A Systematic Analysis of Multi-Task Learning Frameworks for Advanced Cybersecurity Applications

Umair Ayaz Kamangar[1], Sanaullah Khaskheli[2*], Zakria Jamali[3], Zainab Umair Kamangar[4], Abdul Sattar Chan[5], Muhammad Ahsan Kareem[6], Sibgha Mursaleen[7], Muhammad Usman Sarwar[8], Soyam Kapoor[9]

***Abstract*—Increasing reliance on technology has elevated the possibility of cyber-attacks directed towards financial, military and political interests. The significance of cybersecurity to the IT industry can no longer be under-estimated, and the security of data is a paramount concern. The Multi-task Learning (MTL) in cybersecurity offers a promising solution. In this paper, the potential of MTL is being explored as a solution to the sophisticated attacks against financial, defense and governmental system with the main goal being to determine how MTL improves the adaptive and intelligent cyber defense by learning on different, but related, security tasks at once. A SLR methodology was applied using the selected research articles on MTL in cybersecurity, which covered 40 articles. All selected papers were systematically reviewed to identify the application fields as well as common ML techniques. The findings have shown that there are 5 major fields where MTL can be applied: intrusion detection, malware classification, cyber threat detection, critical infrastructure security and online abuse detection. The research conducted concludes that supervised learning models, especially DL models like CNN, RNN and LSTM are the most applied models in this research area. MTL can greatly improve cybersecurity by providing adaptability, learn efficiency and shared representation across various tasks. It contributed to create a consolidated analysis of current MTL use cases in cybersecurity and highlight research challenges for future work in developing robust, scalable and intelligent security defense.**

***Keywords*: cybersecurity, multi-task learning, cyber threats, deep learning**

I. INTRODUCTION

The burgeoning digital world has made cybersecurity non-optional in the tech world. Cybersecurity serves as the first line of protection in the face of digital vulnerabilities such as unauthorized data access, injurious attacks, disruptions, and data corruption. Cyberattacks have evolved and escalated, and carry significant losses, and can affect the protection of personal data, and even extend to massive financial crimes. The FBI Internet Crime Complaint Center (IC3) receives approximately 652,000 com-plaints annually. In addition, according to the IC3, total losses have exceeded 27.6 billion USD since 2018. The statistics above speak profoundly regarding the need for adaptable approaches in security.

[1,2,3,4,5,6,7,8,9] Sukkur IBA University
Country: Pakistan
Email: *sanaullah@iba-suk.edu.pk

The protection of computer systems and other digital systems from information disclosure, theft, or disruption of the information and/or the systems is what cybersecurity is about. Information is the primary object of protection, and is provided by the core components such as cryptographic technologies, formal access control policies, and real-time access control policies. Standard defense mechanisms, such as IDS, IPS, firewalls, and antivirus programs, are essential tools used to counteract the threats posed by hostile cyberattacks on digital infrastructure. [1]. The manifestations and technologies have evolved, but the first iteration of the battle between cybercriminals and defenders can be traced to the 1970s with the emergence of the first computer virus [2].

The rapid progression of artificial intelligence has simultaneously catalyzed a transformation within the field of cybersecurity, forcing defensive strate-gies to adapt at an unprecedented rate. [3]. Its ability to analyze troves of network data in no time is invaluable in the field of cybersecurity. The global market for AI-based cybersecurity solutions has registered immense growth as it grew from14.9 billion in 2021 to 133.8 billion USD in 2030 [4] (Statistics & Trends 2022). The integration of ML and DL models is now pervasive across contemporary digital defense systems, serving as a standard standard for identifying and neutralizing threats. [5]–[8]. However, deep learning techniques are tremendously data hungry and require enormous computing power. This is where the challenge of multi-task learning (MTL) comes in. MTL has been found to be an effective approach to alleviating the theory of deep learning by training a single architecture to perform multiple tasks using inter-related tasks in a model by sharing features [9]. MTL enhances model generalization by mitigating the need for inordinate data and extensive anno-tations to be provided through knowledge transfer across multiple tasks/ datasets. In contrast to single-task learning (STL), MTL cumulatively has other advantages such as regularization and increased robustness to over fitting by virtue of inter-task relations [9], [10], which is very handy in data limited scenarios and complex feature spaces [11], [12].

While earlier studies have examined the appli-cation of MTL in several domains of Machine Learning in security [13]–[20], the design and implementation of MTL in its entirety has never been studied before. To investigate these areas, our current research provides a structured review of the literature, mapping out how MTL is applied within cyber defense. We evaluate its core advantages and implementation techniques as well as existing limitations through the lens of ten specific research inquiries.

II. BACKGROUND

A. Cyber security challenges

A cyber-attack is an attempt by an actor to in-fringe upon the confidentiality, integrity, and avail-ability of any information system and its data, or attempts to execute a cyber-attack against its data [19]. The offender exploits deficiencies in either the software and/or hardware and/or operating system, but also comprises of breaching other security principles (i.e., the principle of authenticity and/or non-repudiation). Newer studies have started to cast a spotlight on several cyber threats that one is likely to face in todays´ digital world, in addition to those of IoT. These studies help one to understand and appreciate the reality that cyberattacks are pervasive, particularly at the IoT application layer, and in every layer of an application, being systematically positioned to take advantage of the interconnected disposition of devices [24]. Table I shows the most common threats, their prevalence, and ranks. Viruses, Spyware, and Malware are ranked as the top with the highest prevalence. Meanwhile Botnet attack is at the 4th rank among all, with a prevalence of 10%. The Table II shows the most common cyberattacks, where the highest prevalence is that of the Denial-of-Service attack, while the Sinkhole attacked ranked as 4th with a prevalence score of 7%.

TABLE 1
Prevalence of Additional Threats/Attacks

Threat / Attack Type	Prevalence (%)	Rank
Viruses	30%	1st
Spyware	30%	1st
Malware	30%	1st
Malicious Code	20%	2nd
Phishing	15%	3rd
Cross-Site Scripting (XSS)	10%	4th
Botnet Attacks	10%	4th

TABLE 2
Prevalence of major Threats/Attacks

Threat / Attack Type	Prevalence (%)	Rank
Denial of Service (DoS)	39%	1st
Replay Attacks	38%	1st
Man-in-the-Middle (MitM) Attacks	29%	2nd
Selective Forwarding Attacks	12%	3rd
Sybil Attacks	11%	3rd
Sinkhole Attacks	8%	4th

Risks related to cybersecurity continue to grow problematically, including large-scale network pen-etrations and intrusions [20], widespread dissemina-tion of malicious software and malware [21], and phishing attacks of rapidly evolving sophistication [22]. Other online threats are spam campaigns [23], cyberbullying [25], hashtag abuse [26], and social metric manipulation via synthetic engagement [27], [28]. There are also assaults (services) on critical systems [29], which are more infrastructure-related, that augment the threat landscape. There are re-search efforts emerging, which indicate the growing need for malware detection [30], mitigation of DoS [31], and adaptive, integrated systems are the need of the times. Hence, the more integrated systems, such as MTL, grow in importance.

