Decentralized Threat Detection and AI-Assisted Incident Response for Cloud Environments

PI: Wajih Ul Hassan, Assistant Professor, Department of Computer Science, University of Virginia

Cash funding needed: $75,000 USD
AWS Promotional Credits needed: $25,000 USD

Abstract

As cloud providers face increasingly sophisticated Advanced Persistent Threats (APTs), scalable Cloud Detection and Response (CDR) systems are essential. Centralized threat detection in cloud environments struggles to handle the vast volume of audit logs generated by distributed worker nodes, creating significant data transfer overhead, network congestion, and slower response times. Additionally, manual investigation of CDR alerts by Security Operations Centers (SOCs) is slow and prone to error, highlighting the need for scalable, automated solutions. This proposal introduces a novel framework that addresses these limitations through a two-pronged approach: decentralized threat detection and AI-assisted alert investigation. By processing threat insights locally on each node using federated learning and Graph Neural Networks, the proposed FEDDETECT system reduces data transfer overhead and enhances scalability. To further improve SOC efficiency, the proposal introduces QUERYAI, an AI-driven assistant that automates the generation of investigation queries for analyzing audit logs stored in Security Information and Event Management (SIEM) systems. Leveraging a pre-trained language model, QUERYAI translates SOC prompts into optimized queries, streamlining investigations and reducing the need for manual analysis. This combined approach aims to significantly enhance cloud security by enabling more efficient threat detection and response.

Keywords: Threat Detection; Cloud Security; Graph Neural Networks; LLMs;

Introduction

Cloud Detection and Response (CDR) systems are essential for identifying threats in cloud environments, where worker nodes across a cloud cluster generate extensive audit logs that are centrally collected and analyzed. In a typical CDR workflow, these logs are gathered at a central point to detect suspicious activity, using either signature-based or anomaly-based detection methods. Signature-based methods [12, 9] rely on matching known threat patterns, which limits them to detecting established attacks. Anomaly-based methods [2, 6], however, detect deviations from typical behavior, making them better suited for identifying novel and evolving threats.

Recent advances in anomaly detection leverage provenance techniques [38, 31, 8], which build data provenance graphs from audit logs to track sequences of related events. In these graphs, nodes represent system entities like processes or files, and edges depict system calls, such as read or fork, that define interactions between entities, as shown in Figure 1. Analyzing these graphs enables systems to detect complex, multi-step malicious behaviors that traditional methods might miss. This approach improves detection by identifying subtle, evolving attack patterns, allowing machine learning models trained on benign patterns to flag anomalies signaling potential threats.

Figure 1: An example provenance graph showcasing the downloading of a malicious file.

Unfortunately, centralized CDR systems that rely on Security Information and Event Management (SIEM) platforms face significant challenges in scalability and efficiency within cloud clusters. SIEM systems typically aggregate and store massive volumes of audit logs from distributed worker nodes. When alerts are generated, Security Operations Centers (SOCs) must investigate by writing complex queries, often in languages like Kusto Query Language (KQL), to extract relevant data from these logs. This manual process is time-intensive, requires substantial expertise, and is prone to human error, especially as analysts interpret complex relationships within provenance graphs to distinguish benign from malicious behavior. Additionally, centralizing audit logs for processing creates data bottlenecks, network congestion, and delays in response times, ultimately slowing SOC operations and leaving incidents unresolved.

This proposal addresses these challenges with two main objectives. First, we will develop FEDDETECT,

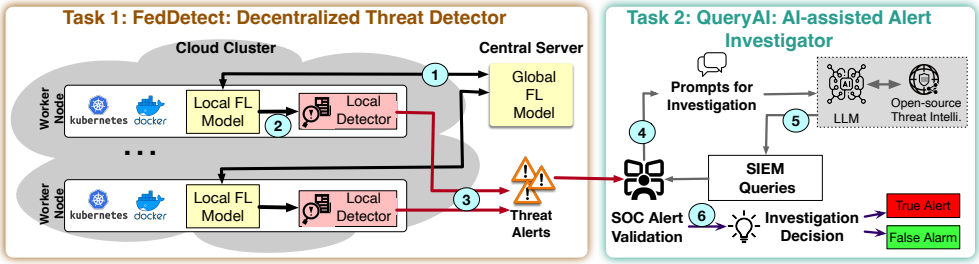

Figure 2: Workflow of our proposed decentralized threat detector and AI-assisted alert investigation framework.

