for cyber security: All insights you need, arXiv preprint arXiv:2405.12750 (2024).
[12] M. Bayer, P. Kuehn, R. Shanehsaz, C. Reuter, Cysecbert: A domain-adapted language model for the cybersecurity domain, ACM Transactions on Privacy and Security 27 (2024) 1–20.
[13] A. Shestov, A. Cheshkov, R. Levichev, R. Mussabayev, P. Zadorozhny, E. Maslov, C. Vadim, E. Bulychev, Finetuning large language models for vulnerability detection, arXiv preprint arXiv:2401.17010 (2024).
[14] E. Karlsen, X. Luo, N. Zincir-Heywood, M. Heywood, Benchmarking large language models for log analysis, security, and interpretation, Journal of Network and Systems Management 32 (2024) 59.
[15] H. Lai, Intrusion detection technology based on large language models, in: 2023 International Conference on Evolutionary Algorithms and Soft Computing Techniques (EASCT), IEEE, 2023, pp. 1–5.
[16] T. Ali, P. Kostakos, Huntgpt: Integrating machine learning-based anomaly detection and explainable ai with large language models (llms), arXiv preprint arXiv:2309.16021 (2023).
[17] V. Jüttner, M. Grimmer, E. Buchmann, Chatids: Explainable cybersecurity using generative ai, arXiv preprint arXiv:2306.14504 (2023).
[18] J. Liu, C. Zhang, J. Qian, M. Ma, S. Qin, C. Bansal, Q. Lin, S. Rajmohan, D. Zhang, Large language models can deliver accurate and interpretable time series anomaly detection, arXiv preprint arXiv:2405.15370 (2024).
[19] P. M. S. Sánchez, A. H. Celdrán, G. Bovet, G. M. Pérez, Transfer learning in pre-trained large language models for malware detection based on system calls, arXiv preprint arXiv:2405.09318 (2024).
[20] C. Patsakis, F. Casino, N. Lykousas, Assessing llms in malicious code deobfuscation of real-world malware campaigns, arXiv preprint arXiv:2404.19715 (2024).
[21] P. Madani, Metamorphic malware evolution: The potential and peril of large language models, in: 2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), IEEE, 2023, pp. 74–81.
[22] L. Jiang, Detecting scams using large language models, arXiv preprint arXiv:2402.03147 (2024).
[23] R. Chataut, P. K. Gyawali, Y. Usman, Can ai keep you safe? a study of large language models for phishing detection, in: 2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC), IEEE, 2024, pp. 0548–0554.
[24] T. Koide, N. Fukushi, H. Nakano, D. Chiba, Detecting phishing sites using chatgpt, arXiv preprint arXiv:2306.05816 (2023).
[25] M. A. Ferrag, A. Battah, N. Tihanyi, M. Debbah, T. Lestable, L. C. Cordeiro, Securefalcon: The next

cyber reasoning system for cyber security, arXiv preprint arXiv:2307.06616 (2023).
[26] M. D. Purba, A. Ghosh, B. J. Radford, B. Chu, Software vulnerability detection using large language models, in: 2023 IEEE 34th International Symposium on Software Reliability Engineering Workshops (ISSREW), IEEE, 2023, pp. 112–119.
[27] A. Mechri, M. A. Ferrag, M. Debbah, Secureqwen: Leveraging llms for vulnerability detection in python codebases, Computers & Security 148 (2025) 104151.
[28] D. Noever, Can large language models find and fix vulnerable software?, arXiv preprint arXiv:2308.10345 (2023).
[29] B. C. Das, M. H. Amini, Y. Wu, Security and privacy challenges of large language models: A survey, arXiv preprint arXiv:2402.00888 (2024).