B. Multi Tasking Learning

By allowing multi-tasking to occur, which, for a given 'task' model, is expected to grow in efficiency, MTL also does system-level optimization [32], configuring many-to-one, a single multi-tasking model system will be able to one-to-many, or even many-to-many, as shown in Fig 1. Thus, optimizing the task of detecting spam by keyword pattern recognition and phishing via detection of urgency and optimizing such recognition interaction of separate STL [33].

In hard parameter sharing, multiple tasks rely on a shared backbone network while using separate output heads, which helps reduce overfitting. Soft parameter sharing works by having separate indi-vidual task models, but by having their parameters constrained to be similar via regularization as shown in Fig 2. The Focus of MTL is to increase learning efficiency by incorporating implicit data augmentation, attention-based task prioritization, cross-task feature sharing, representation bias, and some regularization techniques. The estimation of the optimization is known to have a balancing term λ to adjust the trade-off of the empirical loss versus the value of the relatedness of the tasks [11], [39]–[41]. Multi-Task Learning (MTL) has demonstrated high efficacy across diverse domains, including computer vision [34], bioinformatics [35], drug discovery [36], and natural language processing [37]. Within the cybersecurity landscape, it proves particularly advantageous by enabling the simultaneous execution of multiple detection operations while significantly minimizing resource consumption.

III. RELATED WORK

A broad view of existing survey studies can be found in Table 1. Observing the existing literature it can be inferred that it evolved from a general approach where machine learning solutions are mapped onto the domain of cyber security [16] and an analysis of offense/defense machine learning mechanisms [17], into several distinct and specialized tactical silos: DL solutions on the cyber security infrastructure such as IoT infrastructure [60, 63], cloud computing risks [20] or even phishing detection [21], and Mobile or Android malware classification [19, 61, 62]. It went even further in Mvula et al. [21] where specific repositories and metrics are examined for semi-supervised scenarios. Although such specialized reviews provide detailed explanations for each specific topic, they fail to identify common feature representation across multiple domains needed to solve multi-vector attacks. This collective oversight is precisely the reason why this research has been initiated. Existing single-task models, though successful for the given problem, suffer from significant computational overhead and are unable to transfer their learned features to parallel, distinct threat categories. Ibrahim et al. [114] observed the similar limitation in their analysis of machine learning for multi-task learning in cyber security; however, their research included a limited amount of research papers (28). As stated above, the present paper fills the observed void by presenting a much larger, empirical review on 40 main research papers to demonstrate a generalized multi-objective framework, showing that MTL overcomes data shortage by using shared parameters across several features and can defend from parallel threat categories.

IV. RESEARCH METHODOLOGY

This systematic literature review (SLR) is aligned with the restriction to 2023 data and also aligns with Kitchenham's guidelines [38] and is within the limits of the PRISMA guides [21], [22]. Three review stages were followed: Searching, filtering, and classifying studies, represented in the Fig 3.

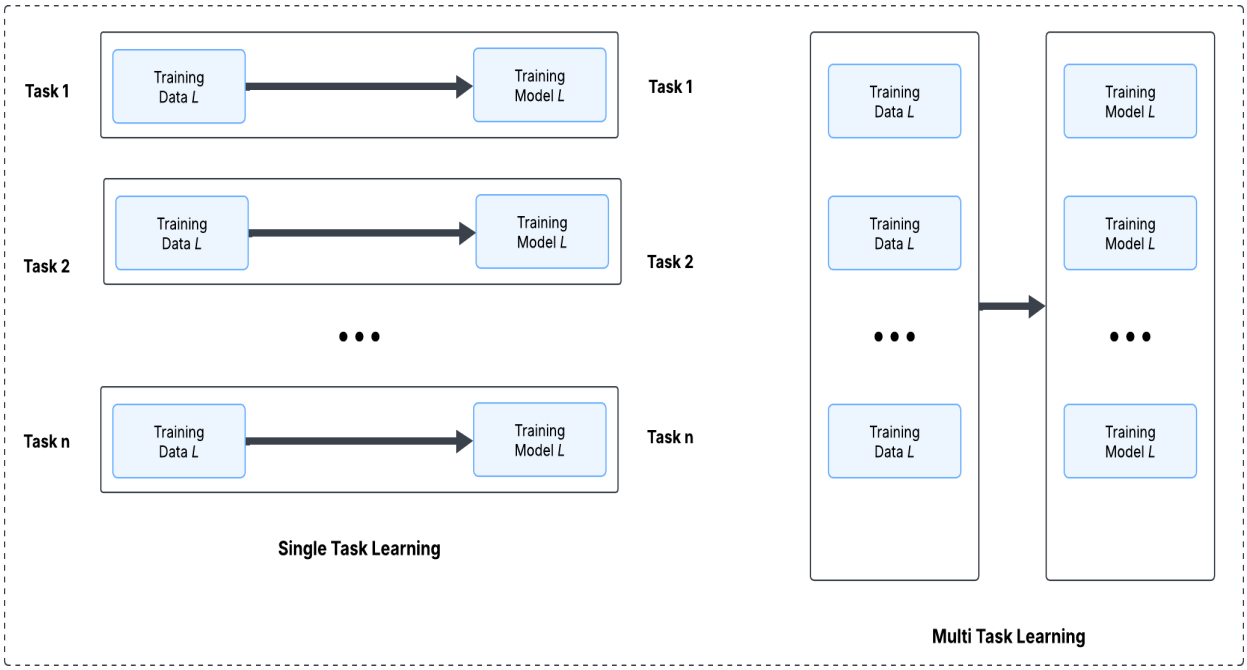

Figure 1: Architectural contrast between single-task and multi-task learning [63]

