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

Abstract

To safeguard against Advanced Persistent Threats (APTs), enterprises increasingly rely on Intrusion Detection Systems (IDS). These systems utilize system monitoring logs to detect and respond to threats. However, the common practice of centrally managing these logs, which contain sensitive data such as IP addresses and file activities, raises privacy concerns, especially when Managed Security Service Providers (MSSPs) are involved. These third parties, which offer intrusion detection services, may inadvertently breach user privacy when analyzing these sensitive logs on central servers located in the cloud.

The central research question guiding this grant proposal is: *How can Federated Learning (FL) and Graph Neural Networks (GNNs) be integrated to develop an IDS that ensures robust threat detection and incident response while prioritizing privacy and scalability?* To address this question, the proposal outlines three research objectives (ROs): **RO1:** Create APTLab, a testbed that generates system logs related to real-world APT attacks along with benign activities representative of large enterprises. These logs will facilitate rigorous IDS testing and will be shared with the research community to advance intrusion detection research. **RO2:** Design and implement FedDetect, a decentralized detection system using FL and GNNs. FL enables the computation of a global threat detection model across distributed clients while keeping data localized, thus enhancing privacy. Concurrently, GNNs, applied to provenance graphs, which are structured representations that trace the origins and historical changes of data within system logs, enable detailed analysis of logs to identify both stealthy and malicious behaviors. **RO3:** Design PrivIR, a framework for secure and private incident response. Leveraging cryptographic techniques, this objective aims to enable security teams to verify and respond to threats without accessing raw, sensitive system logs.

Keywords: Threat and Intrusion Detection; Cloud Security; Data Privacy; Graph Neural Networks

Introduction

Intrusion Detection Systems (IDS) are essential for enterprise security, analyzing system logs to detect malicious activities. Signature-based IDS [13, 8] use known threat patterns to match against system logs for detection but are limited to identifying established threats. In contrast, anomaly-based IDS [2, 4] detect deviations from normal behavior, enabling them to identify novel or evolving threats. A significant development in this area is Provenance-based IDS (PIDS) [33, 28, 7], which enhance detection capabilities by utilizing detailed contextual information from logs to construct data provenance graphs. These graphs, exemplified in Figure 1 where a Firefox process downloads a malicious PDF file, are analyzed with machine learning techniques to discern patterns of benign activity and identify deviations signaling potential threats.

Figure 1: An example provenance graph showcasing the downloading of a malicious file. Diamonds, rectangles, and ovals depict sockets, processes, and files respectively.

Unfortunately, traditional IDS, including PIDS, face privacy issues due to their reliance on centralized log storage and processing, which often contain sensitive data such as URLs visited by employees, posing significant privacy and data leakage risks. Additionally, IDS alert validation generally requires manual analysis by Security Operation Center (SOC) teams to provide context and differentiate between false alarms and true positives. Concurrently, the emergence of Managed Security Service Providers (MSSPs) marks a significant shift in enterprise security strategies. MSSPs, which are external organizations managing the security of client businesses, handle the collection, storage, and analysis of sensitive logs in the cloud for intrusion detection and response. Recent data shows that 70% of businesses plan to engage MSSPs soon [1], attracted by the model's cost-effectiveness and efficiency. However, this model requires processing sensitive data from multiple enterprises in shared environments, greatly increasing the risk of data breaches [25]. Figure 2 depicts the operational architecture of MSSPs.

Given these privacy and efficiency challenges, the need for a privacy-preserving IDS is more pressing than ever. Federated Learning (FL) offers a viable solution by allowing decentralized machine learning models to be trained on distributed data sources without sharing raw data. When applied to intrusion detection, FL leverages the collective intelligence of multiple hosts within an enterprise, enhancing individual data privacy. This approach is particularly beneficial in MSSP scenarios, where it processes data from various organizations without compromising privacy. Moreover, FL significantly improves scalability and reduces network overhead compared to traditional IDS [6, 32].

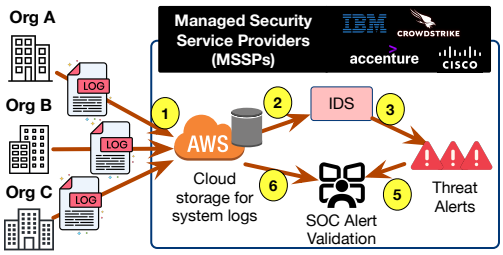

Figure 2: Overall MSSP architecture. The plain-text logs are first collected in a centralized storage. Then these logs are analyzed for intrusion detection and alert investigation

However, integrating FL into IDS presents multiple challenges. Model aggregation in a federated setting becomes complex due to the heterogeneous data distributions from clients running different applications, often leading to suboptimal performance of the unified model [3]. Furthermore, data imbalances, where smaller data contributors have less impact on the federated model, skew the learning outcomes [14, 35]. Another significant challenge is the inconsistent semantic information produced by independently trained semantic models, such as Word2vec across different client machines. This inconsistency can reduce the effectiveness of global detection models, resulting in inaccurate representations of system behavior due to varied feature vector qualities [28].