a decentralized detection system leveraging Federated Learning (FL) to enhance threat detection while minimizing centralized data transfers. FEDDETECT enables worker nodes to process audit logs locally, supporting scalable, cloud-native detection without the network overhead of centralized systems (Task 1). Integrating FL into CDR systems presents challenges due to the heterogeneous, non-IID log distributions across nodes, leading to conflicting updates that degrade model performance [5] and data imbalances that skew outcomes and reduce accuracy [13, 42].

To overcome these issues, we combine FL with Graph Neural Networks (GNNs) to enable decentralized training directly on provenance graphs from worker nodes, removing the need for raw data sharing. Our approach introduces a novel FL aggregation algorithm with layer-wise coefficients to capture latent proximities among local updates, refined through confidence-based entropy minimization on proxy datasets. This system will incorporate worker-specific aggregation, adaptive learning rates, and asynchronous updates for faster model convergence. We will explore GNN architectures like GraphSAGE [25] to capture structural and temporal interactions in provenance graphs, allowing for the detection of multi-step attacks. Additionally, attention mechanisms [34] and Spatio-Temporal Graph Networks [41] will enhance embedding precision and capture evolving patterns, making FEDDETECT a scalable, cloud-native alternative to traditional CDR by minimizing centralized data transfer.

Secondly, we introduce QUERYAI, an AI-driven SOC assistant that automates the generation of investigation queries for SIEM systems. Using a pre-trained language model (LLM), QUERYAI interprets SOC investigation prompts to generate precise, contextually relevant queries. This process involves parsing the prompt to identify key data fields and entities, constructing a structured query, and refining it through an iterative, confidence-based review. By automating query generation, QUERYAI enables SOC teams to conduct faster, more accurate investigations, bridging expertise gaps and streamlining response workflows (Task 2).

PI Qualifications: PI Hassan is a leader in provenance-based system auditing and threat detection. His work includes developing methods for capturing audit logs from large-scale systems in a highly storage- and network-efficient manner [17, 19, 21, 22, 4, 30], as well as developing graph-powered machine learning techniques to detect stealthy threats with high precision [36, 37, 15, 31]. PI Hassan has also led efforts to streamline system log data, reducing log sizes and effectively summarizing long-term attack patterns [15, 18, 20, 16, 27]. His credentials include two patents in the security field and successful industry collaborations with NEC Labs, NortonLifeLock, and Corelight.

Methods

Task 1. *(FEDDETECT: Leveraging Federated Learning for Decentralized Cloud Threat Detection)* In cloud environments, integrating models from diverse worker nodes in a Federated Learning (FL) system presents unique challenges due to the heterogeneous, non-IID distributions of log data across nodes. Each node's local log data contains distinct graph structures and node features, leading to diverging model parameters across cloud nodes. Traditional FL methods like FEDAVG [26] treat all updates uniformly, disregarding conflicting gradient directions, which often diminishes collaborative benefits and can result in worse model utility than isolated training.

Proposed Work - **To address these challenges, we propose a novel FL aggregation algorithm tailored to GNN structures for synchronizing worker node models and accelerating global model convergence.** This algorithm uses *layer-wise coefficients* $\Lambda = \lambda_i^l i \in [N]^{l \in [L]}$ that are *learned* to capture latent proximities among local updates, adapting coefficients through each GNN layer depth $l \in [L]$: $\theta \leftarrow \mathcal{A}(\Lambda, \Theta) \equiv \sum i = 1^N \lambda_i^l \theta_i^l l = 1^L$, where $\mathcal{A}$ is the FL model aggregation on the server, and θ and $\Theta = \theta_i i \in [N]$ represent the global and local node model parameters, respectively. To optimize aggregation coefficients, we minimize the ***entropy*** of the merged model θ on a proxy dataset $\tilde{\mathcal{X}}$:

$$\Lambda^* = \arg\min_{\Lambda} \mathcal{L}_{\Lambda, \tilde{\mathcal{X}}} := \mathbb{H}\left[f(\tilde{\mathcal{X}}; \mathcal{A}(\Lambda, \Theta)) \right],$$

where $\mathbb{H}$ represents entropy, indicating model prediction confidence. The proxy dataset $\tilde{\mathcal{X}}$, a small batch of synthetic log data shared voluntarily by nodes, reduces prediction uncertainty and mitigates non-IID effects. Additionally, we design *personalized node models* by learning node-specific coefficients $\{\Lambda_i\}_{i \in [N]}$, which adjust parameter contributions based on data distribution similarity, ensuring nodes benefit from global collaboration while retaining models tailored to unique data. This approach is compatible with existing FL methods, like FEDPROX [24], further enhancing model personalization.

Our proposed CDR system, FEDDETECT, will incorporate this FL aggregation to create an accurate and scalable anomaly detector, as illustrated in Figure 3. During the training phase, we will use FL to train GNN models across distributed worker nodes using benign log data, allowing the system to learn patterns of normal behavior without centralizing sensitive logs. This decentralized approach enables each worker node to contribute to the model while retaining data locally, building a comprehensive understanding of typical system activities across diverse environments. In the detection or runtime phase, these trained models will then analyze incoming log data for deviations from learned benign patterns, flagging anomalous activities that may indicate potential threats.

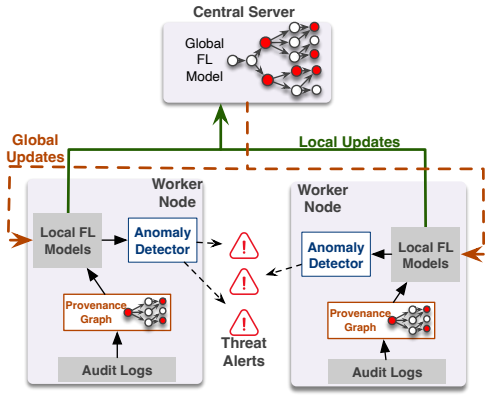

Figure 3: Workflow of our proposed decentralized CDR.

To handle scalability and complexity, we will explore GNN architectures such as GraphSAGE [14] for inductive learning on large graphs, and ChebNet [33] to generalize convolutions across graphs, which is critical for processing large-scale data. Attention mechanisms from Graph Attention Networks [35] will dynamically weigh node importance, enhancing embedding precision. Spatio-Temporal Graph Networks [41] will capture evolving patterns over time, addressing the temporal aspect of system logs. For model efficiency within the FL setup, we will implement adaptive learning rate techniques and asynchronous updates [39]. Additionally, to reduce processing delays common in traditional GNN models, we will adopt efficient architectures like GraphSAGE and ChebNet, which enhance processing speed and scalability in large cloud environments. Through these optimizations, FEDDETECT aims to provide a high-performance, scalable solution for cloud-native anomaly detection.

Evaluation: We will evaluate system scalability by incrementally increasing the number of worker nodes and data volume, monitoring key metrics such as throughput, latency, and resource utilization (CPU and memory) across diverse network environments. For performance benchmarking, we will use DARPA datasets along with additional, systematically generated benign and malicious datasets. Malicious data will be created using MITRE Caldera [7] and Infection Monkey [23], tools designed to emulate a broad range of APTs scenarios by replicating complex attack patterns and testing across diverse network configurations. To generate realistic benign logs, we will employ Generative Adversarial Networks (GANs) [40, 32] which capture the structure and dynamics of typical enterprise logs, producing synthetic, diverse benign data with essential characteristics for effective CDR evaluation.