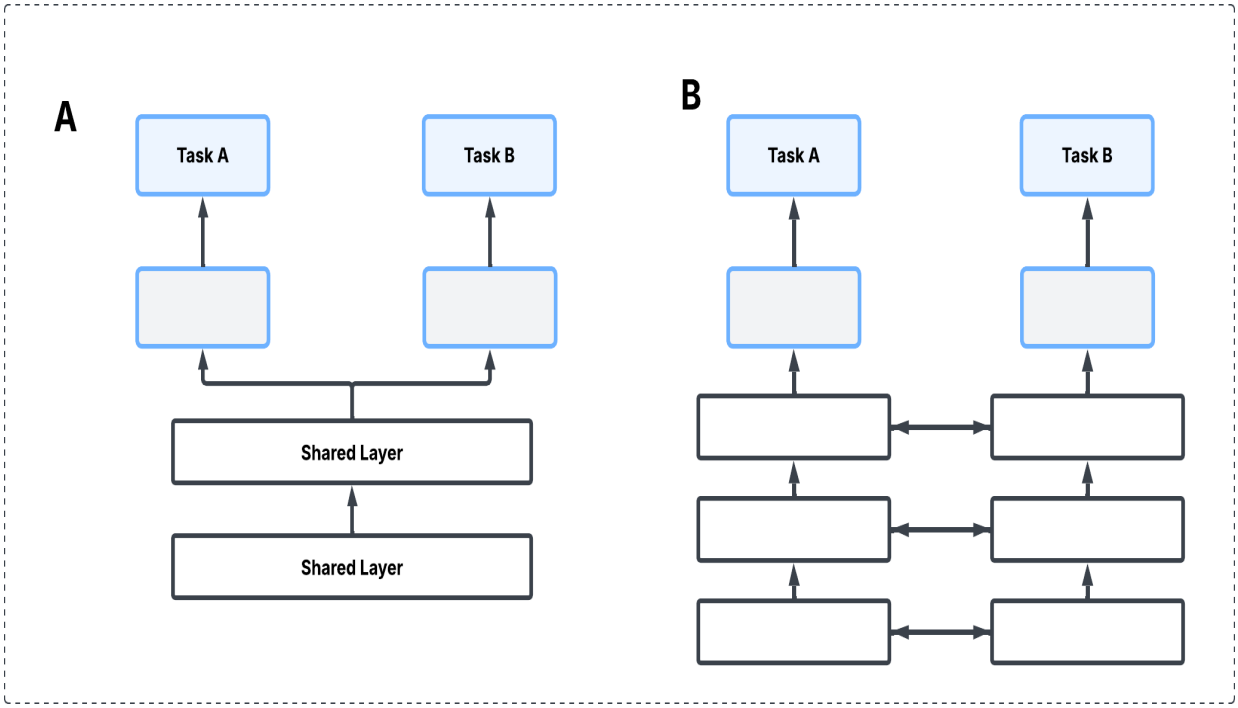

Figure 2: Parameter sharing strategies in deep MTL: (a) Hard sharing (b) Soft Sharing [38]

TABLE 3: Summary of Literature review

Ref No.	Year	Papers	Type	Contributions
Shimaa Ibrahim et al. [75]	2024	28	SLR	Evaluates the deployment of multi-task learning (MTL) across various cybersecurity domains
Mvula et al. [21]	2023	21	SLR	Synthesizes public data repositories and evaluation metrics specific to semi-supervised learning systems.
Idriss et al. [64]	2020	30	SLR	Analyzes deep learning-driven Intrusion Detection Systems (IDS) designed for IoT environments.
Catal et al. [18]	2022	43	SLR	Investigates the implementation of deep learning models explicitly targeted at phishing mitigation.

Nassif et al. [17]	2021	63	SLR	Examines diverse machine learning methodologies and techniques applied to cloud security architectures.
Senanayake et al. [16]	2021	106	SLR	Surveys machine learning approaches utilized for identifying Android-based mobile malware.
Catal et al. [18]	2020	40	SLR	Details the application and performance of deep learning algorithms in mobile malware detection frameworks.
Alvanxo et al. [14]	2020	120	SLR	Explores machine learning paradigms spanning both defensive and offensive cybersecurity strategies.
Ali et al. [13]	2020	21	SLR	Outlines foundational AI and machine learning techniques adapted for cyber defense.
Wang et al. [38]	2020	16	Review	Critiques deep learning frameworks specifically tailored for detecting Android mobile malware.
Sagar et al. [6]	2020	23	Survey	Investigates security vulnerabilities, specifically focusing on adversarial evasion tactics against machine learning models.
Androc˘ec et al. [67]	2018	25	SLR	Reviews machine learning protocols implemented to secure Internet of Things (IoT) ecosystems.
This study	**2026**	**40**	**SLR**	**Provides a comprehensive framework detailing the practical implementation of MTL solutions across cybersecurity applications.**

A. Search Phase

In the beginning of the review, the first step was to gather articles pertaining to the domain of cyber-security, employing pre-defined structured search strategies. At first, 200 papers were collected from highly regarded digital sources, such as Scopus, IEEE Xplore, Springer, Web of Science, and Google Scholar. The search was made with the filtering criterion of only including articles from peer-reviewed sources in the English language, published within the domain of cybersecurity between the years 2014 and 2023. Non-empirical works and studies that were not related to the domain were left out.

B. Inclusion and Exclusion Criteria

To help identify, refine, and manage the large number of results retrieved, a well-defined list of inclusion and exclusion criteria was established Ta-ble 3. These criteria define the selection boundaries, and they serve as a structured tool to ensure each candidate study is analyzed objectively on its own merit. Critical features such as publication year span, language and research type are all factored into the selection matrix, and are designed to ensure that the final review is evidence-based, scientific, and highly relevant to the questions being asked.

C. Study Filtering Phase

The studies were filtered using a stepwise approach shown in figure 3.

- Based on Search-Criteria check 100 papers were excluded.
- Duplicate articles were excluded, thus drop-ping the total from 100 to 80 unique papers.
- The papers were then screened for relevance, primarily based on the title and abstract, and then the selection was filtered down to 40 studies.
- All 40 studies in their entirety were then in-cluded in the review and subjected to detailed analysis.

D. Study Classification Phase

For this purpose, the studies' category breakdown was as follows:

- Cybersecurity (n = 20)
- Application areas of cybersecurity (n = 10)
- Challenges in cybersecurity (n = 10)

This structure provides a solid foundation for analyzing the available literature on cybersecurity.

