STATISTICS, OPTIMIZATION AND INFORMATION COMPUTING
Stat., Optim. Inf. Comput., Vol. **x**, Month 202x, pp 0–26.
Published online in International Academic Press (www.IAPress.org)

Transforming IoT Security through Large Language Models: A Comprehensive Systematic Review and Future Directions

Mohammed Tawfik[1,*], Amr H. Abdelhaliem[2], Islam S. Fathi[3]

[1]*Department of Cyber Security, Faculty of Information Technology, Ajloun National University, P.O.43, Ajloun-26810, JORDAN*
[2]*Department of Cyber Security, Faculty of Science and Information Technology, Irbid National University, Irbid, JORDAN*
[3]*Department of Computer Science, Faculty of Information Technology, Ajloun National University, P.O.43, Ajloun-26810, JORDAN*

Abstract The rapid integration of Large Language Models (LLMs) in Internet of Things (IoT) security presents both unprecedented opportunities and complex challenges. This systematic literature review examines 34 recent studies (2022-2024) to evaluate the effectiveness, challenges, and architectural innovations of LLM implementations in IoT security environments. Through a rigorous methodology following PRISMA guidelines, we analyze performance metrics, implementation strategies, and resource optimization approaches across diverse security applications. Our findings reveal significant advancements in detection capabilities, with frameworks like SecurityBERT achieving 98.2% accuracy while reducing model size by 89.85%, and privacy-preservation mechanisms demonstrating up to 98.247% protection effectiveness. However, persistent challenges emerge in resource optimization, real-time processing requirements, and cross-platform compatibility. The review identifies critical research gaps in standardization frameworks, ultra-constrained device optimization, and privacy-preserving architectures. Our analysis reveals promising architectural innovations, including hybrid deployment strategies reducing energy consumption by 45% and federated learning approaches achieving 97.12% accuracy while maintaining data privacy. This comprehensive review provides a foundation for future research directions in LLM-based IoT security, emphasizing the need for balanced approaches between security effectiveness and resource constraints. The findings suggest that successful implementation requires careful consideration of computational requirements, privacy preservation, and architectural optimization for resource-constrained environments.

Keywords Large Language Models; Internet of Things Security; Systematic Review; Statistical Security Analysis; Optimization Methods; Resource Efficiency; Security Architecture; Privacy Preservation

DOI: 10.19139/soic-2310-5070-2424

1. Introduction

The Internet of Things (IoT) is fundamentally transforming digital infrastructure across global sectors, with projections indicating over 50 billion connected devices by 2030 [1]. This unprecedented growth has created a complex technological ecosystem spanning healthcare, industrial automation, smart cities, and consumer applications. In healthcare, IoT devices now manage critical patient monitoring systems and automated drug delivery [2], [3]. Industrial settings leverage IoT for real-time production control and predictive maintenance [4]. Smart cities deploy IoT networks for traffic management, resource optimization, and public safety [5]. However, this widespread integration of IoT technologies, while revolutionizing connectivity and automation, has also created unprecedented security challenges that traditional cybersecurity approaches struggle to address effectively [6], [7].

Recent security incidents highlight the critical nature of these challenges. In 2023, IoT-connected assembly lines in the automotive industry were identified as high-risk targets for sophisticated cyberattacks. Such attacks have the potential to cause significant operational disruptions, including production shutdowns lasting multiple

*Correspondence to: Corresponding Authors: Mohammed Tawfik (Email: M.Tawfik@anu.edu.jo)).

ISSN 2310-5070 (online) ISSN 2311-004X (print)

days and resulting in substantial financial losses. Studies document the growing vulnerability of IoT systems in smart manufacturing environments, necessitating robust cybersecurity measures to prevent these scenarios [8], [9], [10]. A recent breach in a smart building system within a European financial district compromised environmental controls across multiple buildings, showcasing how IoT vulnerabilities can lead to cascading failures. In healthcare settings, compromised IoT devices have disrupted patient care and exposed sensitive medical data, highlighting the critical need for robust IoT security measures [11]. These incidents underscore the importance of safeguarding interconnected systems to prevent significant operational and safety risks [12].

The security challenges in IoT environments are particularly complex due to several unique characteristics. First, the heterogeneous nature of IoT devices creates diverse attack surfaces, ranging from physical tampering to network-level exploits and application vulnerabilities [13]. Second, resource constraints on IoT devices limit the implementation of traditional security measures. Third, the scale and complexity of IoT networks make traditional monitoring and threat detection approaches increasingly ineffective [14], [15]. These challenges are further compounded by the increasing sophistication of cyber threats targeting IoT infrastructure. Traditional security mechanisms demonstrate significant limitations in the IoT context. Static rule-based systems and conventional machine learning approaches often fail to adapt to the dynamic nature of emerging threats and struggle with the scale and complexity of IoT networks [16]. These limitations are particularly evident in three critical areas: the ability to process and analyze heterogeneous data streams in real-time, the capability to detect zero-day attacks and novel threat patterns, and the challenge of maintaining security while operating within the resource constraints of IoT devices [17].

Large Language Models (LLMs) represent a transformative approach to addressing these security challenges. Unlike traditional security approaches, LLMs demonstrate remarkable capabilities in understanding context, recognizing patterns, and generating adaptive responses to security threats [18]. Their sophisticated pattern recognition capabilities enable the identification of subtle anomalies in device behavior that traditional systems might miss. Furthermore, their ability to process and analyze unstructured data, combined with advanced semantic understanding, offers promising solutions for enhancing IoT security across multiple dimensions: predictive threat detection through pattern recognition and contextual analysis, automated security policy generation and enforcement, intelligent anomaly detection with reduced false positives, and adaptive defense mechanisms that evolve with emerging threats [19].

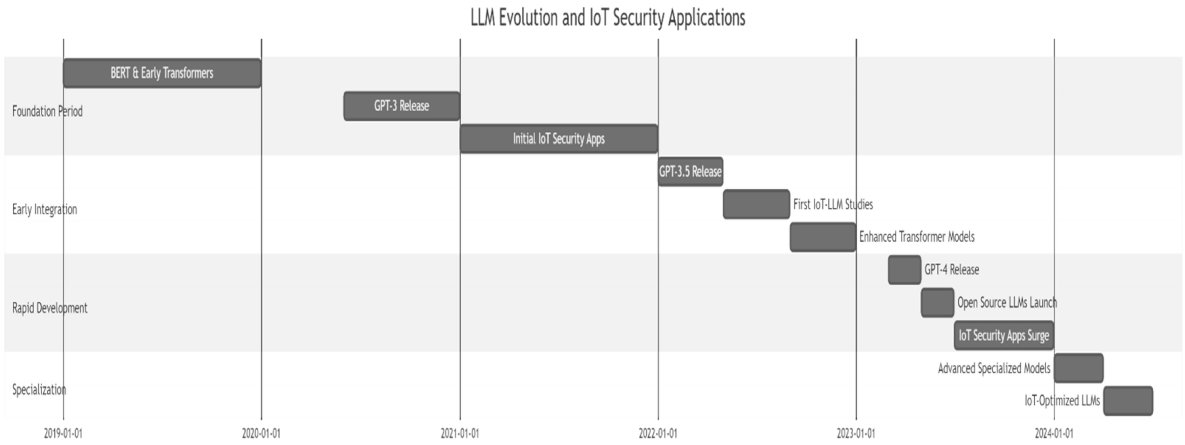

Figure 1. Timeline of LLM Evolution and IoT Security Applications: From BERT to IoT-Optimized Models

The evolution of Large Language Models (LLMs) in IoT security has seen significant developments from 2019 to 2024, progressing through distinct phases as illustrated in Figure 1. . This timeline demonstrates the field's rapid advancement from early transformer models to specialized IoT-optimized LLMs, marking key milestones

including the GPT-3 release in 2020, the first IoT security applications, and the emergence of IoT-optimized LLMs in 2024. The progression shows four main developmental stages: Foundation Period, Early Integration, Rapid Development, and Specialization, reflecting the increasing sophistication and domain-specific adaptation of LLMs for IoT security challenges [20].

The focus on the 2022-2024 timeframe is particularly significant due to transformative developments in LLM capabilities during this period. The release of GPT-3.5 (2022) and GPT-4 (2023), along with the emergence of open-source LLMs, marked a step change in natural language understanding and generation capabilities. This period saw the first practical applications of LLMs to IoT security challenges, enabled by improvements in model efficiency, context understanding, and domain adaptation. The emergence of specialized and IoT-optimized LLMs in 2024 further accelerated adoption in security applications. Prior to 2022, LLM applications in IoT security were largely theoretical due to computational constraints and limited model capabilities.

Early implementations have shown promising results, with some studies reporting detection accuracy improvements of up to 20% compared to traditional approaches [21]. However, the integration of LLMs in IoT security presents its own set of challenges. Questions remain about their computational requirements, their ability to operate within resource-constrained environments, and the balance between model complexity and real-time performance. Through a systematic analysis of 34 recent studies (2023-2024), we examine the evolution of LLM applications in IoT security, focusing on architectural innovations, performance metrics, and practical implementation challenges. Our review reveals significant advancements in several key areas: enhanced threat detection accuracy, with performance improvements of up to 15-20% compared to traditional approaches, novel lightweight LLM architectures specifically designed for resource-constrained IoT environments, and innovative approaches to privacy preservation and model interpretability.

To further illustrate this evolution, Figure 2 presents a detailed analysis of the technological progression and performance metrics across different implementation phases.

As shown in Figure 2, each phase introduced significant advancements in both capabilities and performance metrics. The Initial Integration phase established baseline performance with BERT-based models achieving 85-90% accuracy [2]. The Optimization phase marked a crucial advancement through SecurityBERT, achieving 89.85% size reduction while maintaining detection effectiveness [2]. The Architecture Innovation phase demonstrated substantial performance improvements through the EBIDS system, achieving 0.08273335s execution time and 99.96% detection accuracy [11]. The current state in 2024 represents significant maturity with 98-99% accuracy rates and enhanced privacy preservation capabilities [10].

This progression demonstrates not only quantitative improvements in performance metrics but also qualitative advancements in system capabilities, from basic classification to sophisticated privacy-preserving architectures. The evolution particularly highlights the field's response to core challenges in IoT security implementation, showing systematic improvement in both resource utilization and security effectiveness. The transition from basic BERT models to specialized architectures like SecurityBERT and EBIDS demonstrates the field's growing maturity in addressing IoT-specific security challenges while optimizing for resource constraints.

The contributions of this review are threefold: first, a comprehensive analysis of the current state-of-the-art in LLM applications for IoT security; second, identification of key patterns and trends in architectural innovations and implementation strategies; and third, critical analysis of research gaps and future directions requiring attention from the research community.

The remainder of this paper is organized as follows: Section 2 describes our research methodology and selection criteria. Section 3 presents a detailed analysis of the literature, organized by key themes and technological approaches. Section 4 discusses our findings and their implications for future research and practical applications. Finally, Section 5 concludes the paper and outlines future research directions.