Task 2. *(*QUERYAI*: An AI-Enhanced System for Efficient Alert Investigation in SOCs)* SOC teams often rely on investigation queries in languages like Kusto Query Language (KQL) to analyze alerts from CDR systems, a process that can be time-consuming and demands significant expertise [3, 1]. Automating the conversion of investigation prompts into precise SIEM queries could improve SOC efficiency, enabling analysts to focus more on responding to threats. Current automated tools, like Microsoft's Copilot for Security (CFS), have shown limitations in accuracy. For example, when tasked to retrieve all external emails sent by a user on a specific date, CFS returned only five results due to syntax errors, whereas manual analysis identified 17 relevant emails [28]. This highlights the need for a solution that can consistently generate accurate SIEM queries to enhance alert investigations.

Proposed Work - **To address the above challenges, we develop an LLM-based assistant, QUERYAI, to generate effective investigation queries for SIEM systems from SOC prompts.** Inspired by structured methodologies that improve language model reasoning on complex tasks [29], QUERYAI follows a systematic workflow that enhances SOC response efficiency and accuracy. The approach involves generating structured instructions, followed by iterative query construction and refinement phases to produce high-quality, deployable query outputs tailored to SOC requirements.

- *Structured Instruction Generation*: The process begins with QUERYAI generating a structured instruction set based on the SOC investigation prompt. This structured prompt guides the LLM, outlining clear parameters such as required data fields, relevant event types, specific entities (e.g., user IDs, IP addresses), and contextual filters. These instructions serve as a foundational blueprint, helping the LLM interpret the query requirements accurately and establish the investigation's objectives.
- *Structured Query Generation and Step-by-Step Reasoning*: Using the structured instruction, the LLM constructs an initial investigation query, breaking down the prompt into logical steps. This phase involves identifying and assembling the necessary building blocks—such as data fields, operators, functions, and relationships – into a coherent query flow. The LLM applies step-by-step reasoning to ensure that each component aligns with the investigation's intent, translating prompt instructions into specific SIEM operations like 'where' and 'join' clauses, and verifying that the syntax and logic adhere to SIEM standards.
- *Query Validation and Confidence-Based Refinement*: After generating the preliminary query, QUERYAI initiates a confidence-based review and refinement process. Each part of the query is evaluated for accuracy and logical consistency, with confidence scores assigned to each component. Any segments with low confidence undergo iterative refinement, where QUERYAI revisits the structured instruction and query components, making adjustments to improve performance and coherence. This feedback loop enables QUERYAI to iteratively enhance the query until it meets predefined accuracy and efficiency thresholds.
- *Final Output Generation*: Upon completing the confidence-based refinement, QUERYAI produces a finalized investigation query that is ready for SOC deployment. The resulting query is both context-aware and optimized for effective alert investigation, allowing SOC teams to quickly differentiate between false alarms and genuine threats without extensive manual input.

This structured, multi-phase approach ensures that QUERYAI provides SOC teams with precise, contextually accurate queries, streamlining alert investigation workflows and reducing dependency on manual query formulation. By incorporating step-by-step reasoning and iterative refinement, QUERYAI enables SOCs to handle alerts more effectively and respond to threats with high confidence and minimal error.

Evaluation: The evaluation of QUERYAI 's query generation will focus on accuracy, efficiency, and real-world applicability. Accuracy will be measured by comparing QUERYAI-generated queries to those created by SOC analysts, using precision and recall metrics to assess the retrieval of relevant log data without excess noise. Efficiency will be evaluated by calculating time saved in query formulation, comparing QUERYAI 's speed to that of human analysts to gauge its impact on SOC response times. To test real-world applicability, QUERYAI will be applied to SOC-like prompts using DARPA datasets [11, 10] or similar logs from controlled environments, analyzing its handling of prompts with varied complexity. We will track false positive