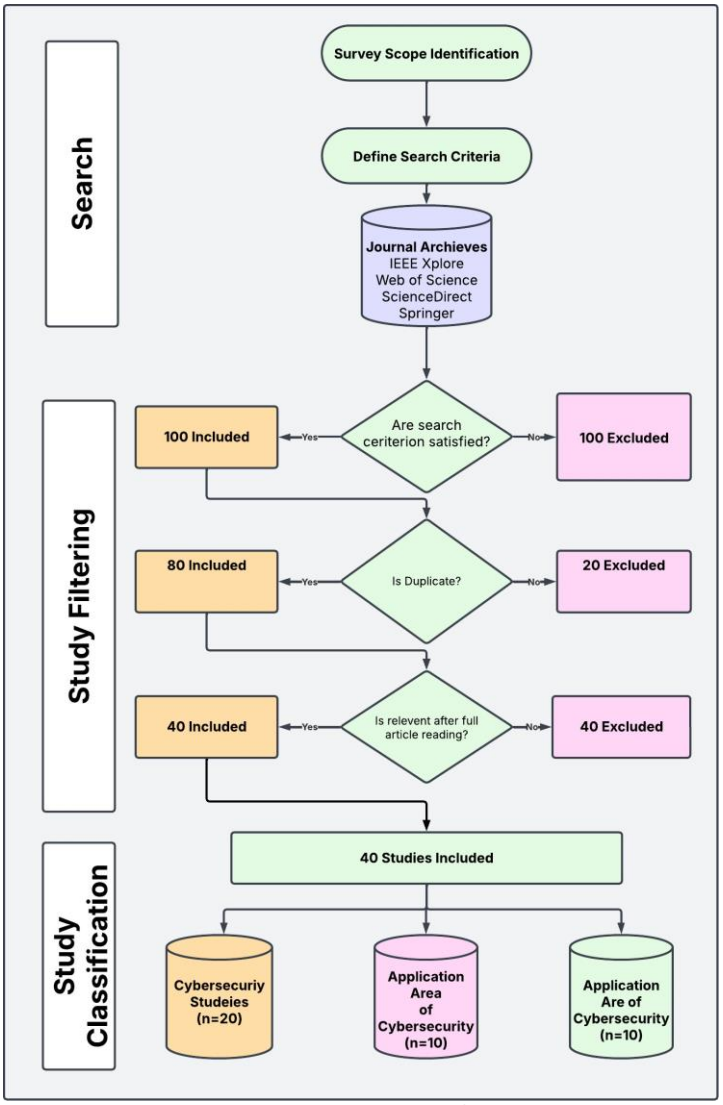

Figure 3: Study Selection and Classification Criteria

TABLE 4: Inclusion and Exclusion criteria

#	Inclusion Criteria	Exclusion Criteria
1	Articles written entirely in English.	Articles written in languages other than English.
2	Original primary empirical studies.	Multiple publications, meta-analyses, and other secondary research reviews.
3	Peer-reviewed journal articles and formal conference documents	Grey literature, white papers, and informal non-peer-reviewed proceedings..
4	Articles which primarily focus on the application or development of multi-task learning for the field of cybersecurity.	Articles not focusing directly on either multi-task architectures or cybersecurity.
5	Full-text articles published over the last decade (10 years).	Brief extended abstracts, editorials, and articles that are not available in full text.

V. RESULT AND DISCUSSION

In this section, we interpret the empirical data collected in response to the research questions. We begin with a look at the temporal distribution of the selected literature to map out the overall development of Multi-Task Learning (MTL) appli-cations within cybersecurity prior to looking into each specific thematic response.

The number of relevant articles by year, from 2017 to early 2026, is listed in Table 1. The original SLR protocol that was used only charted papers up 2023 (Shimaa Ibrahim et al. [75]) but recent breakthrough papers from 2024, 2025, and 2026 have been incorporated into the body to obtain a realistic portrayal of recent trends.

Rather than steady and linear development, the academic field demonstrates a resurgence of re-search activity. There is a stable rate of about 2 papers per year from 2017-2018 followed by a peak in 2019 with 5 papers, followed by 6 papers in 2020, and then a decline to 4 papers in 2021 before a sharp rise to 8 papers in 2022. The domain shows strong evidence of increased interest through 2024-2025. Whereas the 2023 corpus data show a steep drop-off in research volume, this is because our data were compiled relatively early in the year; overall interest in MTL in the security domain has clearly continued to grow. The sustained, growing publi-cation volume signifies a move away from small-scale experiments toward building on deep multi-task learning architectures as foundational methods to tackle more complex, multi-purpose network security and anomaly classification problems.

RQ1. In what specific ways can Multi-Task Learning (MTL) be effectively utilized within the broader landscape of cybersecurity applications?

Multitask learning (MTL) has a broad range of applications in cybersecurity, as shown in Figure. 4, the most significant of which are in network intrusion detection. For instance, in network intrusion detection, the analyzed MTL models consider various traffic features and (ab)normal behaviors [39], [40], [44], [47], [52], [53], [57], [59], [62]. Another of the critical areas of MTL in cybersecurity is malware detection, where the joint learning of static, dynamic, and behavioral attributes of malware improves classification [41], [43], [46], [48], [51]. In cyber threat detection, the MTL has been expanded to social media, where users can identify various online risks, black market content, malicious tweet patterns, and so on [30]–[32]. MTL has also been used for cyberbullying detection, where models learn to identify linguistic, contextual, and sentiment patterns for improved detection [45], [50].

One more of the important uses is Critical Infrastructure Protection, which includes of many interdependent systems [45], [54]–[56], [58], [60], [61]. These include the studies on the detection of cyber-attacks on smart grids, protection of critical infrastructure, securing IoT environments, detection of electricity theft in AMI systems, deployment of strong speaker verification, and detection of voice spoofing.

RQ2. What specific benefits and performance enhancements does the integration of MTL provide to frameworks of Cybersecurity?

MTL in cyber security systems is able to detect multiple attacks of different types concurrently and learn more complex (feature) representations more efficiently due to its shared layered structure [39], [40], [57], [59]. MTL integrates multiple, and often related, tasks into a single end-to-end model, which is able to cater to the different needs of many stakeholders, while also greatly lowering the computational requirements and redundancy (from duplication of efforts), due to shared feature extraction [49]. MTL also facilitates the detection of alarmed regions, rapidly adapts to new strains of malware without the requirement of full model retraining, and is designed for the real world, adaptive to shifting threat surface [52], [53]. For a general perspective, MTL makes cybersecurity systems stronger and more efficient, while also being flexible and adaptive to different situations, resource efficient, and more robust.

RQ3. What types of detection and prevention tasks are typically integrated into a multi-task learning architecture?

As shown in the Table V, tasks are divided into 5 different domains including P1: Intrusion Detection[70,47,49,57], P2: Malware Detection[42,43,48,51], P3: Threats Detection[26,27], P4:Cyberbullying[45,50], and P5: Infrastructure Protection [45,54,56,61].

Table 5: Domains and their associated tasks

Domain	Task
Intrusion Detection	Binary/multi-class anomaly Classification
Malware Detection	Family/type identification
Threats Detection	Semantic matching, intent classification
Cyberbullying	Toxicity scoring, hate speech tagging
Infrastructure Protection	Fault/anomaly forecasting

RQ4. Which specific ML algorithms are most frequently employed to facilitate multi-task learning?

In Fig 5, the dominance of supervised learning methods over other types of learning in multi-task learning in the field of cybersecurity is clear. Conversely, the area of study is likely to focus on techniques such as learning without a teacher, learning semi-supervised, or learning by teaching machines.

RQ5. What is the prevalence of various algorithmic architectures including both classical machine learning and advanced deep learning within the existing literature on security based MTL?