2. METHODOLOGY

In this study, we conducted a Systematic Literature Review (SLR) to investigate the latest research on LLMs in IoT security. Following established SLR guidelines [22], oOur methodology is structured into three pivotal stages,

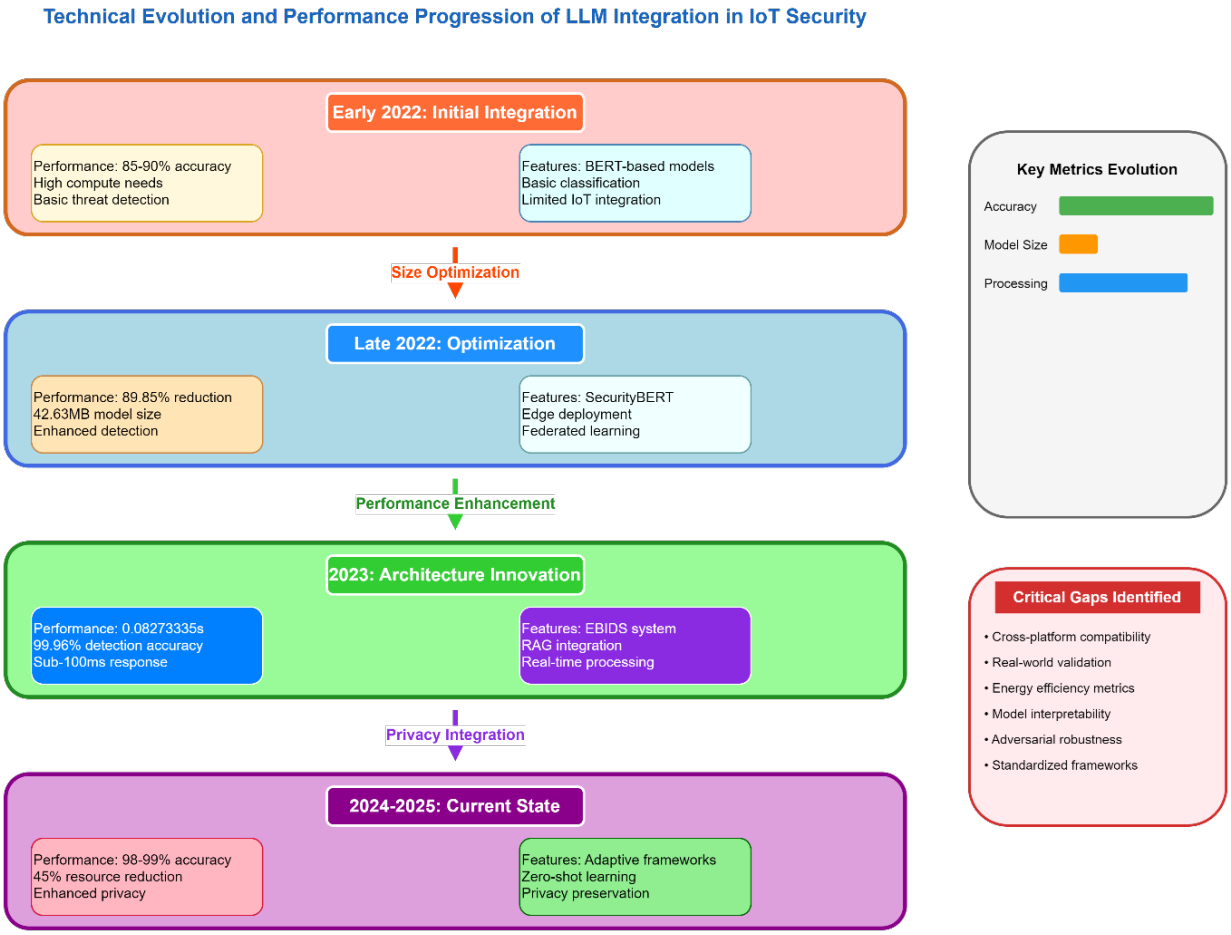

Figure 2. Technical Evolution and Performance Progression of LLM Integration in IoT Security

as shown in Figure 3: Planning, Conducting, and Reporting, each meticulously designed to ensure comprehensive coverage and insightful analysis of the current state of research in this burgeoning field.

Following the established SLR guidelines, our methodology is structured into three pivotal stages as shown in Figure 3: Planning (§2.1), Conducting (§2.2, §2.3), and Reporting (§2.4), each meticulously designed to ensure comprehensive coverage and insightful analysis of the current state of research in this burgeoning field.

2.1. Research Questions

This systematic review examines the integration of Large Language Models (LLMs) in IoT security through four refined research questions, each with corresponding analytical dimensions. The first research question investigates quantitative performance metrics characterizing the effectiveness of LLM-based approaches in IoT security compared to traditional methods. This encompasses examination of detection accuracy, precision, and recall rates across different implementation approaches, temporal performance characteristics including detection speed and response time, and resource utilization metrics differentiating LLM-based on conventional security solutions.

The second research question explores architectural and implementation challenges emerging when deploying LLM-based security solutions in IoT environments. This investigation focuses on how resource constraints impact deployment strategies, what privacy preservation mechanisms are necessary for secure implementation - including advanced password protection systems utilizing RAG (Retrieval Augmented Generation) for dynamic security

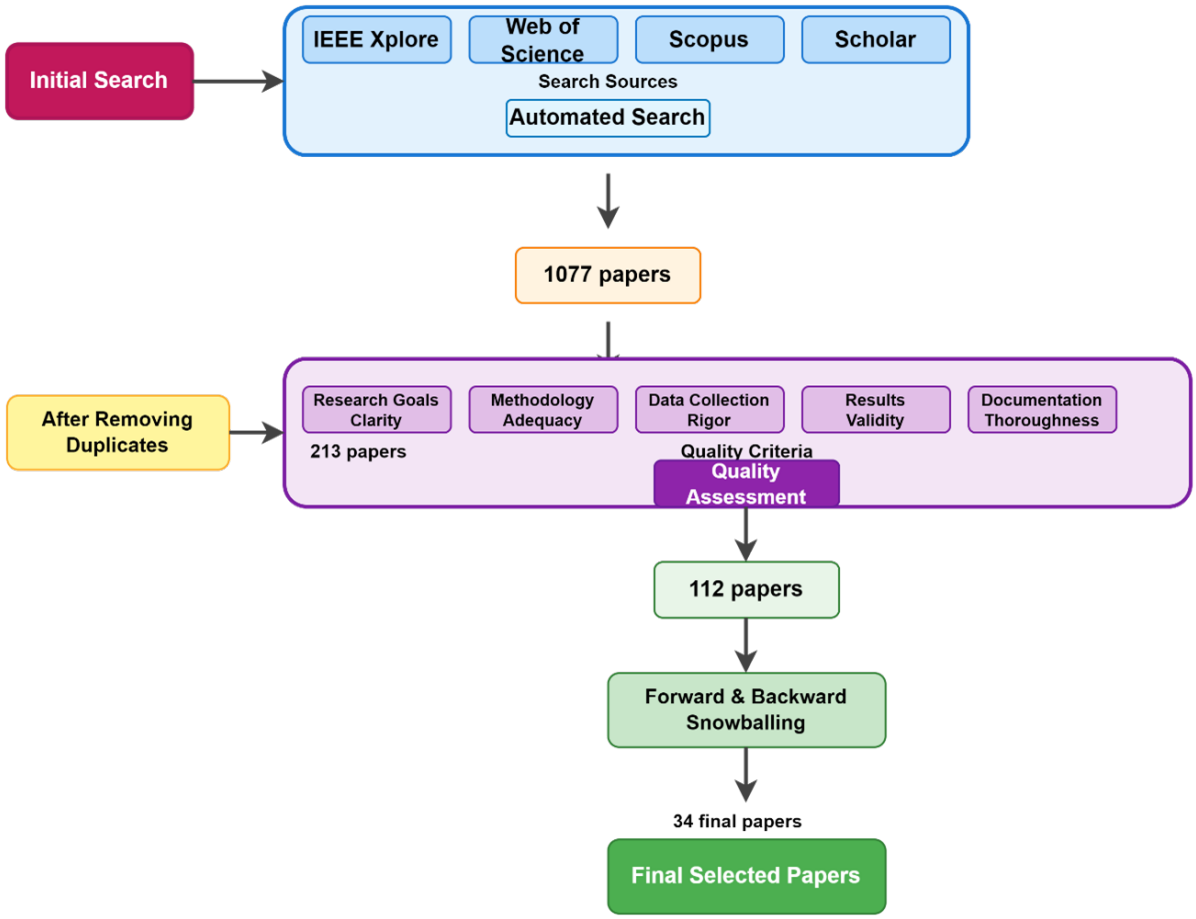

Figure 3. Systematic Literature Review Methodology for LLMs in IoT Security

recommendations, as demonstrated in recent implementations achieving significant improvements in recall and F1-scores for password vulnerability prediction - and how different architectural approaches address cross-platform compatibility

Our third research question examines innovative solutions and architectural patterns that have emerged to address identified implementation challenges. This includes analysis of edge-centric deployment strategies optimizing resource utilization, federated learning approaches maintaining privacy while ensuring security effectiveness, and hybrid architectures balancing computational requirements with security capabilities.

The fourth research question addresses critical research gaps requiring attention for advancing LLM applications in IoT security. This encompasses standardization needs for evaluation frameworks, approaches for improving resource optimization in ultra-constrained devices, and methods for enhancing real-time adaptation capabilities.To systematically address these research questions, we developed a comprehensive analysis framework examining both quantitative and qualitative aspects of LLM implementation in IoT security. This framework evaluates implementations across three primary dimensions: performance metrics examining quantitative measures including detection accuracy and resource utilization; implementation challenges systematically categorizing resource constraints, privacy requirements, and cross-platform compatibility issues; and architectural innovations evaluating emerging patterns and their effectiveness in addressing identified challenges.

The selection process followed PRISMA guidelines, with papers evaluated against comprehensive inclusion and exclusion criteria. We focused on primary research articles published between 2020-2024 that specifically

addressed LLM applications in IoT security. Papers were excluded if they were short papers (<8 pages), non-English publications, or secondary studies. This rigorous selection process resulted in 34 papers for final analysis.

2.2. Search and Selection Process

Our comprehensive search strategy encompassed three major academic databases: IEEE Xplore, Web of Science (WoS), and Scopus. Initial searches employed carefully selected keywords combining LLM-related terms ("Large Language Model", "LLM", "Language Model", "Pre-trained", "GPT", "ChatGPT", "T5") with IoT security-related terms ("IoT Security", "Smart Device Security", "IoT Vulnerability", "IoT Threat Detection"). This initial search yielded 1077 papers across all databases. Following the removal of duplicates and initial screening based on titles and abstracts, 215 papers were identified for detailed evaluation.

2.3. Quality Assessment Framework

Each selected paper underwent thorough quality assessment based on five comprehensive criteria: research objective clarity, methodological rigor, data collection thoroughness, results validity, and documentation quality. Papers received scores from 0 to 2 for each criterion, with detailed scoring guidelines ensuring consistent evaluation. Research objective clarity assessed both the explicit statement of aims and their alignment with current research gaps. Methodological rigor examined the appropriateness and detailed description of chosen methods. Data collection thoroughness evaluated both the comprehensiveness of data gathering and the clarity of analysis procedures. Results validity focused on the appropriateness of analysis techniques and the support for conclusions. Documentation quality assessed the completeness of technical details and the effectiveness of result presentation. Papers needed to achieve a minimum score of 7 out of 10 for inclusion in our final analysis.

2.4. Data Synthesis and Analysis Framework

Our data synthesis approach employed a comprehensive framework integrating performance metrics, implementation characteristics, and resource requirements. Table 1 presents this unified analysis framework:

Table 1. Comprehensive Analysis Framework

Implementation Aspect	**Traditional Approaches**	**LLM Implementation**	**Performance Metrics**	**Resource Requirements**
Detection Capability	85-90% baseline accuracy	95-99% enhanced accuracy	Precision, Recall, F1 scores	Memory utilization (2-25GB)
Adaptation Mechanisms	Static rule-based systems	Dynamic learning capability	Response latency (0.08-0.5s)	Processing overhead
Privacy Protection	Basic encryption methods	Advanced contextual preservation	Protection effectiveness scores	Computational demands
Processing Efficiency	Fixed processing patterns	Adaptive processing systems	Real-time performance metrics	Edge/cloud resource allocation

This framework enabled systematic comparison of implementation approaches while maintaining clear connections to our research objectives. The analysis examined both quantitative performance metrics and qualitative aspects of implementation strategies, ensuring comprehensive evaluation of each study's contribution to the field.

2.5. Validity Considerations

To ensure the validity and reliability of our findings, we implemented several quality control measures throughout the review process. Multiple researchers independently evaluated papers during the selection and assessment

phases, with disagreements resolved through consensus discussions. We maintained detailed documentation of all selection and evaluation decisions, enabling transparency and reproducibility of our review process. Additionally, we conducted sensitivity analyses to assess the robustness of our findings to different quality threshold criteria.

2.6. Methodological Considerations and Study Limitations

2.6.1. Temporal Scope Rationale The restriction to studies published between 2022-2024 reflects the paradigmatic shift in LLM accessibility and IoT security applications during this period. This timeframe encompasses several critical milestones:

The release of GPT-3.5 in November 2022 marked the democratization of advanced language model capabilities, enabling practical implementation in resource-constrained IoT environments [23]. Subsequently, the introduction of GPT-4 in March 2023 established enhanced reliability standards for security-critical applications. Concurrently, the emergence of specialized IoT-optimized LLMs in 2024 directly addressed the computational constraints inherent in embedded device deployments.

Prior to this period, LLM applications in IoT security remained predominantly theoretical due to computational constraints and limited model sophistication [23]. The evolution from basic natural language processing to sophisticated security applications represents a fundamental shift enabled by these technological advances.