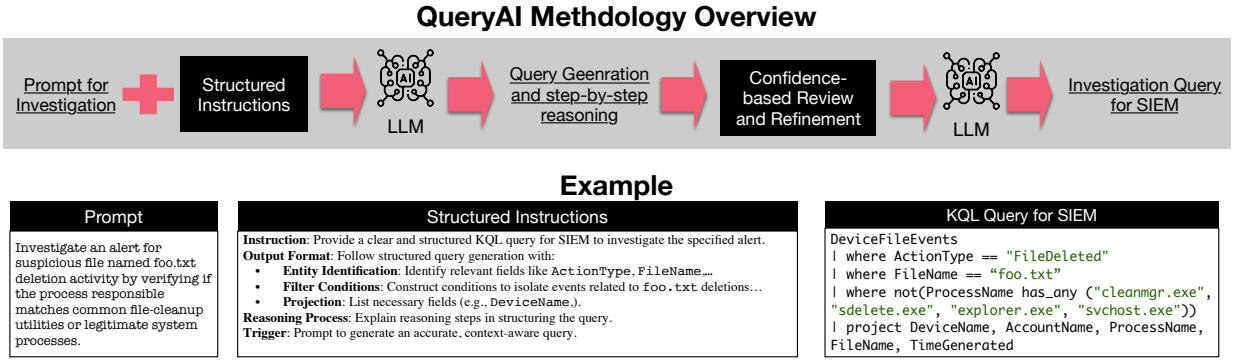

Figure 4: An in-depth illustration of the QueryAI framework for investigation. The workflow begins with structured instructions that prompt the LLM to generate a KQL query tailored to investigate suspicious file deletion activity. The process initiates with the query generation and step-by-step reasoning stage, forming the initial query structure. Each generated query undergoes a confidence-based review and refinement process, with confidence scores guiding iterative adjustments. This cycle is repeated until reaching a refined query that meets accuracy and relevance criteria.

and negative rates in incident detection to assess performance across different scenarios.

Expected Results

A Ph.D. student, under the guidance of PI Hassan at the University of Virginia, will work on this project to bridge academic research with industry needs by advancing CDR systems through scalable, decentralized threat detection and response methods tailored for cloud environments. The project's timeline is outlined in Figure 5. This research will yield several key outcomes:

- We will develop FEDDETECT, a cloud-native, decentralized detection system using FL and GNNs to process logs locally, reducing centralized data transfers. Deliverables for FEDDETECT, available by Q3 2025, include the FL-GNN integration codebase, pre-trained model weights, optimized GNN architectures, and initial datasets of benign and adversarial logs to serve as benchmarks for the cloud security community.
- We will design QUERYAI, an AI-driven SOC assistant that automates investigation query generation from SOC prompts, enhancing alert investigation. QUERYAI will leverage a pre-trained LLM and threat intelligence for context-aware query generation, enabling SOCs to investigate alerts without raw log access. The release, scheduled for Q4 2025, includes QUERYAI's codebase,and a technical report.
- Comprehensive deliverables, including curated datasets, code, model weights, and documentation, will be available by Q1 2026. Findings, methodologies, and benchmarks on scalability and accuracy will be presented at IEEE S&P, USENIX Security, and ACM CCS. We will also offer hands-on tutorials and maintain an online repository to support ongoing updates and community contributions.

Funds Needed

We request cash funding to cover personnel costs, including $60,000 for one year's salary for a graduate student (covering stipend, tuition, health insurance) and $15,000 for one month of summer salary for PI Hassan. Additionally, we seek $25,000 in AWS Promotional Credits to manage computational and storage demands using Amazon EC2 and Amazon S3. Our project involves running experiments on the p3.2xlarge instance for ML tasks at $3.06 per hour, 24 hours a day, 5 days a week, totaling $17,625.60 annually for EC2. We also require secure storage of 5 TB on Amazon S3 for storing and sharing system logs produced in Task 1, with operational costs totaling $2,580 annually. This $25,000 in AWS Promotional Credits will also accommodate potential fluctuations and unforeseen costs.

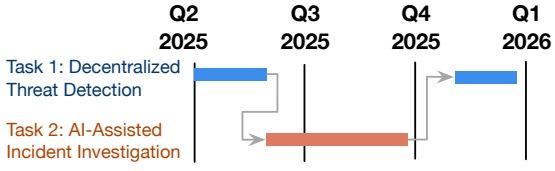

Figure 5: Anticipated timeline of the proposed work.