The proposal introduces a comprehensive approach to enterprise security, focusing on privacy-preserving threat detection and accurate incident response, with the goal of transforming how intrusion detection systems manage data privacy. The overarching workflow of our proposed IDS is illustrated in Figure 3. *The main idea that sets this proposal apart from prior efforts is the novel adaptation of Federated Learning (FL) and Graph Neural Networks (GNNs) to PIDS.* This strategy enables decentralized training of machine learning models using system logs from multiple hosts without the need to share raw data. GNNs are especially effective at analyzing complex structural and temporal data interactions. When applied to provenance graphs, they generate expressive, semantically-rich node embeddings, which facilitate the construction of robust models capable of detecting subtle, anomalous behaviors across an enterprise's network.

The project focuses on three primary activities. First, we aim to develop a comprehensive provenance testbed, referred to as APTLab, to refine detection algorithms and evaluate IDS (Task 1). Second, we will design FedDetect, a privacy-aware intrusion detection system that utilizes federated graph learning to boost detection capabilities while ensuring data privacy (Task 2). Third, we plan to implement PrivIR, a privacy-preserving incident response framework that will empower SOC teams to validate alerts without needing access to raw system logs (Task 3). If successful, this project will significantly enhance enterprise security by improving how intrusion detection systems manage privacy and scalability. By enhancing the privacy of sensitive system logs and minimizing reliance on centralized log storage for threat detection, the project aims to establish new standards for compliance with global data protection regulations. Furthermore, sharing the attack and benign datasets generated from this project will foster greater collaboration within the intrusion detection community, enhancing defensive and responsive strategies.

PI Qualifications: PI Hassan is a leader in the area of provenance-based system auditing and threat detection. He has designed systems that can collect audit logs from large-scale systems in storage- and network-efficient manner [19, 21], accurately identify stealthy threats using graph-powered machine learning [31, 16, 28], and efficiently reduce the size of system logs and summarize long-lived attack campaigns [16, 20, 22, 17]. His credentials also include designing privacy-preserving techniques for fitness tracking applications [18], two patents in the security field and practical industry experience.

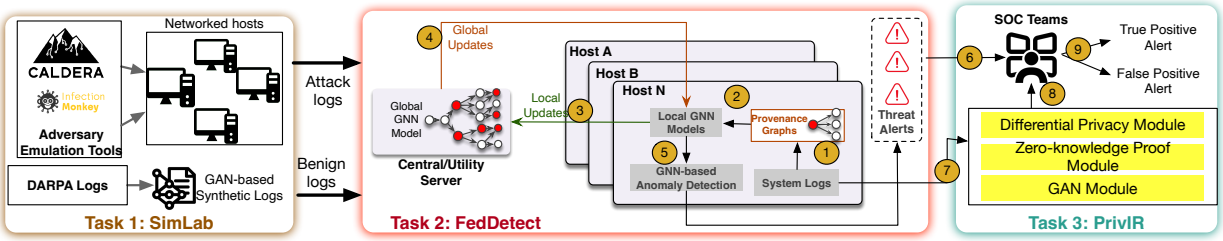

Figure 3: Workflow of our proposed privacy-aware intrusion detector and incident response framework.

Research Methods

Task 1. *(APTLab: Development of a Comprehensive APT Testbed for IDS Evaluation)*

The current landscape of IDS evaluation suffers from a lack of representative datasets that include both benign and malicious activities. Notably, there is a particular scarcity of benign system logs, which are critical for developing realistic models of normal enterprise behavior. Although existing datasets, such as DARPA TC [9, 10], provide valuable insights with their portrayal of both benign activities and APT attack campaigns, the dynamic nature of cybersecurity means that these static datasets quickly become outdated.

To effectively address the above-mentioned issue, we plan to systematically generate both malicious and benign datasets using advanced simulation and deep learning techniques. For the malicious dataset, we intend to utilize the MITRE Caldera tool [5] and Infection Monkey [23]. These tools are specifically designed to replicate a wide range of Advanced Persistent Threat (APT) scenarios. MITRE Caldera is an adversary emulation system that models complex attack patterns and adapts to various defensive strategies, making it a robust choice for creating realistic and challenging environments for IDS testing. Infection Monkey complements this by providing automated testing across diverse network topologies, ensuring that our simulations cover a comprehensive array of attack vectors and system vulnerabilities. For the benign dataset, we will deploy Generative Adversarial Networks (GANs), particularly those tailored for graph data structures. GANs, such as GraphRNN [34] and GraphVAE [29], are robust at capturing the complex distributions of benign activity logs. These networks learn to mimic the inherent patterns and temporal dynamics found in enterprise system logs, resulting in highly realistic and varied synthetic graphs. GraphRNN, for instance, uses a sequential approach to generate graphs with accurate topological structures, while GraphVAE handles variational autoencoding to produce dense representations suitable for intricate graph behaviors. These methods ensure that our synthetic graphs, representing benign system logs, are not only diverse but also retain essential log characteristics critical for effective IDS evaluation.