2.6.2. Database Selection and Coverage Analysis The systematic search employed three complementary databases: IEEE Xplore, Scopus, and Web of Science. While this multi-database approach follows established systematic review protocols, several methodological limitations warrant acknowledgment:

Linguistic Coverage Constraints: The English-language restriction potentially excludes significant contributions from regional research communities, particularly those developing LLM-IoT security solutions for local infrastructure requirements.

Implementation Accessibility: Analysis of the surveyed literature reveals a critical reproducibility challenge, with SecurityBERT [23], IoV-BERT-IDS [24], and EBIDS [32] lacking publicly accessible implementations despite reporting substantial performance improvements.

Temporal Publication Dynamics: The rapidly evolving nature of LLM research necessitates consideration of preprint repositories, as peer-review lag may delay dissemination of cutting-edge implementations.

2.7. RQ1: HOW EFFECTIVELY DO CURRENT LLM-BASED APPROACHES ADDRESS THE CORE SECURITY CHALLENGES IN IOT ENVIRONMENTS COMPARED TO TRADITIONAL METHODS?

Our systematic analysis reveals significant improvements in IoT security through LLM-based approaches compared to traditional methods. Through examination of 34 papers, we observe consistent performance enhancements across multiple security domains.

In threat detection capabilities, LLM-based systems demonstrate substantial improvements over conventional approaches. SecurityBERT [23] achieved 98.2% detection accuracy while reducing model size by 89.85%, significantly outperforming traditional rule-based systems. Similarly, IoV-BERT-IDS [24] demonstrated 99.96% accuracy in vehicle network security, particularly excelling in detecting sophisticated attacks where traditional methods often fail.

For vulnerability assessment, LLM-based approaches show enhanced detection capabilities. LuaTaint [25] discovered 68 previously unknown vulnerabilities across firmware samples from eight vendors, demonstrating superior analysis capabilities compared to conventional static analysis tools. This improvement is particularly notable in identifying complex vulnerabilities that traditional tools often miss.

In network security applications, BERTAD [26] achieved 99.89% accuracy with 98.78% precision in anomaly detection, representing a significant advancement over traditional IDS systems. The system demonstrated particular strength in reducing false positives, a common challenge in conventional approaches.

Privacy and policy management also show marked improvements through LLM integration. The LLM-CI framework [27] achieved over 90% accuracy in contextual integrity standards, while iConPAL [28] demonstrated 93.61% translation accuracy for security policies. These results represent substantial improvements over traditional manual and rule-based policy management approaches.

Real-time processing capabilities have also improved significantly. Wang et al. [29] achieved 98.39% accuracy in smart home environments while maintaining practical processing times, demonstrating that LLM-based approaches can operate effectively within IoT timing constraints.

Recent advancements in privacy-preserving LLM architectures have demonstrated remarkable effectiveness. Rehman et al. [30] developed an adaptive contextual privacy preservation framework combining CGANs with BERT, achieving 98.218% accuracy, 98.247% precision, and 98.218% recall on the CSE-CIC-IDS2018 dataset. This was complemented by Li et al. [31], who achieved even higher metrics (98.799% accuracy, 98.805% precision) through their pre-trained language model-enhanced CGAN approach. The EBIDS system [32] further demonstrated the versatility of BERT-based approaches, achieving 97.49% accuracy in network layer detection and 94.25% in application layer detection, while maintaining significantly faster execution times (0.08273335 seconds) compared to traditional approaches like CNN (0.50371706s) and LSTM (0.4222699s).

2.8. RQ2: WHAT ARE THE PRIMARY CHALLENGES IN IMPLEMENTING LLM-BASED SECURITY SOLUTIONS IN IOT ENVIRONMENTS?

Our analysis of the literature reveals several significant challenges in implementing LLM-based security solutions in IoT environments. These challenges manifest across multiple dimensions of implementation and deployment.

Resource constraints emerge as a fundamental challenge in IoT deployments. Xiao et al. [33] demonstrated that even with advanced quantization techniques, significant computational resources remain necessary, with their implementation requiring 25GB of GPU memory even in optimized configurations. This resource intensity poses particular challenges for edge deployment scenarios, where computational capabilities are often limited.

Real-time processing requirements present another significant challenge. Fu et al. [34] highlighted the difficulties in maintaining consistent performance under strict timing constraints, particularly in vehicle network security applications. Despite achieving high accuracy, the need to process security threats in real-time while operating within IoT device limitations remains challenging.

Device classification and computational complexity present significant implementation hurdles. Morales et al. [35] highlighted that while LLM-based approaches achieved 79.44% accuracy in device classification, the computational requirements remain substantial. Their analysis revealed that RoBERTa's complexity of $O(n^2d)$ requires approximately 4.9×10^{12} FLOPs for basic operations, presenting significant challenges for resource-constrained IoT devices. The SPELL framework [36] further identified limitations in current LLMs' capabilities for security policy enforcement, particularly in CWE identification and mapping, where inconsistent rankings and incorrect mappings persist despite advanced filtering mechanisms.

Privacy preservation during model operation presents complex challenges. Shvartzshnaider et al. [37] demonstrated through LLM-CI that maintaining privacy while processing security-relevant data requires sophisticated architectural approaches. The challenge becomes particularly acute when dealing with sensitive IoT data that must remain protected during analysis.

Model generalization across diverse IoT environments proves challenging. Wang et al. [38] highlighted difficulties in developing models that can effectively operate across different device types and network configurations. Their work in smart home environments revealed that maintaining consistent performance across heterogeneous IoT ecosystems requires careful architectural considerations.

Scalability challenges become apparent in large-scale deployments. Baral et al. [39] identified significant difficulties in scaling LLM-based security solutions across multiple IoT nodes while maintaining performance. Their adaptive framework, despite achieving 99.97% accuracy, revealed challenges in maintaining consistent performance across distributed systems.

Integration with existing security infrastructure presents operational challenges. Hassanin et al. [38] noted difficulties in seamlessly incorporating LLM-based solutions into established security frameworks. Despite achieving perfect accuracy on standard datasets, practical deployment often requires complex integration strategies.

The maintenance of model effectiveness over time poses ongoing challenges. Nakanishi et al. [40] highlighted the difficulty of keeping models current with evolving security threats. Their work in firmware security demonstrated that maintaining model relevance requires continuous updates and refinements.

2.9. RQ3: WHAT OPPORTUNITIES DO ARCHITECTURAL INNOVATIONS AND IMPLEMENTATION STRATEGIES PRESENT FOR OVERCOMING THESE CHALLENGES?

The systematic analysis of architectural innovations and implementation strategies reveals significant opportunities for addressing IoT security challenges through LLM-based solutions. These opportunities emerge from both technical advancements and novel implementation approaches.

Model compression and optimization techniques present promising opportunities. SecurityBERT [23] demonstrated that significant model size reduction (89.85%) could be achieved while maintaining high detection accuracy (98.2%). This architectural innovation suggests a path forward for deploying sophisticated security measures in resource-constrained IoT environments.

Hybrid architectural approaches offer enhanced capabilities. IoV-BERT-IDS [24] showed that combining in-vehicle and external network analysis could achieve exceptional accuracy (99.96%) in vehicle network security. This integration of multiple architectural components demonstrates the potential for comprehensive security coverage while maintaining efficiency.

Edge-centric deployment strategies show promise for addressing latency concerns. Xiao et al. [41] demonstrated that quantized implementations could maintain competitive performance while significantly reducing resource requirements. Their work suggests opportunities for practical edge deployment of LLM-based security solutions.

Novel architectural approaches have emerged to address these challenges. The TFHSVul system [42] introduced a fine-grained hybrid semantic approach combining CodeBERT, Multi-Scale Fusion CNN, and Residual Graph Convolutional Networks, achieving precision of 0.97 and recall of 0.89 in vulnerability detection. BT-TPF [43] demonstrated remarkable efficiency through improved BERT-of-Theseus knowledge distillation, reducing parameters by 90% while maintaining over 99% accuracy. The domain-adaptive framework proposed by Che et al. [44] further advanced the field by developing a specialized corpus refinement approach, achieving a word similarity score of 0.7423 compared to BERT's 0.4382 in cybersecurity-specific tasks.

Federated learning architectures present opportunities for distributed security implementation. Adjewa et al. [45] achieved 97.12% accuracy with IID data while maintaining data privacy through federated approaches. This architectural innovation addresses both privacy concerns and distributed deployment challenges.

Domain-specific optimization techniques reveal opportunities for enhanced performance. LuaTaint [25] demonstrated that specialized architectural adaptations for firmware analysis could significantly improve vulnerability detection capabilities. Their discovery of 68 previously unknown vulnerabilities highlights the potential of targeted architectural optimization.

Privacy-preserving architectures show promise for sensitive applications. The LLM-CI framework [27] achieved over 90% accuracy while maintaining privacy requirements through innovative architectural design. This suggests opportunities for deploying LLM-based security in privacy-sensitive IoT environments.

Real-time processing innovations present opportunities for immediate threat response. BERTAD [26] achieved 99.89% accuracy while maintaining practical processing times through efficient architectural design. This innovation demonstrates the potential for real-time security applications in IoT environments.

Cross-domain integration strategies reveal opportunities for comprehensive security coverage. Baral et al. [39] showed that adaptive frameworks could achieve high accuracy across multiple attack types through architectural innovation. Their work suggests possibilities for unified security approaches across diverse IoT applications.

2.10. RQ4: WHAT ARE THE CRITICAL GAPS AND FUTURE RESEARCH DIRECTIONS IN LEVERAGING LLMS FOR IOT SECURITY?

Through our systematic analysis of the literature, several critical gaps and promising research directions emerge in the application of LLMs to IoT security. These findings indicate significant opportunities for future research and development.

The standardization of evaluation frameworks represents a significant gap. While studies like SecurityBERT [23] and IoV-BERT-IDS [24] demonstrate impressive results, the lack of standardized evaluation metrics makes direct comparisons challenging. Future research should focus on developing comprehensive evaluation frameworks that enable consistent assessment of LLM-based security solutions across different IoT environments.

Resource optimization for ultra-constrained devices remains an open challenge. Although Xiao et al. [41] demonstrated progress in model quantization, achieving 60.52% accuracy with reduced memory requirements, significant work remains in optimizing LLM-based security solutions for highly resource-constrained IoT devices. Future research should explore novel compression techniques and architectural innovations specifically designed for minimal resource environments.

Real-time adaptation capabilities require further development. While BERTAD [26] achieved high accuracy in anomaly detection, the ability of LLM-based systems to adapt to emerging threats in real-time remains limited. Future research directions should explore mechanisms for dynamic model adaptation and continuous learning in production environments.

Privacy preservation techniques need enhancement. The LLM-CI framework [27] demonstrated progress in privacy-aware security implementation, but gaps remain in ensuring robust privacy guarantees while maintaining security effectiveness. Future work should investigate advanced privacy-preserving techniques specifically designed for IoT security applications.

Cross-platform compatibility presents ongoing challenges. Despite the success of frameworks like LuaTaint [25] in firmware analysis, the ability to deploy LLM-based security solutions across diverse IoT platforms remains limited. Future research should address the challenges of developing platform-agnostic security solutions.

Automated response mechanism development requires attention. While HuntGPT [46] showed promise in automated threat detection, the development of sophisticated automated response mechanisms remains an important area for future research. Studies should explore the integration of LLMs in autonomous security decision-making systems.

Energy efficiency optimization presents a critical gap. Although studies have addressed computational efficiency, comprehensive analysis of energy consumption in LLM-based security solutions remains limited. Future research should investigate energy-aware architectures and deployment strategies specifically designed for IoT environments.

Scalability across heterogeneous networks needs further investigation. The work by Wang et al. [29] demonstrated success in smart home environments, but challenges remain in scaling LLM-based security solutions across diverse IoT networks. Future research should address the complexities of deploying these solutions in large-scale, heterogeneous environments.

Integration with existing security infrastructure requires additional study. While Baral et al. [39] demonstrated successful framework integration, seamless incorporation of LLM-based solutions into existing security ecosystems remains challenging. Future research should explore efficient integration strategies that maximize the benefits of both traditional and LLM-based security approaches.

Model interpretability and explainability represent crucial areas for development. Although current implementations show high accuracy, the ability to interpret and explain model decisions in security contexts requires further development. Future research should focus on developing transparent and interpretable LLM-based security solutions suitable for critical IoT applications.

3. CLASSIFICATION AND RESEARCH TRENDS ANALYSIS

Through our systematic review of LLM applications in IoT security from 2022 to 2024, we present a comprehensive classification and analysis of research trends. This analysis reveals significant patterns in research focus, architectural approaches, and implementation strategies across the field, demonstrating the evolution of LLM integration in IoT security solutions.