References

[1] B. A. Alahmadi, L. Axon, and I. Martinovic. "99% False Positives: A Qualitative Study of {SOC} Analysts' Perspectives on Security Alarms". In: *31st USENIX Security Symposium (USENIX Security 22)*. 2022, pp. 2783–2800.

[2] S. Aljawarneh, M. Aldwairi, and M. B. Yassein. "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model". In: *Journal of Computational Science* 25 (2018).

[3] *An ESG Research Insights Report*. http://pages.siemplify.co/rs/182-SXA-457/images/ESG-Research-Report.pdf.

[4] A. Bates, W. U. Hassan, K. Butler, A. Dobra, B. Reaves, P. Cable, T. Moyer, and N. Schear. "Transparent web service auditing via network provenance functions". In: *International World Wide Web Conference (WWW)*. 2017.

[5] K. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, A. Ingerman, V. Ivanov, C. Kiddon, J. Konečnỳ, S. Mazzocchi, B. McMahan, et al. "Towards federated learning at scale: System design". In: *Proceedings of machine learning and systems* 1 (2019), pp. 374–388.

[6] L. Cai, Z. Chen, C. Luo, J. Gui, J. Ni, D. Li, and H. Chen. "Structural temporal graph neural networks for anomaly detection in dynamic graphs". In: *ACM international conference on Information & Knowledge Management*. 2021.

[7] *CALDERA*. https://www.mitre.org/research/technology-transfer/open-source-software/caldera.

[8] Z. Cheng, Q. Lv, J. Liang, Y. Wang, D. Sun, T. Pasquier, and X. Han. "Kairos:: Practical Intrusion Detection and Investigation using Whole-system Provenance". In: *arXiv preprint arXiv:2308.05034* (2023).

[9] *Chronicle Detection Rules*. https://github.com/chronicle/detection-rules.

[10] *DARPA OpTC*. https://github.com/FiveDirections/OpTC-data.

[11] *DARPA TC*. https://github.com/darpa-i2o/Transparent-Computing.

[12] *Elastic Detection Rules*. https://github.com/elastic/detection-rules.

[13] W. Guo, Z. Yao, Y. Liu, L. Zhang, L. Li, T. Li, and B. Wu. "A New Federated Learning Model for Host Intrusion Detection System Under Non-IID Data". In: *IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. 2023.

[14] W. Hamilton, Z. Ying, and J. Leskovec. "Inductive representation learning on large graphs". In: *Advances in neural information processing systems* 30 (2017).

[15] W. U. Hassan, A. Bates, and D. Marino. "Tactical Provenance Analysis for Endpoint Detection and Response Systems". In: *IEEE Symposium on Security and Privacy (S&P)*. IEEE. 2020.

[16] W. U. Hassan, S. Guo, D. Li, Z. Chen, K. Jee, Z. Li, and A. Bates. "NoDoze: Combatting threat alert fatigue with automated provenance triage". In: *Network and Distributed System Security (NDSS)*. 2019.

[17] W. U. Hassan, M. Lemay, N. Aguse, A. Bates, and T. Moyer. "Towards scalable cluster auditing through grammatical inference over provenance graphs". In: *Network and Distributed System Security (NDSS)*. San Diego, CA, 2018.

[18] W. U. Hassan, D. Li, K. Jee, X. Yu, K. Zou, D. Wang, Z. Chen, Z. Li, J. Rhee, J. Gui, et al. "This is Why We Can't Cache Nice Things: Lightning-Fast Threat Hunting using Suspicion-Based Hierarchical Storage". In: *Annual Computer Security Applications Conference (ACSAC)*. 2020.

[19] W. U. Hassan, M. A. Noureddine, P. Datta, and A. Bates. "OmegaLog: High-Fidelity Attack Investigation via Transparent Multi-layer Log Analysis". In: *Network and Distributed System Security (NDSS)*. 2020.