Evaluation: We plan to create a state-of-the-art testbed to validate our proposed IDS, which will also serve as a reference for public sharing with researchers. To ensure the datasets' accuracy and completeness, we will conduct comparisons against established benchmarks, such as DARPA datasets [10, 9], verifying that our synthetic attack logs and benign graphs accurately reflect current threat scenarios. Our evaluation will include cross-validation to test generalizability across different networks, and statistical analysis to ensure data fidelity in capturing essential temporal and causal relationships. œ

Task 2. *(FedDetect: Leveraging Federated Graph Learning for Privacy-Aware Intrusion Detection)*

Our primary goal in FedDetect is to develop a robust IDS framework using provenance graphs within a FL paradigm. We aim to deploy GNNs to extract expressive node embeddings from these graphs, creating an accurate and scalable IDS. PI Hassan has previously implemented GNNs on provenance graphs to construct effective an IDS system [28]; however, this system has encountered issues with privacy leakage. Additionally, feature space heterogeneity from independent local training leads to inconsistent input encoding, complicating the training process. Moreover, the computational intensity of GNN architectures can result in slow processing times, especially when scaling to handle large enterprise datasets.

To effectively tackle these issues, we plan to implement a multi-tiered strategic approach. Initially, we

will develop an ensemble learning framework where each submodel is tailored to specific process entities, standardized across all clients through a sophisticated categorization scheme. This categorization, facilitated by a dual-server architecture, organizes process entities into privacy-preserving bins. Clients will align their process node types with these bins, build provenance subgraphs for each, and train individual GNNs on these graphs. Subsequently, the models from all clients will be aggregated into model pairs, creating a comprehensive global ensemble model set that maintains the integrity of unique activity patterns across varied client environments.

To address feature space heterogeneity, we will introduce a Word2Vec harmonization scheme utilizing our dual-server architecture. A central server will distribute encryption keys to clients, enabling them to securely encode Word2Vec tokens. A utility server will then process these encrypted tokens to create a unified, privacy-preserving vector representation, ensuring data protection while allowing for accurate and consistent semantic encoding across different clients. Furthermore, to mitigate the processing delays inherent in traditional GNN models, we will explore the adoption of more efficient GNN architectures like GraphSAGE [15], which supports inductive learning, and ChebNet [30], which extends convolution operations across graph data, thereby enhancing processing speed and overall system scalability.

Furthermore, to combat feature space heterogeneity, we will implement a Word2Vec harmonization scheme using a dual-server architecture. A central server will issue encryption keys to clients, allowing them to securely encode Word2Vec tokens. A utility server will then process these encrypted tokens to achieve a unified, privacy-preserving vector representation. This method will ensure that sensitive data remains protected while facilitating accurate and consistent semantic encoding across different clients. To address the slow processing times associated with GNN architectures, we will explore the use of more efficient GNN models, such as GraphSAGE [15], which enables inductive learning, and ChebNet [30], which generalizes convolution operations over graph data, thus improving processing speed and scalability.

Evaluation: To evaluate scalability, we will test the system under varying loads by incrementally increasing the number of client nodes and data volume, measuring performance using metrics such as throughput, latency, and resource utilization (CPU and memory usage) across diverse network environments. For privacy assessment, we will simulate potential inference attacks to evaluate the system's ability to prevent information leakage, using key metrics like the success rate of these attacks and the integrity of post-processing data, focusing on potential data reconstruction capabilities. Further, we will assess the effectiveness of our harmonization techniques to ensure that sensitive features remain unintelligible to the central and utility servers. For datasets, we will utilize DARPA datasets [10, 9] along with datasets generated in Task 1.

Task 3. *(PrivIR: Designing Privacy-preserving Alert Validation and Investigation Framework)*

To enhance the privacy of alert validations by SOCs, we propose integrating synthetic data generation with advanced cryptographic techniques. When a threat alert such as a keylogger activation is generated by an IDS, SOCs traditionally analyze raw system logs for historical context, as shown in Figure 1. To mitigate privacy risks associated with transmitting raw logs to a central server, we will utilize Generative Adversarial Networks (GANs) [26] to synthesize datasets. These GANs are designed to replicate the behavioral patterns found in original system logs while anonymizing sensitive details like IP addresses and user identifiers.