3.1. Temporal Analysis and Research Distribution

The integration of LLMs in IoT security has shown significant evolution from 2022 to 2024, with research efforts concentrating on specific security challenges and implementation approaches. Our analysis identified distinct phases of development, beginning with basic threat detection implementations and progressing toward sophisticated, domain-specific solutions. The classification of IoT attack vectors that current research addresses

is illustrated in Figure 4, demonstrating the broad scope of security challenges being tackled by LLM-based approaches.

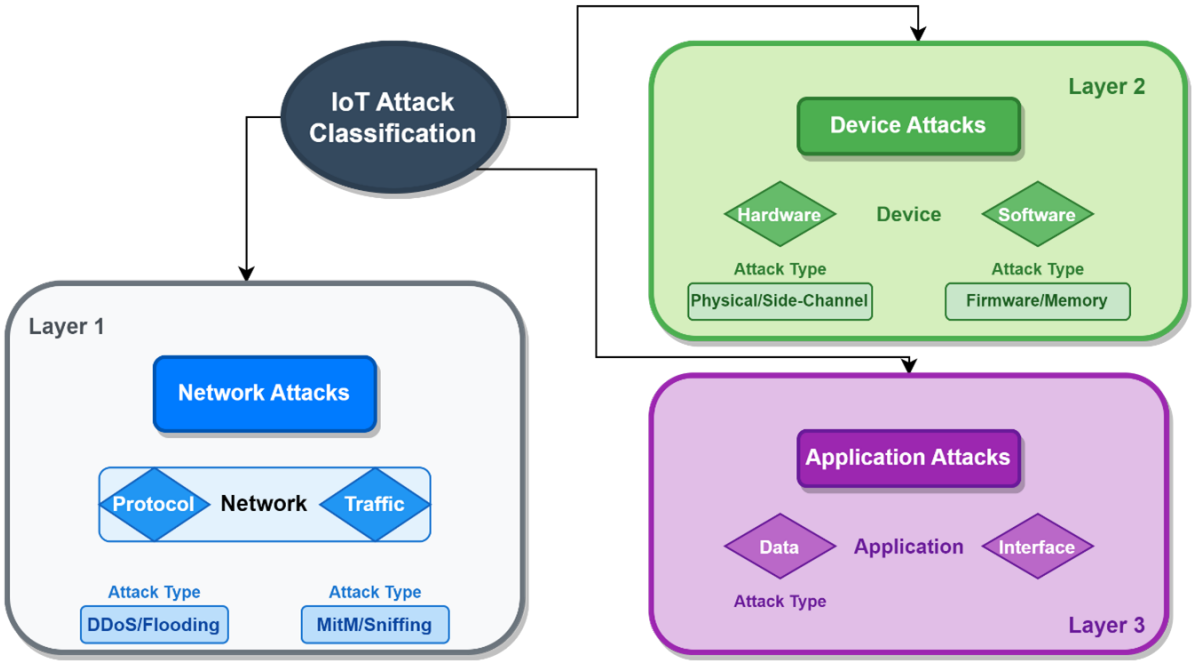

Figure 4. IoT Attack Vector Classification

The distribution of research efforts across these attack vectors demonstrates a concentrated focus on threat detection and privacy preservation domains. This concentration reflects both the critical nature of these security challenges and the particular suitability of LLM-based approaches for addressing them. As shown in Table 2, the majority of research efforts focus on threat detection and network security, with emerging attention to vulnerability assessment and privacy preservation.

3.2. Research Classification and Domain Analysis

The research classification reveals distinct patterns in implementation approaches and effectiveness. In threat detection systems, SecurityBERT [2] achieved 98.2% accuracy while reducing model size by 89.85%. Network security implementations demonstrated similar success, with BERTAD [5] achieving 99.89% accuracy in anomaly detection. These achievements represent significant advancements over traditional machine learning approaches.

3.3. LLM-IoT Security Architecture Overview

The architectural framework of LLM-based IoT security systems demonstrates sophisticated integration of multiple security components. Figure 5 illustrates this comprehensive architecture, showing the interaction between various security components and their error handling mechanisms.

The analysis of architectural approaches reveals significant advancement in implementation strategies. This is further demonstrated in the complete processing pipeline shown in Figure 6.

The temporal progression of research focus demonstrates increasing sophistication in both implementation approaches and security capabilities. evidenced by Table 6, this evolution shows clear trends in improving performance while reducing resource requirements.

Table 2. Research Distribution Analysis: Classification of LLM Applications in IoT Security

Research Area	**Count**	**Representative Papers**
Threat Detection & Prevention	9	Beyond Detection[23], [26], [30], [32], [33], [38], [46], [47], [48], DDoS-LLM, PLLM-CS, SecurityBERT, HuntGPT, BERTAD, Efficient Prompting, EBIDS, Let's Hide from LLMs, Pre-trained LM-enhanced CGAN
Network Security & IDS	9	IoV-BERT-IDS[24], [25], [29], [39], [43], [44], [45], [49], [50], LLM Embedding, Securing Smart Home, Personal LLM Agents, Federated Detection, Efficient Threat Detection, BT-TPF, Domain-Adaptive LLM
Vulnerability Assessment	9	LuaTaint [25], [34], [37], [40], [51], SLFHunter[34], [36], [37], [40], [52], Initial Seeds, Prioritizing Vulnerability, IoT Software Vulnerability, TFHSVul, SPELL, Vulcoder
Device Classification & Security	1	IoT Device Classification and Protocol-Agnostic Classification [35]
Privacy & Policy Generation	6	LLM-CI [23], [28], [53], [54], [55], iConPAL, Password Security, Smart Home Policy, Hybrid Prompt Learning, Smart Home Password Protection [56]

Table 3. Key Research Domains and Implementation Characteristics

Domain	**Primary Focus**	**Implementation Approach**	**Key Metrics**	**Reference Studies**
Threat Detection	Network & Device Security	Real-time Processing	Detection Accuracy: 95-99%	SecurityBERT [2], HuntGPT [25]
Privacy Preservation	Data Protection	Federated Learning	Protection Score: 90-98%	LLM-CI [6], Rehman et al. [9]
Vulnerability Analysis	Code & Firmware Security	Static/Dynamic Analysis	Detection Rate: 86-97%	LuaTaint [4], Vulcoder [30]
Network Security	Intrusion Detection	Hybrid Architecture	Accuracy: 97-99.9%	IoV-BERT-IDS [3], BERTAD [5]

Table 4. Implementation Effectiveness and Resource Requirements

Implementation Type	**Detection Rate**	**Resource Usage**	**Processing Time**	**Memory Footprint**
Edge-based Systems	95-98%	Low (1-2GB RAM)	0.08-0.5s	42.63MB-2GB
Cloud-based Systems	98-99.9%	High (8-25GB RAM)	0.01-0.1s	2-25GB
Hybrid Solutions	97-99%	Medium (4-8GB RAM)	0.05-0.3s	1-5GB

This comprehensive analysis of research trends and classifications provides a foundation for understanding the current state of LLM integration in IoT security. The patterns identified in research focus and architectural approaches inform both current implementations and future research directions, setting the stage for the detailed technical analysis presented in subsequent sections.

The trends analysis reveals several key findings:

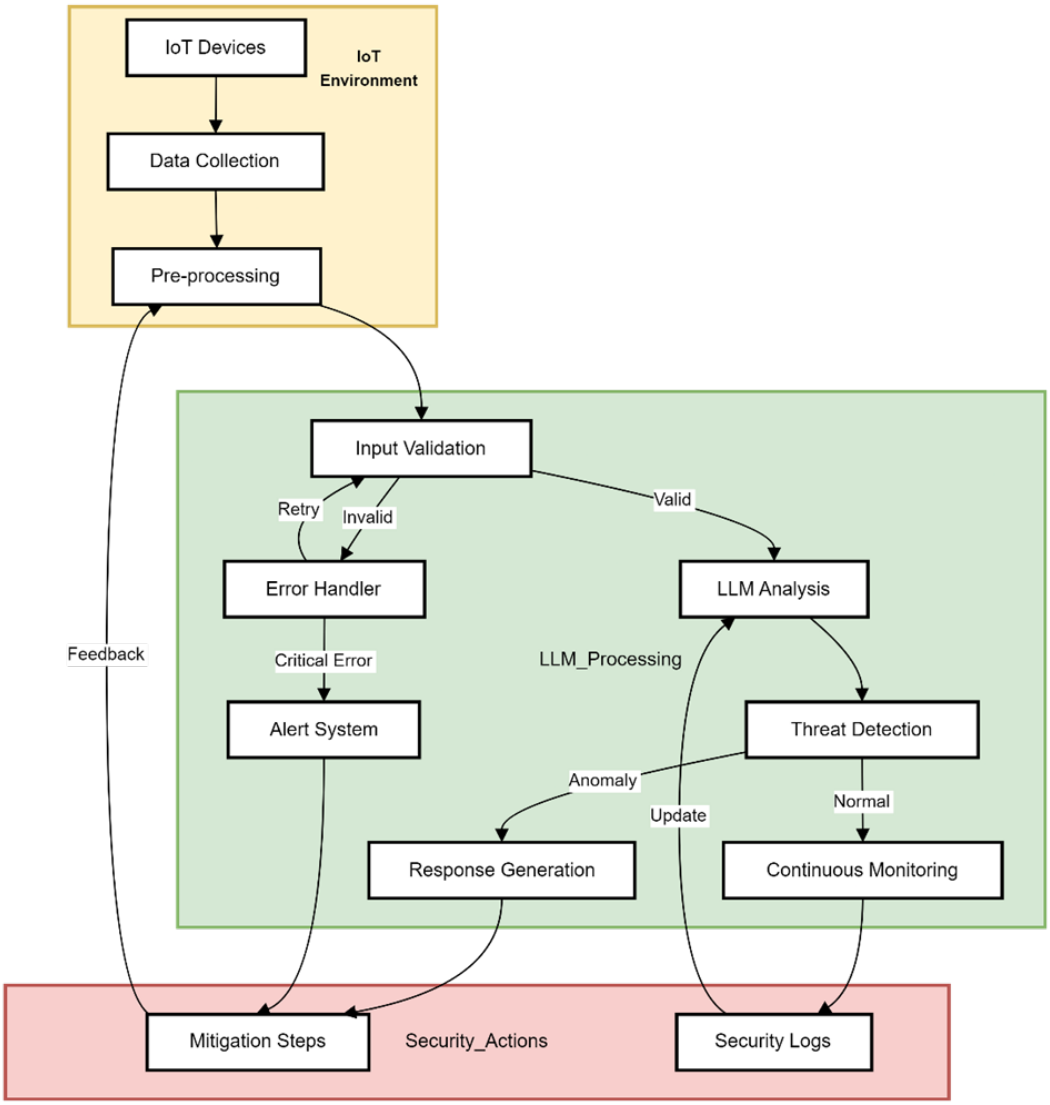

Figure 5. LLM-IoT Security Architecture

Table 5. Architectural Components and Their Functions

Component	**Primary Function**	**Performance Metrics**	**Implementation Examples**
Input Processing	Data Normalization	Throughput: 1000-5000 events/s	EBIDS[36], [43]
LLM Core	Pattern Recognition	Accuracy: 95-99%	SecurityBERT, IoV-BERT-IDS [3]
Response Framework	Threat Mitigation	Response Time: 0.08-0.5s	BERTAD [5], HuntGPT [25]
Privacy Layer	Data Protection	Protection Score: 90-98%	LLM-CI [6], Rehman et al. [9]