Key security challenges are numerous, including P1: Intrusions on Networks, P2: Malware, P3: Cyber Bullying, P4: Cyber Threats, and P5: Critical Infrastructure Problems. Figure 1 shows that the Algorithm Support Vector Machine (SVM) is primarily used to solve P1, P2, P4, and P5 [45, 48 , 49, 56]. In contrast, Random Forest remains the preferred classical approach for addressing cyberbullying detection (P3) [27]. Within the deep learning (DL) landscape, Convolutional Neural Networks (CNN) emerge as the primary architecture for network intrusion (P1) [70] and critical infrastructure protection (P5) [61]. For malware detection (P2) [43, 51], the literature shows an even distribution between CNN, Deep Neural Networks (DNN), and Autoencoders (AE). Notably, Multi-Layer Perceptrons (MLP) are the most frequently cited DL models for P3 [26]. It is essential to distinguish between MLPs and DNNs: while an MLP specifically refers to a feed-forward network with several fully connected layers, DNN is a broader classification encompassing highly layered architectures designed for complex, multi-purpose tasks. Finally, BERT (Bidirectional Encoder Representations from Transformers) dominates the cyber threat detection (P4) category [45], while CNNs maintain their prevalence in P5[61].

RQ6. Which multi-task learning models have been empirically shown to yield the highest levels of optimization and threat detection reliability across the literature?

Among the evaluated models, 99.62% accuracy in BELONGING category among all considered models in critical infrastructure [69, 18, 54, 56, 60]. It is DISTILLER who is the best in the cyber threat domain with an F1 score of 90% [26, 27, 28], achieving comparable values of precision and recall. For network-related security issues, MT-CNN has a 98.7% accuracy [52]. These results indicate that different MTL models excel in various areas of cyber security and thus the right model can yield considerably better results depending on the type.

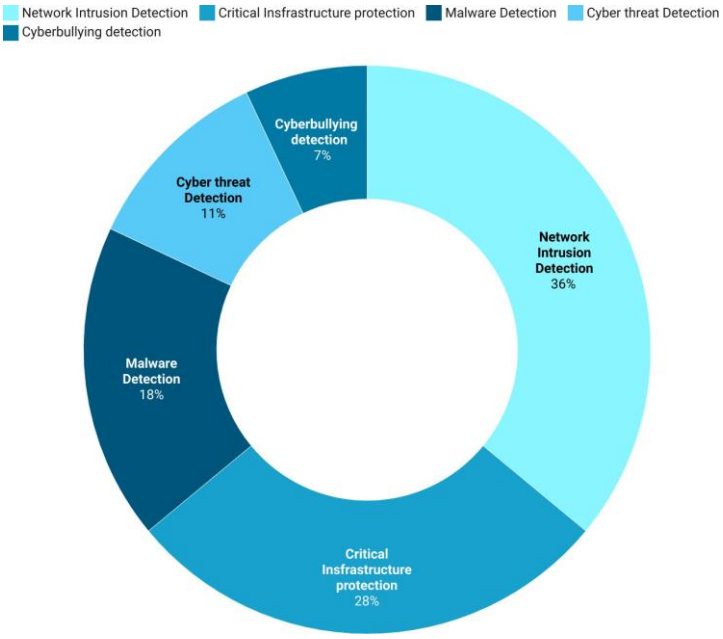

Figure 4: Applications

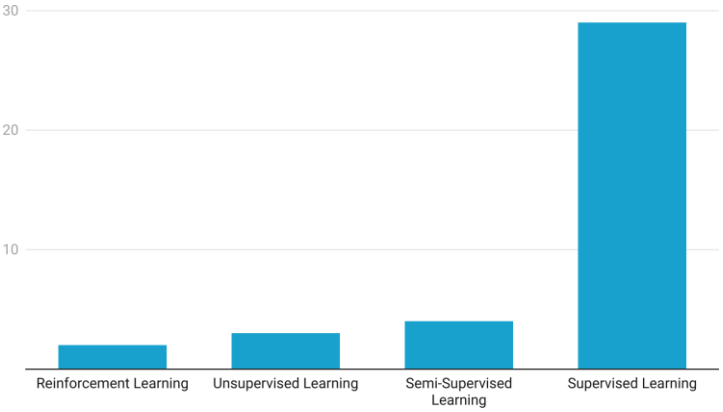

Figure 5: Paradigm Distribution

RQ7. What are the commonly used benchmark datasets for MTL in cybersecurity?

There are several widely accepted benchmark datasets that are used to assess MTL models across various cyber security domains. In the domain of network security, there are 2 benchmark datasets UNSW-NB15 [70, 44, 53] and CICIDS2017 (containing 2.5 million flows and 3 million records, respectively)[70, 42, 49, 53, 57] which are widely used to evaluate network intrusion and anomaly detection tasks. For malware analysis in the IoT context, the IoT-23 dataset [42] enables the evaluation of IoT malware detection mechanisms at scale.

RQ8. What evaluation strategies and quantitative parameters are most prevalent in validating multi-task learning results?

Various metrics are deployed to validate MTL models in security, ranging from detection and error rates to complex loss functions as shown in Figure 6. While accuracy is the dominant metric for intrusion and malware detection (P1, P2, P5) [70,43,45], precision and recall are more prevalent in social-media-based security tasks like cyberbullying detection

(P3)[26,27]. For broader threat detection (P4)[45,50], researchers typically adopt a multi-metric approach involving macro- or weighted-F1 scores. The widespread adoption of cross-validation across these studies highlights its perceived reliability as a validation framework. In summary, the literature identifies accuracy, F-measure, and cross-validation as the most established parameters for evaluating MTL efficacy in cybersecurity.

RQ9. Which computational environments and development frameworks are typically utilized for the construction of MTL systems?

Numerous academic articles display the application of free software for machine/deep learning, including, but not limited to, TensorFlow, PyTorch, and Keras, in the development of multi-task learning models. However, in the research this paper reviews, close to half (48%) of the studies did not mention any of the frameworks. From the studies that did mention, 24% of them used Keras, 14% used PyTorch, and another 14% used TensorFlow to model. This indicates that there are still gaps in mentioning what of the open-source frameworks were used for MTL development, despite the frameworks' popularity.

RQ10. What are the primary technical hurdles and potential mitigation strategies associated with the adoption of multi-task learning in cybersecurity?

Modern frameworks have applied complex MTL and deep learning architectures in order to handle network detection bottlenecks, data quality limitation and the issues associated with feature extraction: inference/labeling/optimization bottlenecks can be solved by applying hybrid Autoencoders [72], specific MTL classification net-works [52], generative models (DCGAN/SGAN) [51], end-to-end supervised-unsupervised training approach [55], adaptive loss weighing [26] whereas limited data, class imbalance and dataset diversity can be dealt with the application of cross task knowledge sharing [53], two auxiliary tasks [44], multi-task architecture using LSTM [42], and synthetic data generation [69]. Finally, the insufficient feature representations issue has been dealt by combining memory-based storage with an attention mechanism [44].