[20] M. A. Inam, Y. Chen, A. Goyal, J. Liu, J. Mink, N. Michael, S. Gaur, A. Bates, and W. U. Hassan. "Sok: History is a vast early warning system: Auditing the provenance of system intrusions". In: *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2023, pp. 2620–2638.

[21] M. A. Inam, A. Goyal, J. Liu, J. Mink, N. Michael, S. Gaur, A. Bates, and W. U. Hassan. "FAuST: Striking a Bargain between Forensic Auditing's Security and Throughput". In: *Proceedings of the 38th Annual Computer Security Applications Conference*. 2022, pp. 813–826.

[22] M. A. Inam, W. U. Hassan, A. Ahad, A. Bates, R. Tahir, T. Xu, and F. Zaffar. "Forensic Analysis of Configuration-based Attacks". In: *NDSS*. 2022.

[23] *Infection Monkey*. https://www.akamai.com/infectionmonkey.

[24] T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith. "Federated optimization in heterogeneous networks". In: *Proceedings of Machine learning and systems* 2 (2020), pp. 429–450.

[25] W. W. Lo, S. Layeghy, M. Sarhan, M. Gallagher, and M. Portmann. "E-graphsage: A graph neural network based intrusion detection system for iot". In: *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*. IEEE. 2022.

[26] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas. "Communication-efficient learning of deep networks from decentralized data". In: *Artificial intelligence and statistics*. PMLR. 2017, pp. 1273–1282.

[27] N. Michael, J. Mink, J. Liu, S. Gaur, W. U. Hassan, and A. Bates. "On the Forensic Validity of Approximated Audit Logs". In: *ACSAC*. 2020.

[28] *Microsoft Copilot for Security (6 months later)*. https://thecloudtechnologist.com/2024/10/04/microsoft-copilot-for-security-6-months-later/.

[29] S. Ouyang, Z. Zhang, B. Yan, X. Liu, Y. Choi, J. Han, and L. Qin. "Structured chemistry reasoning with large language models". In: *arXiv preprint arXiv:2311.09656* (2023).

[30] R. Paccagnella, P. Datta, W. U. Hassan, A. Bates, C. Fletcher, A. Miller, and D. Tian. "Custos: Practical tamper-evident auditing of operating systems using trusted execution". In: *Network and distributed system security symposium*. 2020.

[31] M. U. Rehman, H. Ahmadi, and W. U. Hassan. "FLASH: A Comprehensive Approach to Intrusion Detection via Provenance Graph Representation Learning". In: *IEEE Symposium on Security and Privacy (S&P)*. 2024.

[32] M. Simonovsky and N. Komodakis. "Graphvae: Towards generation of small graphs using variational autoencoders". In: *Artificial Neural Networks and Machine Learning–ICANN*. Springer. 2018.

[33] S. Tang, B. Li, and H. Yu. "ChebNet: Efficient and stable constructions of deep neural networks with rectified power units using chebyshev approximations". In: *arXiv preprint arXiv:1911.05467* (2019).

[34] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, Ł. Kaiser, and I. Polosukhin. "Attention is all you need". In: *Advances in neural information processing systems* 30 (2017).

[35] P. Veličković, G. Cucurull, A. Casanova, A. Romero, P. Lio, and Y. Bengio. "Graph attention networks". In: *arXiv preprint arXiv:1710.10903* (2017).

[36] Q. Wang, W. U. Hassan, A. Bates, and C. Gunter. "Fear and Logging in the Internet of Things". In: *Network and Distributed System Security (NDSS)*. 2018.

[37] Q. Wang, W. U. Hassan, D. Li, K. Jee, X. Yu, K. Zou, J. Rhee, Z. Chen, W. Cheng, C. A. Gunter, et al. "You Are What You Do: Hunting Stealthy Malware via Data Provenance Analysis." In: *Network and Distributed System Security (NDSS)*. 2020.

[38] F. Yang, J. Xu, C. Xiong, Z. Li, and K. Zhang. "PROGRAPHER: An Anomaly Detection System based on Provenance Graph Embedding". In: (2023).