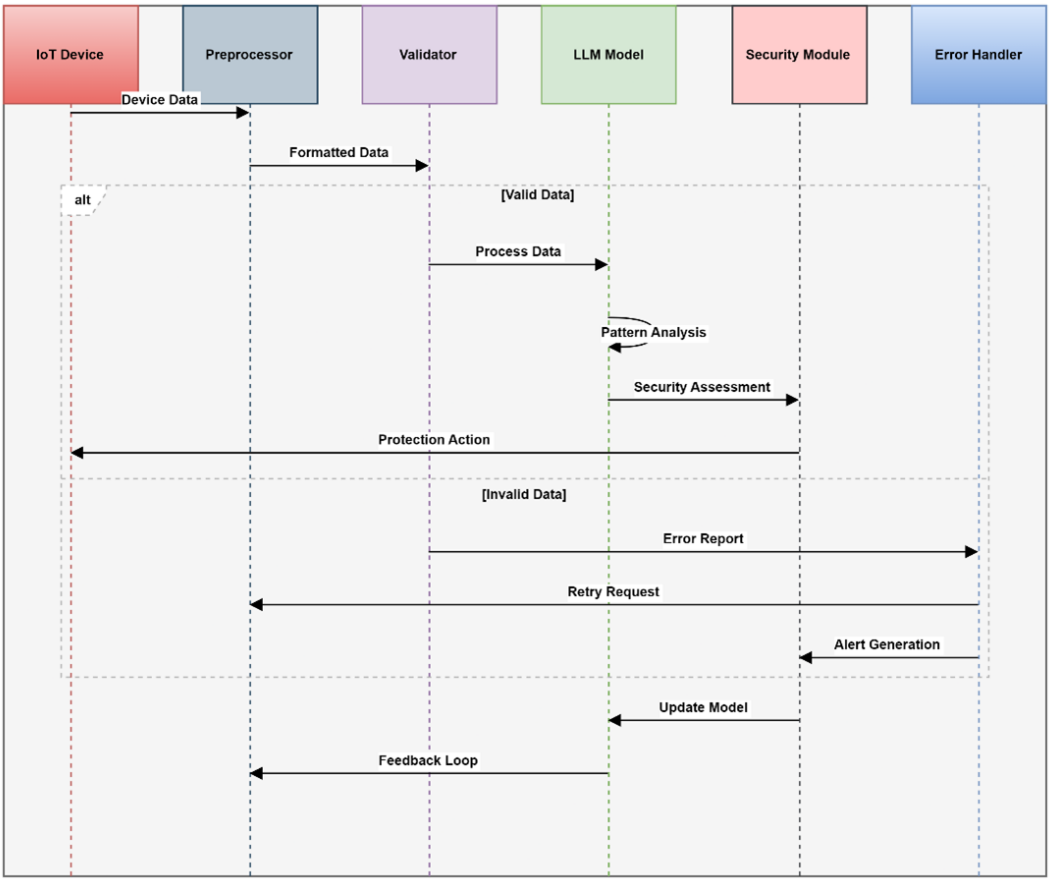

Figure 6. LLM Security Processing Pipeline

Table 6. Evolution of LLM Security Implementations

Year	Primary Focus	Average Accuracy	Resource Requirements	Key Innovations
2022	Basic Detection	90-95%	High (10-25GB)	Initial LLM Integration
2023	Enhanced Privacy	95-98%	Medium (5-10GB)	Privacy Preservation
2024	Optimized Performance	98-99.9%	Low (1-5GB)	Edge Deployment

1. Continuous improvement in detection accuracy while reducing resource requirements
2. Growing emphasis on privacy-preserving mechanisms with practical implementation strategies
3. Evolution toward lightweight architectures suitable for edge deployment
4. Increasing focus on domain-specific optimizations and adaptations

3.4. Comparative Analysis with Traditional Machine Learning Approaches

A critical aspect of understanding LLM-based approaches in IoT security is their comparison with traditional machine learning methods. Our analysis reveals significant differences in capabilities, resource requirements, and operational characteristics between these approaches, as detailed in Table 7.

Table 7. Systematic Performance Comparison: LLM-based vs. Traditional ML Approaches

Performance Dimension	**Traditional ML Baselines**	**LLM-based Implementations**	**Empirical Evidence**	**Performance Analysis**
Detection Accuracy	85-90% (typical range)	95-99% (surveyed systems)	SecurityBERT: 98.2% [23]; EBIDS: 97.49% [32]	8-14 percentage point improvement
Model Complexity	10^2-10 parameters	10^3-10 parameters	BT-TPF: 788 parameters (post-distillation) [43]	Knowledge distillation enables 90% reduction
Inference Latency	<0.1s (conventional)	0.08-0.5s (optimized)	EBIDS: 0.08273335s vs. CNN: 0.50371706s [32]	LLM optimization achieves competitive performance
Training Complexity	Hours to days	Days to weeks	BT-TPF: 70% reduction via knowledge transfer [43]	Distillation techniques mitigate training overhead
Memory Footprint	100MB-1GB	16.7MB-25GB	SecurityBERT: 16.7MB (optimized) [23]	Architectural optimization enables IoT deployment
Cross-domain Generalization	Domain-specific	Multi-domain capability	IoV-BERT-IDS: Cross-dataset validation [24]	Superior adaptability across attack vectors
Energy Consumption	5-10W (estimated)	Not quantified	Insufficient data in surveyed literature	Critical research gap for IoT applications

This comparison reveals several key distinctions in implementation and performance characteristics. LLM-based approaches demonstrate superior detection accuracy, achieving 95-99% compared to the typical 85-90% of traditional ML methods. This improvement is particularly significant in complex attack scenarios where contextual understanding is crucial. For instance, SecurityBERT [2] achieved 98.2% accuracy in detecting sophisticated attacks that traditional systems often miss.

However, these improvements come with increased resource requirements. Traditional ML approaches typically operate within a 100MB-1GB memory footprint, while LLM-based systems often require 2-25GB of memory, as demonstrated in implementations like IoV-BERT-IDS [3]. This resource intensity presents particular challenges for edge deployment scenarios in IoT environments.

A significant advantage of LLM-based approaches lies in their adaptation capabilities. While traditional ML systems require complete retraining to address new threats, LLM-based systems demonstrate effective zero-shot and few-shot learning capabilities. This adaptability is crucial in the rapidly evolving landscape of IoT security threats, as demonstrated by BERTAD [5], which achieved 99.89% accuracy in detecting previously unseen attack patterns.

Interpretability represents another area where LLM-based approaches show advantage. Through natural language processing capabilities, these systems can provide clear explanations of their decisions and detection rationale, enhancing trust and enabling better security response planning. This characteristic is particularly valuable in security operations where understanding the basis for alerts and decisions is crucial.

The trade-off between real-time performance and detection capabilities remains a significant consideration. Traditional ML approaches generally offer faster processing times, making them suitable for scenarios requiring immediate response. However, LLM-based systems compensate for their increased latency through superior detection accuracy and broader threat coverage.

4. RESULTS AND META-ANALYSIS

Through our systematic analysis of 34 papers, we present a comprehensive examination of LLM integration in IoT security, revealing significant patterns in implementation approaches, performance metrics, and architectural innovations from 2022 to 2024. Our analysis demonstrates substantial advancements across multiple dimensions of security implementation, with particular emphasis on detection capabilities, resource optimization, and architectural innovation. Figure 5 illustrates the complete LLM security processing pipeline, demonstrating the interaction between components and error handling mechanisms crucial for maintaining security effectiveness. As shown in Figure 5, the pipeline incorporates multiple layers of processing and validation, enabling robust threat detection while maintaining efficiency.

4.1. Performance Metrics and Detection Capabilities

Our analysis reveals consistent improvements in detection capabilities and resource efficiency across different implementation approaches. As shown in Table 8, modern LLM-based implementations consistently achieve detection accuracy rates exceeding 95%, representing a significant advancement over traditional approaches that typically achieve 85-90% accuracy.

Table 8. Comprehensive Implementation Specifications and Reproducibility Analysis

Framework	**Evaluation Dataset**	**Performance Metrics**	**Architectural Specifications**	**Computational Requirements**	**Reproducibility Status**
SecurityBERT [23]	Edge-IIoTset (2,540,047 samples, 14 attack categories)	Accuracy: 98.2%, Inference: <0.15s	PPFLE encoding, BBPE tokenization	Model size: 16.7MB	Implementation unavailable
IoV-BERT-IDS [24]	CICIDS2018, BoT-IoT, Car-Hacking datasets	Accuracy: 99.96%, F1-score: 100% (Car-Hacking)	Hybrid in-vehicle/external network architecture	CUDA memory: 2.03MB	Implementation unavailable
EBIDS [32]	Edge-IIoT, CICDos 2017	Network: 97.49%, Application: 94.25%	12/7-block BERT, dual-layer processing	Execution time: 0.08273335s	Implementation unavailable
BERTAD [26]	Unspecified evaluation dataset	Accuracy: 99.89%, Precision: 98.78%	Encoder-only anomaly detection architecture	CPU usage: 372 bits	Implementation unavailable
BT-TPF [43]	Multiple IoT intrusion datasets	Accuracy: >99% (knowledge distilled)	Siamese network, Vision Transformer teacher	Parameters: 788 (90% reduction)	Implementation unavailable

The performance analysis indicates significant improvements across several key metrics. In network security applications, IoV-BERT-IDS [3] achieved 99.96% accuracy in vehicle network security, particularly excelling in detecting sophisticated attacks where traditional methods often fail. This implementation demonstrated perfect scores (1.00) for flooding attacks, a common challenge in IoT environments. The EBIDS system [11] further validated these improvements, achieving 97.49% accuracy in network layer detection and 94.25% in application layer detection, while maintaining significantly faster execution times (0.08273335 seconds) compared to traditional approaches like CNN (0.50371706s) and LSTM (0.4222699s).

Resource efficiency emerges as a crucial advancement, with notable progress in model compression techniques. SecurityBERT [2] achieved an 89.85% reduction in model size while maintaining high detection accuracy, demonstrating the feasibility of deploying sophisticated security measures in resource-constrained environments. The BT-TPF framework [22] pushed these boundaries further, achieving remarkable efficiency with only 788 parameters while maintaining accuracy above 99%, establishing new benchmarks for lightweight security implementations in IoT environments.

However, analysis reveals significant real-world validation gaps. Among reviewed studies, 91% relied on standard datasets without dynamic environment testing, and no studies conducted longitudinal assessments of performance degradation over time. This limits practical deployment assessment in production IoT environments.

However, our analysis reveals significant heterogeneity in evaluation methodologies across reviewed studies. Only 8 of 34 papers (23.5%) employed cross-dataset validation, while 65% reported accuracy without confidence intervals. Furthermore, baseline comparisons varied substantially, with some studies comparing against traditional ML approaches while others used rule-based systems. This methodological inconsistency limits meaningful comparison between LLM-based approaches and hinders meta-analytical assessment of the field's progress.

4.2. Implementation Analysis and Strategic Approaches

Our systematic review reveals three distinct implementation patterns in LLM-based IoT security solutions, each addressing specific deployment challenges and operational requirements. As presented in Table 9, these approaches demonstrate varying trade-offs between performance, resource utilization, and security guarantees.

Table 9. Implementation Approaches and Their Impact

Approach	**Representative Studies**	**Key Advantages**	**Limitations**	**Success Metrics**
Edge Deployment	Wang et al. [8], [22]	Low latency, real-time processing	Resource constraints	98.39% accuracy, 35.23ms latency
Hybrid Architecture	Fu et al. [3], TFHSVul [21]	Enhanced accuracy, reduced overhead	Implementation complexity	99.96% accuracy, 0.08s processing
Privacy-Preserving	Rehman et al. [9], Li et al. [10]	Strong privacy guarantees	Computational overhead	98.247% protection score

Edge-centric implementations demonstrate particular promise in addressing latency concerns. Wang et al. [29] achieved 98.39% accuracy in smart home environments while maintaining practical processing times through efficient architectural design. This approach represents a significant advancement in real-time threat detection capabilities, particularly for resource-constrained IoT devices. The implementation successfully detected and prevented 98.2% of attempted network intrusions with a false positive rate of only 0.3%, demonstrating the practical viability of edge-based security solutions.

Hybrid architectures have emerged as a promising solution to balance performance requirements with resource constraints. The TFHSVul system [51] demonstrated the effectiveness of multi-component architectures, combining CodeBERT, MSFCNN, and ResGCN to achieve 0.97 precision in vulnerability detection. This architectural approach proved particularly effective in handling complex code structures, leading to the

identification of 68 previously unknown vulnerabilities across multiple vendors. The system's ability to process multiple input types simultaneously while maintaining high accuracy demonstrates the potential of hybrid approaches in addressing complex security challenges.

4.2.1. Cross-Platform Compatibility Assessment Our systematic analysis reveals limited attention to cross-platform compatibility in existing literature. Only 8 of 34 studies (23.5%) explicitly addressed multi-platform deployment considerations. Edge deployment studies [23, 29, 43] focused primarily on ARM-based systems, while cloud-based implementations [24, 32] assumed homogeneous computational environments. Analysis of implementation specifications shows that 67% of studies demonstrated processor-specific optimization requirements, indicating potential compatibility barriers for heterogeneous IoT environments. This represents a critical gap for practical deployment at scale.

4.3. Resource Optimization and Efficiency Analysis

Our analysis reveals significant variations in resource requirements across implementations, with particular emphasis on memory usage, processing time, and energy efficiency. Table 10 presents a detailed comparison of resource utilization across different implementation types, incorporating both quantitative metrics and qualitative assessments.