VI. CONCLUSION AND FUTURE DIRECTIONS

The first of its kind SLR brings together multi-task learning across 40 studies in this particular area to identify 5 key areas and a dominant use of supervised deep learning. The ability of MTL to customize multiple security tasks at once improves performance and flexibility overall when compared to doing isolated, separate models.

However, challenges in negative task transfer, limited data, and deployment scalability remain. Potential solutions include:

- The use of semi-supervised and reinforcement MTL to reduce the need for labeling.
- The use of LLMs language models for contextual threat reasoning.
- The creation of benchmarks for real-world assessments.
- The use of a mix of hard and soft adaptive weight sharing.
- The application of MTL in real-world scenarios, for instance, SOCs.

This SLR sets the ground for the cybersecurity field to be able to progress further and enhance the flexibility and the overall efficacy of the defense mechanisms.

Figure 6: Evaluation Metrics

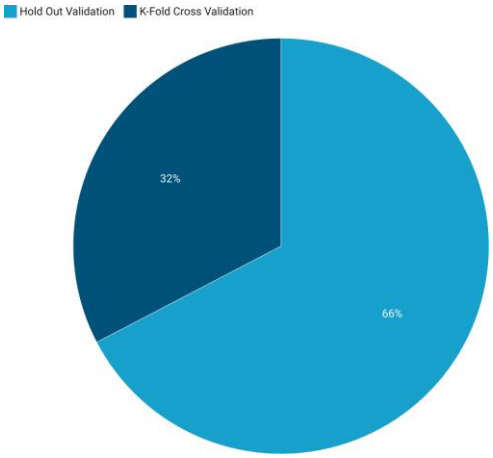

Figure 7: Validation Methods

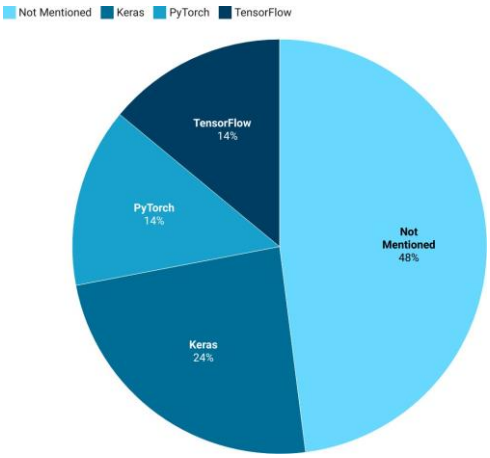

Figure 8: Platforms Used to Develop MTL

REFERENCES

[1] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, "A survey on machine learning techniques for cyber security in the last decade," IEEE Access, vol. 8, pp. 222310–222354, 2020.

[2] P. Szor, The Art of Computer Virus Research and Defense. Upper Saddle River, NJ, USA: Pearson Education, 2005.

[3] D. Gümüşbaş, T. Yıldırım, A. Genovese, and F. Scotti, "A comprehensive survey of databases and deep learning methods for cybersecurity and intrusion detection systems," IEEE Systems Journal, vol. 15, no. 2, pp. 1717–1731, 2021.

[4] M. F. Ansari, B. Dash, P. Sharma, and N. Yathiraju, "The impact and limitations of artificial intelligence in cybersecurity: A literature review," International Journal of Advanced Research in Computer and Communication Engineering, 2022.

[5] M. Taddeo, "Three ethical challenges of applications of artificial intelligence in cybersecurity," Minds and Machines, vol. 29, no. 2, pp. 187–191, 2019.

[6] R. Sagar, R. Jhaveri, and C. Borrego, "Applications in security and evasions in machine learning: A survey," Electronics, vol. 9, no. 1, p. 97, 2020.

[7] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, S. Chen, D. Liu, and J. Li, "Performance comparison and current challenges of using machine learning techniques in cybersecurity," Energies, vol. 13, no. 10, p. 2509, 2020.

[8] M. Macas, C. Wu, and W. Fuertes, "A survey on deep learning for cybersecurity: Progress, challenges, and opportunities," Computer Networks, vol. 212, p. 109032, 2022.

[9] M. Crawshaw, "Multi-task learning with deep neural networks: A survey," arXiv preprint arXiv:2009.09796, 2020.

[10] S. Ruder, "An overview of multi-task learning in deep neural networks," arXiv preprint arXiv:1706.05098, 2017.

[11] Y. Zhang and Q. Yang, "An overview of multi-task learning," National Science Review, vol. 5, no. 1, pp. 30–43, 2018, doi: 10.1093/nsr/nwx105

[12] A. Yan, X. Wang, Y. Yang, R. Fox, X. Wang, and J. Gonzalez, Multi-task Learning Architectures and Applications, Master's thesis, Dept. EECS, Univ. California, Berkeley, CA, USA, 2020.

[13] R. Ali, A. Ali, F. Iqbal, A. M. Khattak, and S. Aleem, "A systematic review of artificial intelligence and machine learning techniques for cyber security," in Big Data and Security, Y. Tian, T. Ma, and M. K. Khan, Eds. Singapore: Springer, 2020, pp. 584–593.

[14] I. D. Aiyanyo, H. Samuel, and H. Lim, "A systematic review of defensive and offensive cybersecurity with machine learning," Applied Sciences, 2020, doi: 10.3390/app10175811

[15] R. Ahmad and I. Alsmadi, "Machine learning approaches to IoT security: A systematic literature review," Internet of Things, vol. 14, p. 100365, 2021, doi: 10.1016/j.iot.2021.100365

[16] J. Senanayake, H. Kalutarage, and M. O. Al-Kadri, "Android mobile malware detection using machine learning: A systematic review," Electronics, vol. 10, no. 13, p. 1606, 2021, doi: 10.3390/electronics10131606

[17] A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani, and F. M. Dakalbab, "Machine learning for cloud security: A systematic review," IEEE Access, vol. 9, pp. 20717–20735, 2021, doi: 10.1109/ACCESS.2021.3054129

[18] C. Catal, G. Giray, B. Tekinerdogan, S. Kumar, and S. Shukla, "Applications of deep learning for phishing detection: A systematic literature review," Knowledge and Information Systems, vol. 64, pp. 1457–1500, 2022, doi: 10.1007/s10115-022-01672-x

[19] R. Moore, Cybercrime: Investigating High-Technology Computer Crime. Canada: Taylor & Francis, 2014, pp. 1–318.