[39] S. Ye, L. Zeng, Q. Wu, K. Luo, Q. Fang, and X. Chen. "Eco-fl: Adaptive federated learning with efficient edge collaborative pipeline training". In: *Proceedings of the 51st International Conference on Parallel Processing*. 2022, pp. 1–11.

[40] J. You, R. Ying, X. Ren, W. Hamilton, and J. Leskovec. "Graphrnn: Generating realistic graphs with deep auto-regressive models". In: *International conference on machine learning*. PMLR. 2018, pp. 5708–5717.

[41] B. Yu, H. Yin, and Z. Zhu. "Spatio-temporal graph convolutional networks: A deep learning framework for traffic forecasting". In: *arXiv preprint arXiv:1709.04875* (2017).

[42] Y. Zhao, M. Li, L. Lai, N. Suda, D. Civin, and V. Chandra. "Federated learning with non-iid data". In: *arXiv preprint arXiv:1806.00582* (2018).

Wajih Ul Hassan

+1 217-904-5884 • hassan@virginia.edu • www.cs.virginia.edu/~hur7wv/
wajihulhassan • Lab Website: dartlab.org

Research Interests

System Security, Threat Detection, Forensic Investigation, and Data Provenance

Current Professional Appointment

The University of Virginia (UVA) **USA**
Tenure-Track Assistant Professor *August 2022 – Present*
Department of Computer Science and School of Data Science

Education

University of Illinois at Urbana-Champaign (UIUC), USA
Ph.D., Computer Science *2015 – 2021*
Advisor: Dr. Adam Bates.
Thesis: Investigating System Intrusions with Data Provenance Analytics

Lahore University of Management Sciences (LUMS), Pakistan
Bachelor of Science, Computer Science *2011 – 2015*

Selected Awards & Honors

- NSF CAREER Award 2024-2029
- Weaver Faculty Fellowship, UVA 2022-2025

Selected Publications

[1] Mati Ur Rehman, Hadi Ahmadi, and Wajih Ul Hassan. "FLASH: A Comprehensive Approach to Intrusion Detection via Provenance Graph Representation Learning". In: *IEEE Symposium on Security and Privacy (S&P)*. Acceptance Rate: 17.8%. 2024.

[2] Muhammad Adil Inam, Yinfang Chen, Akul Goyal, Jason Liu, Jaron Mink, Noor Michael, Sneha Gaur, Adam Bates, and Wajih Ul Hassan. "SoK: History is a Vast Early Warning System: Auditing the Provenance of System Intrusions". In: *IEEE Symposium on Security and Privacy (S&P)*. Acceptance Rate: 17.1%. 2023.

[3] Wajih Ul Hassan, Adam Bates, and Daniel Marino. "Tactical Provenance Analysis for Endpoint Detection and Response Systems". In: *IEEE Symposium on Security and Privacy (S&P)*. Acceptance Rate: 12.3%. 2020.

[4] Qi Wang, Wajih Ul Hassan, Ding Li, Kangkook Jee, Xiao Yu, Kexuan Zou, Junghwan Rhee, Zhengzhang Chen, Wei Cheng, Carl A Gunter, et al. "You Are What You Do: Hunting Stealthy Malware via Data Provenance Analysis." In: *Symposium on Network and Distributed System Security (NDSS)*. Acceptance Rate: 17.4%. 2020.

[5] Wajih Ul Hassan, Shengjian Guo, Ding Li, Zhengzhang Chen, Kangkook Jee, Zhichun Li, and Adam Bates. "NoDoze: Combatting threat alert fatigue with automated provenance triage". In: *Symposium on Network and Distributed System Security (NDSS)*. Acceptance Rate: 17%. 2019.

[6] Wajih Ul Hassan, Mark Lemay, Nuraini Aguse, Adam Bates, and Thomas Moyer. "Towards scalable cluster auditing through grammatical inference over provenance graphs". In: *Symposium on Network and Distributed System Security (NDSS)*. Acceptance Rate: 21.5%. 2018.

Previously Funded Project Summary

PI Hassan has not previously received cash funding or AWS Promotional Credits directly or indirectly from Amazon.