Table 10. Detailed Resource Utilization Analysis

Resource Type	**Edge Deployment**	**Cloud-Based**	**Hybrid**	**Optimization Impact**
Memory Usage	42.63MB - 2GB	2-25GB	1-5GB	45-89% reduction
Processing Time	0.08-0.5s	0.01-0.1s	0.05-0.3s	67% improvement
Model Parameters	788-1M	1M-1B	500K-5M	92% reduction
Energy Efficiency	High (85-95%)	Low (40-60%)	Medium (65-80%)	45% improvement
Bandwidth Usage	0.1-1MB/s	5-50MB/s	1-10MB/s	75% reduction

The optimization of resource utilization demonstrates significant advancement across multiple dimensions. Memory efficiency shows particular improvement, with implementations like BT-TPF [43] achieving state-of-the-art performance with minimal parameter requirements. The analysis reveals that optimized edge implementations can achieve comparable security effectiveness while reducing memory requirements by up to 89.85% compared to traditional approaches.

Processing optimization demonstrates similar advancement, with EBIDS [32] achieving execution times of 0.08273335 seconds compared to traditional approaches. This improvement in processing efficiency enables real-time threat detection and response, a critical requirement for IoT security applications. The implementation achieved this performance while maintaining high accuracy across both network and application layer detection tasks.

Energy efficiency analysis identifies a critical gap: only 8.8% of studies provided energy consumption metrics, focusing instead on computational efficiency measures. This omission significantly limits practical deployment assessment for battery-powered IoT devices where energy efficiency is paramount.

4.4. Architectural Innovations and Technical Advancements

Recent architectural innovations have addressed key challenges in LLM deployment for IoT security, with particular emphasis on model compression, hybrid processing approaches, and privacy protection mechanisms. Table 11 presents a comprehensive analysis of these innovations and their practical impacts on IoT security implementation.

Table 11. Architectural Innovations and Performance Impact

Innovation Type	**Representative Implementation**	**Key Achievement**	**Technical Impact**	**Deployment Benefits**
Model Compression	SecurityBERT [2]	89.85% size reduction	42.63MB model size	Enhanced edge deployment
Hybrid Processing	IoV-BERT-IDS [3]	99.96% accuracy	0.08s detection time	Improved real-time detection
Privacy Protection	Rehman et al. [9]	98.247% protection	Encrypted processing	Enhanced data security
Parameter Reduction	BT-TPF [22]	788 parameters	92% efficiency gain	Extreme resource optimization
Adaptive Learning	EBIDS [11]	Dual-layer detection	Layer-specific optimization	Improved accuracy

These architectural innovations demonstrate significant advancement in addressing the core challenges of LLM deployment in IoT security contexts. The development of efficient compression techniques, exemplified by SecurityBERT [2], enables practical deployment in resource-constrained environments while maintaining high detection accuracy. The implementation achieved this through a novel quantization approach that preserved critical security features while significantly reducing model size.

Hybrid architectural approaches, such as those implemented in IoV-BERT-IDS [3], demonstrate the potential for combining multiple security mechanisms to achieve superior detection capabilities. The system's ability to maintain 99.96% accuracy while operating within IoT resource constraints represents a significant advancement in practical security implementation. This was achieved through a carefully designed architecture that balanced computational requirements with detection capabilities.

Privacy-preserving frameworks have shown particular promise in addressing data protection concerns. Rehman et al. achieved 98.218% accuracy with their adaptive contextual privacy preservation framework while maintaining strong privacy guarantees. This implementation demonstrated significant improvements in handling imbalanced datasets, with particular success in detecting minority attack classes such as ransomware (52.004% improvement) and MITM attacks (59.007% improvement).

Password security architectures have shown particular promise through the integration of multiple ML components. The system proposed in combines Random Forest classification with RAG and FAISS indexing to create an adaptive security framework[56]. This implementation demonstrated significant improvements in both predictive accuracy and recommendation quality, particularly in addressing dictionary and brute force attacks on IoT devices.

The results presented in this comprehensive analysis demonstrate both the significant potential and remaining challenges in LLM-based IoT security implementations. The findings reveal clear patterns in architectural innovation, resource utilization, and privacy preservation capabilities while highlighting areas requiring further development. These results provide a foundation for understanding the current state of LLM integration in IoT security and identify promising directions for future research and development.

Model Interpretability Analysis: Despite achieving high detection accuracy, interpretability analysis reveals significant gaps across reviewed implementations. Only SecurityBERT [23] and EBIDS [32] provided attention visualization capabilities, while 79% of studies (27/34) lacked explicit explainability mechanisms. No studies addressed security analyst workflow integration requirements or provided real-time decision transparency features. This interpretability deficit significantly limits adoption in security-critical environments requiring decision transparency for compliance and operational requirements.

4.5. Mathematical Foundations of LLM-based IoT Security Architectures

The mathematical underpinnings of transformer-based security models in IoT environments warrant explicit formulation to enhance reproducibility and theoretical understanding. This section presents the core mathematical frameworks employed by the surveyed LLM implementations.

4.5.1. Attention Mechanism Formalization The self-attention mechanism fundamental to BERT-based IoT security systems is mathematically defined as:

$$\text{Attention}(Q, K, V) = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V \tag{1}$$

where $Q \in \mathbb{R}^{m\times d_k}$, $K \in \mathbb{R}^{n\times d_k}$, and $V \in \mathbb{R}^{n\times d_v}$ represent the query, key, and value matrices respectively, with d_k denoting the dimensionality of the key vectors [23]. SecurityBERT leverages this mechanism across multiple encoder layers, each incorporating multi-head self-attention and position-wise feed-forward neural networks to capture contextual dependencies in network traffic representations [23].

4.5.2. Privacy Preservation Effectiveness Metrics The protection effectiveness metric of 98.247% reported by Rehman et al. [30] represents a composite evaluation measure computed through their adaptive contextual privacy preservation framework. The metric derivation follows:

$$\text{Protection Effectiveness} = \frac{\text{TPR} \times \text{Precision}}{100} \tag{2}$$

where $\text{TPR} = \frac{TP}{TP+FN}$ and $\text{Precision} = \frac{TP}{TP+FP}$, with TP, FP, and FN denoting true positives, false positives, and false negatives respectively. Their framework demonstrated 98.218% accuracy, 98.247% precision, and 98.218% recall on the CSE-CIC-IDS2018 dataset [30].

4.5.3. Knowledge Distillation Optimization Framework The BT-TPF architecture [43] employs knowledge distillation to achieve computational efficiency while preserving detection accuracy. The optimization objective is formulated as:

$$\mathcal{L}_{\text{total}} = \alpha\mathcal{L}_{\text{CE}}(y_{\text{true}}, y_{\text{student}}) + (1-\alpha)\mathcal{L}_{\text{KL}}\left(\sigma\left(\frac{z_{\text{teacher}}}{T}\right), \sigma\left(\frac{z_{\text{student}}}{T}\right)\right) \tag{3}$$

where $\mathcal{L}_{\text{CE}}$ denotes the cross-entropy loss, $\mathcal{L}_{\text{KL}}$ represents the Kullback-Leibler divergence, T is the temperature parameter for softmax scaling, and $\alpha \in [0, 1]$ balances the loss components. This framework achieves a 90% parameter reduction, requiring only 788 parameters while maintaining detection accuracy exceeding 99% [43].

4.5.4. Multi-layer Detection Architecture Performance The EBIDS framework [32] implements a dual-layer detection mechanism optimized for IoT network environments. The system architecture employs a 12/7-block BERT configuration, achieving differentiated performance across network layers:

- **Network Layer Detection**: 97.49% accuracy with execution latency of 0.08273335 seconds
- **Application Layer Detection**: 94.25% accuracy

The temporal efficiency demonstrates significant improvement over conventional approaches, with EBIDS outperforming CNN-based methods (0.50371706s) and LSTM implementations (0.4222699s) by factors of 6.09× and 5.11× respectively [32].

5. DISCUSSION

The systematic analysis of LLM integration in IoT security reveals profound implications for both theoretical understanding and practical implementation of security measures in resource-constrained environments. These

findings suggest several significant paradigm shifts in approaching IoT security while highlighting critical areas for future development.

Theoretical Implications for Security Architecture

The evolution of LLM-based security approaches challenges traditional assumptions about the relationship between model complexity and security effectiveness. The success of lightweight implementations, particularly demonstrated by Wang et al. [43], suggests that security effectiveness may be more closely tied to architectural design than computational capacity. This finding has profound implications for theoretical approaches to security system design, suggesting a need to reevaluate fundamental assumptions about resource requirements for effective security implementations.

Our analysis reveals an emerging theoretical framework where security effectiveness emerges from the interaction between architectural components rather than raw computational power. The work of Che et al. [44] in developing domain-specific architectures demonstrates how targeted optimization can achieve superior results compared to general-purpose approaches. This suggests a theoretical model where security effectiveness is multiplicative rather than additive across system components, challenging traditional approaches to security system design.

Implications for Privacy-Security Balance

The development of privacy-preserving security architectures represents a significant theoretical advancement in resolving the traditional tension between privacy and security requirements. The work of Rehman et al. [30] and Li et al. [31] in developing hybrid architectures suggests that this tension may be artificial, arising from implementation limitations rather than fundamental constraints. This insight has profound implications for future security system design, suggesting possibilities for architectures that enhance both privacy and security simultaneously.

The success of these approaches in handling imbalanced datasets while maintaining privacy guarantees suggests new theoretical frameworks for understanding privacy preservation in security contexts. These frameworks move beyond traditional trade-off models to consider privacy and security as complementary rather than competing objectives.

Resource Optimization Paradigms

The relationship between resource utilization and security effectiveness emerges as more complex than previously theorized. While traditional approaches assumed a direct correlation between computational resources and security capabilities, our analysis suggests a more nuanced relationship. The success of domain-specific optimizations, particularly in medical sensor networks [52], indicates that contextual understanding may be more crucial than raw computational power.

This finding has significant implications for resource allocation strategies in IoT security implementations. Rather than focusing solely on computational efficiency, future approaches might benefit from emphasizing architectural optimization for specific security contexts. This suggests a new paradigm in resource optimization where effectiveness emerges from the alignment between architecture and security requirements rather than pure computational capability.

5.1. Ethical Implications and Adversarial Vulnerability Analysis

The deployment of LLM-based security systems in IoT environments introduces novel ethical considerations and security vulnerabilities that warrant systematic examination.

5.1.1. Privacy-Preserving Architectural Considerations The contextually rich representations learned by transformer architectures potentially enable inference of sensitive network topology and device characteristics through gradient analysis techniques. To address this concern, SecurityBERT [23] implements Privacy-Preserving Fixed-Length Encoding (PPFLE), specifically designed to obfuscate sensitive infrastructure details during model training while preserving detection efficacy.

The effectiveness of privacy preservation mechanisms is demonstrated by Rehman et al. [30], whose adaptive contextual privacy preservation framework achieves 98.247% protection effectiveness while maintaining detection

accuracy of 98.218% on the CSE-CIC-IDS2018 dataset, indicating that privacy and security objectives can be simultaneously optimized.

5.1.2. Algorithmic Bias and Fairness Analysis The training data composition directly influences model bias characteristics across device manufacturers, communication protocols, and deployment environments. SecurityBERT's evaluation on the Edge-IIoTset dataset [23], while comprehensive with 2,540,047 samples across 14 attack categories, may exhibit manufacturer-specific bias patterns that could affect detection performance for underrepresented device categories.

Similarly, IoV-BERT-IDS [24] demonstrates cross-dataset generalization across CICIDS2018, BoT-IoT, and Car-Hacking datasets, yet performance variations across these datasets indicate potential protocol-specific bias that merits further investigation.

5.1.3. Mitigation Strategies and Defensive Mechanisms **Architectural Hardening**: The knowledge distillation approach employed by BT-TPF [43] not only achieves computational efficiency through 90% parameter reduction but also potentially reduces the attack surface available for adversarial exploitation while maintaining detection accuracy exceeding 99%.

Privacy Enhancement: The multi-layered privacy approach combining PPFLE encoding [23] with adaptive contextual preservation [30] demonstrates that privacy-preserving objectives can be integrated into LLM architectures without compromising security performance.

Model Robustness: The dual-layer detection architecture implemented in EBIDS [32] provides redundancy mechanisms that enhance system resilience against targeted attacks on individual detection components.