[20] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets and challenges," Cybersecurity, 2019, doi: 10.1186/s42400-019-0038-7

[21] P. K. Mvula, P. Branco, G.-V. Jourdan, and H. L. Viktor, "A systematic literature review of cyber-security data repositories and performance assessment metrics for semi-supervised learning," Discover Data, 2023, doi: 10.1007/s44248-023-00003-x

[22] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing attacks: A recent comprehensive study and a new anatomy," Frontiers in Computer Science, 2021, doi: 10.3389/fcomp.2021.563060

[23] F. Jáñez-Martino, R. Alaiz-Rodríguez, V. González-Castro, E. Fidalgo, and E. Alegre, "A review of spam email detection: Analysis of spammer strategies and the dataset shift problem," Artificial Intelligence Review, vol. 56, no. 2, pp. 1145–1173, 2023, doi: 10.1007/s10462-022-10184-7

[24] A. A. Almuqren, "Cybersecurity threats, counter-measures and mitigation techniques on the IoT: Future research directions," Journal of Computer Science Research and Applications, vol. 2025, no. 1, 2025.

[25] P. K. Smith, J. Mahdavi, M. Carvalho, S. Fisher, S. Russell, and N. Tippett, "Cyberbullying: Its nature and impact in secondary school pupils," Journal of Child Psychology and Psychiatry, vol. 49, no. 4, pp. 376–385, 2008, doi: 10.1111/j.1469-7610.2007.01846.x

[26] Z. Qu, C. Lyu, and C.-H. Chi, "Multi-task learning framework for detecting hashtag hijack attack in mobile social networks," Proceedings of the IEEE, pp. 90–98, 2022.

[27] U. Arora, W. S. Paka, and T. Chakraborty, "Multi-task learning for blackmarket tweet detection," in Proc. ACM, pp. 127–130, 2019.

[28] N. Dionísio, F. Alves, P. Ferreira, and A. Bessani, "Towards end-to-end cyberthreat detection from Twitter using multi-task learning," in Proc. IEEE World Congress on Computational Intelligence (WCCI), 2020.

[29] E. Vigano, M. Loi, and E. Yaghmaei, "Cybersecurity of critical infrastructure," in The Ethics of Cybersecurity, 2020, pp. 157–177.

[30] S. S. Shafin, G. Karmakar, and I. Mareels, "Obfuscated memory malware detection in resource-constrained IoT devices for smart city applications," Sensors, 2023, doi: 10.3390/s23115348

[31] S. S. Shafin, S. A. Prottoy, S. Abbas, S. B. Hakim, A. Chowdhury, and M. M. Rashid, "Distributed denial of service attack detection using machine learning and class oversampling," in Applied Intelligence and Informatics, M. Mahmud et al., Eds. Cham, Switzerland: Springer, 2021, pp. 247–259.

[32] K.-H. Thung and C.-Y. Wee, "A brief review on multi-task learning," Multimedia Tools and Applications, vol. 77, no. 22, pp. 29705–29725, 2018, doi: 10.1007/s11042-018-6463-x

[33] I. Firdausi, C. Lim, A. Erwin, and A. S. Nugroho, "Analysis of machine learning techniques used in behavior-based malware detection," in Proc. 2010 2nd Int. Conf. Advances in Computing, Control, and Telecommunication Technologies, 2010, pp. 201–203, doi: 10.1109/ACT.2010.33

[34] Y. Ganin and V. Lempitsky, "Unsupervised domain adaptation by backpropagation," in Proc. 32nd Int. Conf. Machine Learning, vol. 37. PMLR, 2015, pp. 1180–1189.

[35] C. Widmer, N. C. Toussaint, Y. Altun, and G. Rätsch, "Inferring latent task structure for multitask learning by multiple kernel learning," BMC Bioinformatics, vol. 11, p. S5, 2010, doi: 10.1186/1471-2105-11-S8-S5

[36] B. Ramsundar, S. Kearnes, P. Riley, D. Webster, D. Konerding, and V. Pande, "Massively multitask networks for drug discovery," arXiv preprint arXiv:1502.02072, 2015.

[37] R. Collobert and J. Weston, "A unified architecture for natural language processing: Deep neural networks with multitask learning," in Proc. 25th Int. Conf. Machine Learning (ICML '08), 2008, pp. 160–167, doi: 10.1145/1390156.1390177

[38] S. Wang, Q. Wang, and M. Gong, "Multi-task learning based network embedding," Frontiers in Neuroscience, 2020, doi: 10.3389/fnins.2019.01387

[39] A. Argyriou, T. Evgeniou, and M. Pontil, "Multi-task feature learning," in Advances in Neural Information Processing Systems, vol. 19. Cambridge, MA, USA: MIT Press, 2006.

[40] K. Weiss, T. M. Khoshgoftaar, and D. Wang, "A survey of transfer learning," Journal of Big Data, 2016, doi: 10.1186/s40537-016-0043-6

[41] G. Y. Ke, Y. Pan, J. Yin, and C. Q. Huang, "Optimizing evaluation metrics for multitask learning via the alternating direction method of multipliers," IEEE Transactions on Cybernetics, vol. 48, no. 3, pp. 993–1006, 2018.

[42] S. Ali, O. Abusabha, F. Ali, M. Imran, and T. Abuhmed, "Effective multitask deep learning for IoT malware detection and identification using behavioral traffic analysis," IEEE Transactions on Network and Service Management, vol. 20, pp. 1199–1209, 2023, doi: 10.1109/TNSM.2022.3200741

[43] O. Bader, A. Lichy, C. Hajaj, R. Dubin, and A. Dvir, "MalDIST: From encrypted traffic classification to malware traffic detection and classification," in Proc. 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), 2022, pp. 527–533.

[44] J. Lan, X. Liu, B. Li, J. Sun, B. Li, and J. Zhao, "MEMBER: A multitask learning model with hybrid deep features for network intrusion detection," Computers & Security, 2022, doi: 10.1016/j.cose.2022.102919

[45] K. Maity, T. Sen, S. Saha, and P. Bhattacharyya, "MTBullyGNN: A graph neural network-based multitask framework for cyberbullying detection," IEEE Transactions on Computational Social Systems, 2023, doi: 10.1109/TCSS.2022.3230974

[46] A. Bensaoud and J. Kalita, "Deep multi-task learning for malware image classification," Journal of Information Security and Applications, vol. 64, p. 103057, 2022.

[47] G. Aceto, D. Ciuonzo, A. Montieri, and A. Pescapè, "Distiller: Encrypted traffic classification via multimodal multitask deep learning," Journal of Network and Computer Applications, 2021, doi: 10.1016/j.jnca.2021.102985

[48] S. H. Lee, S. C. Lan, H. C. Huang, C. W. Hsu, Y. S. Chen, and S. Shieh, "EC-model: An evolvable malware classification model," in Proc. 2021 IEEE Conf. Dependable and Secure Computing (DSC), 2021, pp. 1–8.

[49] O. Barut, Y. Luo, T. Zhang, W. Li, and P. Li, "Multi-task hierarchical learning based network traffic analytics," in Proc. IEEE Int. Conf. Communications (ICC), 2021, pp. 1–6.