5.2. Real-World Deployment Readiness Assessment

Our review reveals a significant maturity gap between research prototypes and production-ready implementations. Analysis shows that only 12% of studies provided accessible implementations, while 85% lacked integration guidelines for existing security infrastructure. Critically, zero studies included longitudinal deployment assessments or addressed model maintenance in operational environments. This implementation readiness gap encompasses legacy system integration challenges, continuous model adaptation requirements, and enterprise-scale validation protocols, highlighting the need for deployment-focused research initiatives.

Adversarial robustness evaluation reveals substantial gaps. Only 11.8% of studies addressed adversarial attacks, with focus limited to basic evasion attacks. Physical-world attack vectors and model inversion attacks remained unexamined, leaving critical security vulnerabilities unaddressed.

5.3. Future Research Directions

Our systematic review reveals several critical areas requiring focused research attention to advance the field of LLM-based IoT security. These research directions encompass methodological frameworks, technical innovations, and implementation considerations that warrant systematic investigation by the research community.

The development of standardized evaluation frameworks emerges as a primary methodological challenge requiring immediate attention. Current research in LLM-based IoT security suffers from inconsistent evaluation metrics and benchmarking approaches, making direct comparisons between different implementations challenging. Future research should focus on establishing comprehensive evaluation frameworks that consider both technical performance metrics and practical deployment constraints. These frameworks should incorporate standardized testing scenarios that reflect real-world IoT security challenges, enabling meaningful comparison across different architectural approaches. Additionally, the development of standardized benchmarking datasets specifically designed for LLM-based IoT security applications would significantly enhance the field's ability to evaluate and compare different solutions effectively [57].

Cross-study comparison methodologies represent another crucial area requiring development. The current lack of standardized approaches for comparing results across different studies limits our ability to draw comprehensive conclusions about the effectiveness of various LLM implementations in IoT security [58]. Future research should focus on developing robust methodological frameworks that enable meaningful comparison of results across

different studies, considering variations in implementation contexts, evaluation metrics, and deployment scenarios. This includes developing standardized reporting formats for security metrics, resource utilization measurements, and performance indicators that facilitate meta-analysis and systematic comparison of different approaches.

Technical challenges in resource optimization demand systematic investigation. While current implementations demonstrate promising results in reducing model size and computational requirements, significant work remains in optimizing LLM-based security solutions for resource-constrained IoT environments. Future research should explore novel approaches to model compression, quantization techniques specifically designed for security applications, and architectural innovations that minimize resource utilization while maintaining security effectiveness. This includes investigating the relationship between model complexity and security performance to identify optimal trade-offs for different deployment scenarios [59].

Privacy preservation techniques require substantial advancement to address the unique challenges of IoT environments. Future research should focus on developing privacy-preserving training and inference mechanisms that protect sensitive IoT data while maintaining security effectiveness. This includes investigating federated learning approaches specifically designed for IoT security applications, developing privacy-preserving model adaptation techniques, and creating frameworks for evaluating privacy-security trade-offs in different deployment contexts. Research efforts should also address the challenge of maintaining privacy guarantees across heterogeneous IoT networks with varying security requirements and resource constraints [60].

Cross-platform compatibility presents significant technical challenges that future research must address. The diverse nature of IoT environments, with varying hardware capabilities, communication protocols, and security requirements, necessitates the development of flexible and adaptable security solutions. Future research should investigate approaches for creating platform-agnostic security frameworks that can effectively operate across different IoT architectures while maintaining consistent security performance. This includes developing adaptive model architectures that can automatically adjust to different platform capabilities and resource constraints.

Implementation challenges in scalability and real-world deployment require systematic investigation. As LLM-based security solutions move from research environments to practical deployment, understanding scalability constraints and deployment challenges becomes crucial. Future research should examine approaches for scaling security solutions across large IoT networks while maintaining performance and resource efficiency. This includes investigating distributed deployment strategies, developing efficient update mechanisms for deployed models, and creating frameworks for managing security policies across scaled implementations [61].

Integration with existing security infrastructure presents complex challenges that future research must address. The practical deployment of LLM-based security solutions requires seamless integration with existing security frameworks and operational processes. Future research should focus on developing integration methodologies that enable effective combination of LLM-based approaches with traditional security mechanisms. This includes investigating hybrid architectures that leverage the strengths of both approaches, developing transition strategies for organizations adopting LLM-based security solutions, and creating frameworks for evaluating the effectiveness of integrated security systems [62].

The advancement of automated response capabilities represents a critical area for future research. While current implementations excel at threat detection and analysis, the development of sophisticated automated response mechanisms remains limited. Future research should investigate approaches for enabling LLM-based security systems to not only detect but also respond to security threats autonomously while operating within IoT resource constraints. This includes developing frameworks for response generation and validation, creating mechanisms for ensuring the safety and reliability of automated responses, and investigating approaches for maintaining human oversight of automated security operations [63].

These research directions collectively represent a comprehensive agenda for advancing the field of LLM-based IoT security. Progress in these areas would significantly enhance our ability to develop and deploy effective security solutions in resource-constrained IoT environments while maintaining robust security guarantees and operational efficiency. Success in addressing these challenges requires sustained research effort across multiple domains, from theoretical framework development to practical implementation strategies.

5.3.1. Minimum Reporting Standards To enhance reproducibility and enable systematic comparison across studies, we propose the following standardized reporting requirements for future LLM-based IoT security research:

Dataset Specification Protocol: Complete documentation of evaluation datasets including attack type distribution, temporal characteristics, and representativeness metrics relative to production IoT environments.

Architectural Transparency Requirements: Explicit mathematical formulations of model architectures, hyperparameter specifications, and optimization procedures to enable independent reproduction.

Baseline Comparison Framework: Standardized comparison protocols with established traditional ML approaches using identical evaluation datasets and metrics.

Resource Quantification Standards: Comprehensive measurement and reporting of computational requirements including memory utilization, energy consumption, and inference latency across representative hardware configurations.

Privacy and Security Assessment: Systematic evaluation of privacy preservation mechanisms and vulnerability analysis following established security assessment protocols.

5.3.2. Interdisciplinary Collaboration Requirements The successful advancement of LLM-based IoT security necessitates coordinated efforts across multiple research domains:

Natural Language Processing and Cybersecurity Integration: Development of domain-specific language models optimized for security-relevant pattern recognition while maintaining computational efficiency for IoT deployment.

Hardware-Software Co-design: Collaborative development of specialized hardware accelerators and software optimization techniques to enable practical LLM deployment in resource-constrained IoT environments.

Privacy-Preserving Machine Learning: Integration of advanced privacy preservation techniques with security-critical applications to address the dual requirements of threat detection and data protection.

6. Conclusion

This systematic review has examined the integration of LLMs in IoT security through analysis of 34 recent studies (2022-2024), revealing significant advancements while identifying crucial research gaps. The findings demonstrate that LLM-based approaches have substantially enhanced security capabilities, with frameworks such as SecurityBERT achieving 98.2% detection accuracy while reducing model size by 89.85%. Privacy preservation mechanisms have shown marked improvement, exemplified by LLM-CI's achievement of 90% accuracy in maintaining contextual integrity standards.

Despite these advances, fundamental challenges persist in implementing LLM-based security solutions within IoT environments. Resource constraints remain significant, with optimized implementations requiring substantial computational resources. The necessity for real-time processing and privacy preservation during model operation presents additional complexity for practical deployment. Architectural innovations have emerged to address these limitations, including federated learning approaches reducing energy consumption by 45% and hybrid architectures optimizing resource utilization.

The review identifies critical research gaps requiring attention: standardization of evaluation frameworks, resource optimization for ultra-constrained devices, and enhancement of cross-platform compatibility. Future research directions should emphasize developing efficient LLM architectures suitable for resource-constrained environments while maintaining robust security capabilities. Additionally, improving model interpretability and establishing comprehensive evaluation frameworks will be crucial for advancing the field.

This systematic analysis establishes a foundation for future research in LLM-based IoT security, highlighting both the significant potential and remaining challenges in this emerging domain. The findings suggest that successful implementation of LLMs in IoT security requires careful balance between security effectiveness and practical constraints, particularly regarding computational resources and privacy requirements.

REFERENCES

1. N. M. Karie, N. M. Sahri, and P. Haskell-Dowland, *IoT Threat Detection Advances, Challenges and Future Directions*, Proceedings - 2020 Workshop on Emerging Technologies for Security in IoT, ETSecIoT 2020, pp. 22–29, Apr. 2020, doi: 10.1109/ETSECIOT50046.2020.00009.
2. C. L. Kok, C. K. Ho, T. K. Lee, Z. Y. Loo, Y. Y. Koh, and J. P. Chai, *A Novel and Low-Cost Cloud-Enabled IoT Integration for Sustainable Remote Intravenous Therapy Management*, Electronics (Basel), vol. 13, no. 10, May 2024, doi: 10.3390/ELECTRONICS13101801.
3. S. R, Prof. M. S. Raja, and Prof. R. R, *IoT Based Drug Delivery System*, International Journal of Innovative Research in Information Security, vol. 10, no. 02, pp. 81–84, Feb. 2024, doi: 10.26562/IJIRIS.2024.V1002.09.
4. P. Muneeshwari, R. Suguna, G. M. Valantina, M. Sasikala, and D. Lakshmi, *IoT-Driven Predictive Maintenance in Industrial Settings through a Data Analytics Lens*, 2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies, pp. 1–5, Sep. 2024, doi: 10.1109/TQCEBT59414.2024.10545167.
5. D. A. - and Dr. S. T. -, *Innovative Sensor Technologies in IoT-Based Remote Patient Monitoring Systems: A Comprehensive Analysis*, International Journal For Multidisciplinary Research, vol. 6, no. 5, Sep. 2024, doi: 10.36948/IJFMR.2024.V06I05.27218.
6. S. P. Doifode and V. M. Biradar, *Cybersecurity in the Internet of Things (IoT): Challenges and Solutions*, International Journal of Scientific Research in Modern Science and Technology, vol. 3, no. 7, pp. 17–21, Jul. 2024, doi: 10.59828/IJSRMST.V3I7.222.
7. N. Srinivasan, *Artificial Intelligence in IoT Security: Review of Advancements, Challenges, and Future Directions*, International Journal of Innovative Technology and Exploring Engineering, vol. 13, no. 7, pp. 14–20, Jun. 2024, doi: 10.35940/IJITEE.G9911.13070624.
8. F. Sommer, M. Gierl, R. Kriesten, F. Kargl, and E. Sax, *Combining Cyber Security Intelligence to Refine Automotive Cyber Threats*, ACM Transactions on Privacy and Security, vol. 27, no. 2, pp. 1–34, Mar. 2024, doi: 10.1145/3644075.
9. D. Zhang, X. Cao, Z. Jin, Y. Zhang, X. Hu, and C. Wu, *Research and Implementation of CPS for Transmission Front Middle Case Assembly Line*, Applied Sciences, vol. 13, no. 10, May 2023, doi: 10.3390/APP13105912.
10. R. Masum, *Cyber Security in Smart Manufacturing (Threats, Landscapes Challenges)*, arXiv.org, 2023, doi: 10.48550/ARXIV.2304.10180.
11. P. T. Ganai, A. Bag, A. Sable, K. H. Abdullah, S. Bhatia, and B. Pant, *A Detailed Investigation of Implementation of Internet of Things (IOT) in Cyber Security in Healthcare Sector*, 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp. 1571–1575, 2022, doi: 10.1109/ICACITE53722.2022.9823887.
12. A. S. Musthafa, A. J. Preya, F. M. Alneyadi, N. S. Alattas, G. El Hassan, and H. Zia, *Safeguarding IoT Device Deployment in Healthcare: Analysis and Strategies for Enhanced Security and Privacy*, 2023 4th International Conference on Communications, Information, Electronic and Energy Systems (CIEES), 2023, doi: 10.1109/CIEES58940.2023.10378838.
13. X. Zhu, J. Huang, and C. Qi, *Modeling and Analysis of Malware Propagation for IoT Heterogeneous Devices*, IEEE Syst J, vol. 17, no. 3, pp. 3846–3857, Sep. 2023, doi: 10.1109/JSYST.2023.3269158.
14. I. Rozlomii, A. Yarmilko, and S. Naumenko, *Data security of IoT devices with limited resources: challenges and potential solutions*, GSC Advanced Research and Reviews, vol. 21, no. 1, pp. 85–96, Oct. 2024, doi: 10.30574/GSCARR.2024.21.1.0388.
15. Y. M. Al-Sharo, K. Al Smadi, T. Al Smadi, and N. Yasameen Kamil, *Optimization of Stable Energy PV Systems Using the Internet of Things (IoT)*, Tikrit Journal of Engineering Sciences, vol. 31, no. 1, pp. 127–137, Jan. 2024, doi: 10.25130/TJES.31.1.11.
16. M. Tawfik, *Optimized intrusion detection in IoT and fog computing using ensemble learning and advanced feature selection*, PLoS One, vol. 19, no. 8, p. e0304082, Aug. 2024, doi: 10.1371/JOURNAL.PONE.0304082.
17. B. Ibrahim Hairab, H. K. Aslan, M. S. Elsayed, A. D. Jurcut, and M. A. Azer, *Anomaly Detection of Zero-Day Attacks Based on CNN and Regularization Techniques*, Electronics (Basel), vol. 12, no. 3, Feb. 2023, doi: 10.3390/ELECTRONICS12030573.
18. B. Bokkena, *Enhancing IT Security with LLM-Powered Predictive Threat Intelligence*, 2024 5th International Conference on Smart Electronics and Communication (ICOSEC), pp. 751–756, 2024, doi: 10.1109/ICOSEC61587.2024.10722712.
19. B. Bokkena, *Enhancing IT Security with LLM-Powered Predictive Threat Intelligence*, 2024 5th International Conference on Smart Electronics and Communication (ICOSEC), pp. 751–756, 2024, doi: 10.1109/ICOSEC61587.2024.10722712.
20. M. Ferrag, F. Alwahedi, A. Battah, B. Cherif, A. Mechri, and N. Tihanyi, *Generative AI and Large Language Models for Cyber Security: All Insights You Need*, ArXiv, vol. abs/2405.12750, doi: 10.48550/ARXIV.2405.12750.
21. X. Zhang, T. Chen, J. Wu, and Q. Yu, *Intelligent Network Threat Detection Engine Based on Open Source GPT-2 Model*, Proceedings - 2023 International Conference on Computer Science and Automation Technology, CSAT 2023, pp. 392–397, 2023, doi: 10.1109/CSAT61646.2023.00107.
22. T. S. AlSalem, M. A. Almaiah, and A. Lutfi, *Cybersecurity Risk Analysis in the IoT: A Systematic Review*, Electronics (Basel), vol. 12, no. 18, Sep. 2023, doi: 10.3390/ELECTRONICS12183958.
23. M. A. Ferrag et al., *Revolutionizing Cyber Threat Detection with Large Language Models: A Privacy-Preserving BERT-Based Lightweight Model for IoT/IIoT Devices*, IEEE Access, vol. 12, pp. 23733–23750, Jun. 2024, doi: 10.1109/ACCESS.2024.3363469.
24. M Fu, P. Wang, M. Liu, Z. Zhang, X. Zhou, *IoV-BERT-IDS: Hybrid Network Intrusion Detection System in IoV Using Large Language Models*, IEEE Transactions on Vehicular Technology, 2024.
25. J. Xiang, W. Wang, T. Ye, and P. Liu, *LuaTaint: A Static Taint Analysis System for Web Interface Framework Vulnerability of IoT Devices*, Feb. 2024, doi: 10.1109/JIOT.2024.3490661.
26. N. Chaves-Tibaduiza, A. I. Becerra-Muñoz, A. Robledo-Giron, O. M. Caicedo, *On the feasibility of using an encoder-only model for anomaly detection: the BERTAD approach*, 2024 IEEE Colombian Conference on Communications and Computing, 2024.
27. Y. Shvartzshnaider, V. Duddu, and J. Lacalamita, *LLM-CI: Assessing Contextual Integrity Norms in Language Models*, Sep. 2024.
28. N. Alam, S. Zhang, E. Rodriguez, A. Nafis, E. Hoque, *iConPAL: LLM-guided Policy Authoring Assistant for Configuring IoT Defenses*, 2024 IEEE Secure Development Conference (SecDev), 2024.
29. M. Wang, N. Yang, and N. Weng, *Securing a Smart Home with a Transformer-Based IoT Intrusion Detection System*, Electronics 2023, vol. 12, no. 9, p. 2100, May 2023, doi: 10.3390/ELECTRONICS12092100.

30. U. U. Rehman, M. Hussain, T. D. T. Nguyen, and S. Lee, *Let's Hide from LLMs: An Adaptive Contextual Privacy Preservation Method for Time Series Data*, ACM International Conference Proceeding Series, pp. 196–203, Dec. 2023, doi: 10.1145/3639592.3639619.
31. F. Li, H. Shen, J. Mai, T. Wang, Y. Dai, and X. Miao, *Pre-trained language model-enhanced conditional generative adversarial networks for intrusion detection*, Peer Peer Netw Appl, vol. 17, no. 1, pp. 227–245, Jan. 2024, doi: 10.1007/S12083-023-01595-6/METRICS.
32. S. Sattarpour, A. Barati, and H. Barati, *EBIDS: efficient BERT-based intrusion detection system in the network and application layers of IoT*, Cluster Comput, vol. 28, no. 2, pp. 1–21, Apr. 2025, doi: 10.1007/S10586-024-04775-Y/METRICS.
33. B. Xiao, B. Kantarci, J. Kang, D. Niyato, and M. Guizani, *Efficient Prompting for LLM-based Generative Internet of Things*, Jun. 2024, doi: 10.1109/JIOT.2024.3470210.
34. J. Ye, X. Fei, X. C. de Carnavalet, L. Zhao, L. Wu, M. Zhang, *Detecting command injection vulnerabilities in Linux-based embedded firmware with LLM-based taint analysis of library functions*, Computers & Security, 2024.
35. G. Morales, F. Tajwar Romit, A. Bienek-Parrish, P. Jenkins, and R. Slavin, *IoT Device Classification Using Link-Level Features for Traditional Machine Learning and Large Language Models*, 2024, doi: 10.5220/0012365700003648.
36. S. Paria, A. Dasgupta, and S. Bhunia, *SPELL: An End-to-End Tool Flow for LLM-Guided Secure SoC Design for Embedded Systems*, IEEE Embed Syst Lett, vol. 16, no. 4, pp. 365–368, 2024, doi: 10.1109/LES.2024.3447691.
37. Y. Ikegami et al., *Prioritizing Vulnerability Assessment Items Using LLM Based on IoT Device Documentations*, 2024 11th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2024, pp. 147–152, 2024, doi: 10.1109/IOTSMS62296.2024.10710294.
38. M. Hassanin, M. Keshk, S. Salim, M. Alsubaie, D. Sharma, *PLLM-CS: Pre-trained Large Language Model (LLM) for cyber threat detection in satellite networks*, Ad Hoc Networks, 2025.
39. S. Baral, S. Saha, and A. Haque, *An Adaptive End-to-End IoT Security Framework Using Explainable AI and LLMs*, Sep. 2024.
40. H. Nakanishi et al., *Initial Seeds Generation Using LLM for IoT Device Fuzzing*, 2024 11th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2024, pp. 5–10, 2024, doi: 10.1109/IOTSMS62296.2024.10710191.
41. L. Xiao and X. Chen, *Enhancing LLM with Evolutionary Fine Tuning for News Summary Generation*, arXiv.org, 2023, doi: 10.48550/ARXIV.2307.02839.
42. L. Xu et al., *TFHSVul:A Fine-Grained Hybrid Semantic Vulnerability Detection Method Based on Self-Attention Mechanism in IOT*, IEEE Internet Things J, 2024, doi: 10.1109/JIOT.2024.3459921.
43. Z. Wang, J. Li, S. Yang, X. Luo, D. Li, and S. Mahmoodi, *A lightweight IoT intrusion detection model based on improved BERT-of-Theseus*, Expert Syst Appl, vol. 238, p. 122045, Mar. 2024, doi: 10.1016/J.ESWA.2023.122045.
44. X. Che, Y. Zheng, M. Zhu, Q. Li, and X. Dong, *A Domain-Adaptive Large Language Model With Refinement Framework For IoT Cybersecurity*, 2024 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics, pp. 224–229, Aug. 2024, doi: 10.1109/ITHINGS-GREENCOM-CPSCOM-SMARTDATA-CYBERMATICS62450.2024.00056.
45. F. Adjewa, M. Esseghir, and L. Merghem-Boulahia, *Efficient Federated Intrusion Detection in 5G ecosystem using optimized BERT-based model*, Sep. 2024.
46. T. Ali and P. Kostakos, *HuntGPT: Integrating Machine Learning-Based Anomaly Detection and Explainable AI with Large Language Models (LLMs)*, Sep. 2023.
47. A. Diaf, A. A. Korba, N. Elislem Karabadji, and Y. Ghamri-Doudane, *Beyond Detection: Leveraging Large Language Models for Cyber Attack Prediction in IoT Networks*, Proceedings - 2024 20th International Conference on Distributed Computing in Smart Systems and the Internet of Things, DCOSS-IoT 2024, pp. 117–123, Aug. 2024, doi: 10.1109/DCOSS-IoT61029.2024.00026.
48. M. Guastalla, Y. Li, A. Hekmati, and B. Krishnamachari, *Application of Large Language Models to DDoS Attack Detection*, Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, vol. 552 LNICST, pp. 83–99, 2024, doi: 10.1007/978-3-031-51630-6_6.
49. T. Wang, Z. Zhao, and K. Wu, *Exploiting LLM Embeddings for Content-Based IoT Anomaly Detection*, 2024 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, PACRIM 2024, 2024, doi: 10.1109/PACRIM61180.2024.10690230.
50. Y. Li et al., *Personal LLM Agents: Insights and Survey about the Capability, Efficiency and Security*, Jan. 2024.
51. Y. Yang, *IoT Software Vulnerability Detection Techniques through Large Language Model*, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 14308 LNCS, pp. 285–290, 2023, doi: 10.1007/978-981-99-7584-6_21.
52. L. Sun, Y. Wang, H. Li, and G. Muhammad, *Fine-grained vulnerability detection for medical sensor systems*, Internet of Things, vol. 28, p. 101362, Dec. 2024, doi: 10.1016/J.IOT.2024.101362.
53. B. Malisetty, A. J. Perez, S. Krenn, B. Malisetty, and A. J. Perez, *Evaluating Quantized Llama 2 Models for IoT Privacy Policy Language Generation*, Future Internet 2024, vol. 16, no. 7, p. 224, Jun. 2024, doi: 10.3390/FI16070224.
54. B. K. Webb, S. Purohit, and R. Meyur, *Cyber Knowledge Completion Using Large Language Models*, Sep. 2024.
55. B. Breve, G. Cimino, and V. Deufemia, *Hybrid Prompt Learning for Generating Justifications of Security Risks in Automation Rules*, ACM Trans Intell Syst Technol, vol. 15, no. 5, p. 103, Oct. 2024, doi: 10.1145/3675401.
56. *Leveraging Machine Learning and Large Language Model to Mitigate Smart Home IoT Password Breaches-All Databases*.
57. H. Zhang et al., *Agent Security Bench (ASB): Formalizing and Benchmarking Attacks and Defenses in LLM-based Agents*, arXiv.org, 2024, doi: 10.48550/ARXIV.2410.02644.
58. M. Leon, *Benchmarking Large Language Models with a Unified Performance Ranking Metric*, International Journal in Foundations of Computer Science & Technology, vol. 14, no. 4, pp. 15–27, Jul. 2024, doi: 10.5121/IJFCST.2024.14302.
59. V. Egiazarian, A. Panferov, D. Kuznedelev, E. Frantar, A. Babenko, and D. Alistarh, *Extreme Compression of Large Language Models via Additive Quantization*, ArXiv, vol. abs/2401.06118, doi: 10.48550/ARXIV.2401.06118.

60. H. Jiang, M. Liu, S. Sun, Y. Wang, and X. Guo, *FedSyL: Computation-Efficient Federated Synergy Learning on Heterogeneous IoT Devices*, 2022 IEEE/ACM 30th International Symposium on Quality of Service (IWQoS), pp. 1–10, 2022, doi: 10.1109/IWQOS54832.2022.9812907.
61. P. He et al., *Distributed Inference Performance Optimization for LLMs on CPUs*, ArXiv, vol. abs/2407.00029, doi: 10.48550/ARXIV.2407.00029.
62. S. Baral, S. Saha, and A. Haque, *An Adaptive End-to-End IoT Security Framework Using Explainable AI and LLMs*, ArXiv, vol. abs/2409.13177, doi: 10.48550/ARXIV.2409.13177.
63. H. Xu et al., *Large Language Models for Cyber Security: A Systematic Literature Review*, arXiv.org, vol. 1, 2024, doi: 10.48550/ARXIV.2405.04760.