[50] P. Kapil and A. Ekbal, "A deep neural network based multi-task learning approach to hate speech detection," Knowledge-Based Systems, p. 106458, 2020, doi: 10.1016/j.knosys.2020.106458

[51] S. Wang, Q. Wang, Z. Jiang, X. Wang, and R. Jing, "A weak coupling of semi-supervised learning with generative adversarial networks for malware classification," Institute of Electrical and Electronics Engineers, 2020, pp. 3775–3782.

[52] S. Rezaei and X. Liu, "Multitask learning for network traffic classification," in Proc. 29th Int. Conf. Computer Communications and Networks (ICCCN), 2020, pp. 1–9.

[53] L. Sun, Y. Zhou, Y. Wang, C. Zhu, and W. Zhang, "The effective methods for intrusion detection with limited network attack data: Multi-task learning and oversampling," IEEE Access, vol. 8, pp. 185384–185398, 2020, doi: 10.1109/ACCESS.2020.3029100

[54] X. Li, L. Zhu, Z. Yu, B. Guo, and Y. Wan, "Vanishing point detection and rail segmentation based on deep multi-task learning," IEEE Access, vol. 8, pp. 163015–163025, 2020, doi: 10.1109/ACCESS.2020.3019318

[55] T. Hu, Q. Guo, X. Shen, H. Sun, R. Wu, and H. Xi, "Utilizing unlabeled data to detect electricity fraud in AMI: A semisupervised deep learning approach," IEEE Transactions on Neural Networks and Learning Systems, vol. 30, pp. 3287–3299, 2019, doi: 10.1109/TNNLS.2018.2890663

[56] H. H. Nguyen, F. Fang, J. Yamagishi, and I. Echizen, "Multi-task learning for detecting and segmenting manipulated facial images and videos," in Proc. 2019 IEEE 10th Int. Conf. Biometrics Theory, Applications and Systems (BTAS), 2019, pp. 1–8.

[57] Y. Zhao, J. Chen, D. Wu, J. Teng, and S. Yu, "Multi-task network anomaly detection using federated learning," in Proc. ACM Conf., 2019, pp. 273–279.

[58] J. Li, M. Sun, and X. Zhang, "Multi-task learning of deep neural networks for joint automatic speaker verification and spoofing detection," in Proc. 2019 Asia-Pacific Signal and Information Processing Association Annual Summit and

Conference (APSIPA ASC), 2019, pp. 1517–1522.

[59] H. Huang, H. Deng, J. Chen, L. Han, and W. Wang, "Automatic multi-task learning system for abnormal network traffic detection," International Journal of Emerging Technologies in Learning, vol. 13, pp. 4–20, 2018, doi: 10.3991/ijet.v13i04.8466

[60] K. Demertzis, L. Iliadis, and V. D. Anezakis, "MO-LESTRA: A multi-task learning approach for real-time big data analytics," in Proc. 2018 Innovations in Intelligent Systems and Applications (INISTA), 2018, pp. 1–8.

[61] J. Yu, B. Zhang, Z. Kuang, D. Lin, and J. Fan, "IPrivacy: Image privacy protection by identifying sensitive objects via deep multi-task learning," IEEE Transactions on Information Forensics and Security, vol. 12, pp. 1005–1016, 2017, doi: 10.1109/TIFS.2016.2636090

[62] B. Li, Y. Lin, and S. Zhang, "Multi-task learning for intrusion detection on web logs," Journal of Systems Architecture, vol. 81, pp. 92–100, 2017, doi: 10.1016/j.sysarc.2017.10.011

[63] C. Park, Y. Kim, Y. Park, and S. B. Kim, "Multitask learning for virtual metrology in semiconductor manufacturing systems," Computers & Industrial Engineering, vol. 123, pp. 209–219, 2018, doi: 10.1016/j.cie.2018.06.024

[64] I. Idriss, M. Azizi, and O. Moussaoui, "IoT security with deep learning-based intrusion detection systems: A systematic literature review," in Proc. 2020 Fourth Int. Conf. Intelligent Computing in Data Sciences (ICDS), 2020, pp. 1–10.

[65] C. Catal, G. Giray, and B. Tekinerdogan, "Applications of deep learning for mobile malware detection: A systematic literature review," Neural Computing and Applications, vol. 34, no. 2, pp. 1007–1032, 2022.

[66] Z. Wang, Q. Liu, and Y. Chi, "Review of Android malware detection based on deep learning," IEEE Access, vol. 8, pp. 181102–181126, 2020, doi: 10.1109/ACCESS.2020.3028370

[67] D. Androcec and N. Vrcek, "Machine learning for the Internet of Things security: A systematic review," in Proc. SciTePress, Portugal, 2019, pp. 563–570.

[68] B. Kitchenham, R. Pretorius, D. Budgen, O. Pearl Brereton, M. Turner, M. Niazi, and S. Linkman, "Systematic literature reviews in software engineering—A tertiary study," Information and Software Technology, vol. 52, no. 8, pp. 792–805, 2010, doi: 10.1016/j.infsof.2010.03.006

[69] A. Takiddin, R. Atat, M. Ismail, K. Davis, and E. Serpedin, "A graph neural network multi-task learning-based approach for detection and localization of cyberattacks in smart grids," Institute of Electrical and Electronics Engineers, 2023, pp. 1–5.

[70] S. A. Albelwi, "An intrusion detection system for identifying simultaneous attacks using multi-task learning and deep learning," in Proc. 2022 2nd Int. Conf. Computing and Information Technology (ICCIT), 2022, pp. 349–353.

[71] S. Hamdan, S. Almajali, M. Ayyash, H. B. Salameh, and Y. Jararweh, "An intelligent edge-enabled distributed multi-task learning architecture for large-scale IoT-based cyber-physical systems," Simulation Modelling Practice and Theory, 2023, doi: 10.1016/j.simpat.2022.102685

[72] Q. Liu, D. Wang, Y. Jia, S. Luo, and C. Wang, "A multi-task based deep learning approach for intrusion detection," Knowledge-Based Systems, 2022, doi: 10.1016/j.knosys.2021.107852

[73] K. Maity, T. Sen, S. Saha, and P. Bhattacharyya, "MTBullyGNN: A graph neural network-based multitask framework for cyberbullying detection," IEEE Transactions on Computational Social Systems, 2022, doi: 10.1109/TCSS.2022.3230974

[74] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in Proc. 2015 Military Communications and Information Systems Conference (MilCIS), 2015, pp. 1–6, doi: 10.1109/MilCIS.2015.7348942

[75] S. Ibrahim, C. Catal, and T. Kacem, "The use of multi-task learning in cybersecurity applications: A systematic literature review," Neural Computing and Applications, vol. 36, pp. 22053–22079, 2024.