Additionally, we will employ Zero-Knowledge Proofs (ZKPs) [11], specifically zk-SNARKs [27], to allow SOC teams to verify incidents like unauthorized software executions or multiple failed login attempts from a specific IP without needing to access or reveal actual data. For instance, a ZKP could confirm the occurrence of a keylogger download from an IP address without disclosing the address itself or other sensitive details linked to it. This method ensures that the validation process maintains user privacy.

Further improving our approach, we will integrate Differential Privacy (DP) techniques [24, 12] to refine our analysis and feedback mechanisms. By adding Laplacian noise to aggregated data, we can offer SOC teams insightful trends and anomaly reports that cannot be traced back to specific data points, thereby protecting individual privacy. An example could be the analysis of login patterns to detect brute force attacks,

providing insights without revealing specific user information or precise timestamps. This comprehensive strategy not only secures privacy but also enhances the robustness of threat detection and response protocols.

Evaluation: We will compare the accuracy of synthetic data to real datasets to verify behavioral fidelity, ensuring that our synthetic logs accurately mimic true user behavior. The performance of ZKPs will be assessed by evaluating their computational efficiency and the robustness of their privacy protection against various inference attacks. Additionally, we will evaluate our DP techniques by measuring how well they maintain data utility while ensuring privacy, particularly focusing on the impact of added noise on the accuracy of security insights. These evaluations will be carried out through DARPA datasets [10, 9] and the datasets generated in Task 1.

Expected Results

This research is poised to significantly enhance IDS with a strong focus on log privacy. In Task 1, we aim to develop APTLab, an advanced adversary emulation lab that accurately reflects modern host-level threats across diverse enterprise environments. This lab will leverage existing emulation tools to simulate a wide range of APT attacks, producing datasets of system logs that capture these scenarios. Importantly, we will also release datasets of benign logs, which are essential for developing systems that can distinguish between normal activities and actual threats. These datasets will be invaluable to the research community, facilitating the development, testing, and benchmarking of IDS technologies and will be publicly released to further this goal. Task 2 is focused on creating a deployable IDS that incorporates novel federated learning applied to provenance graphs, designed to enhance privacy by ensuring rapid and secure multi-host learning with minimal exposure of sensitive data. Additionally, we plan to develop and implement new GNN architectures specifically designed to handle the complexities of heterogeneous data found in provenance graphs. In Task 3, our goal is to establish a robust framework for privacy-preserving incident response. This framework will utilize advanced cryptographic techniques to enable SOC teams to validate threat alerts without accessing raw system logs, thus ensuring that the validation process does not compromise sensitive data. Further, we will submit papers detailing our findings and methodologies to top security and systems conferences.

Figure 4 shows a timeline for this proposal. Overall, the project will be led by a Ph.D. student at the University of Virginia under PI Hassan's supervision. The expected outcomes are set to redefine IDS standards in efficiency and privacy and provide a robust training platform for the student. Participation in research-based internships will enhance the student's industry experience, amplifying the impact of our research on real-world systems.

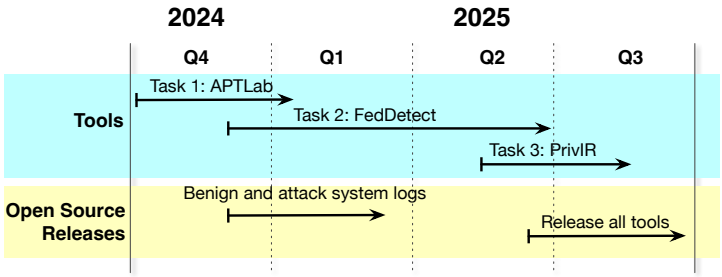

Figure 4: The anticipated timeline of the proposed work.

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.

References

[1] *70% of Organizations Will Use MSSPs*. https://www.msspalert.com/cybersecurity-research/70-of-organizations-will-use-mssps-for-outsourced-security-in-next-12-months-study-finds/.

[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] 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.

[4] 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: *Proceedings of the 30th ACM international conference on Information & Knowledge Management*. 2021.

[5] *CALDERA*. https://caldera.mitre.org/.

[6] R. B. Chaabene, D. Ameyed, F. Jaafer, A. Roger, A. Esma, and M. Cheriet. "A privacy-preserving federated learning for IoT intrusion detection system". In: *2023 9th International Conference on Control, Decision and Information Technologies (CoDIT)*. IEEE. 2023, pp. 351–356.

[7] 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).

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

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

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

[11] A. De Santis, S. Micali, and G. Persiano. "Non-interactive zero-knowledge proof systems". In: *Advances in Cryptology—CRYPTO'87: Proceedings 7*. Springer. 1988, pp. 52–72.

[12] C. Dwork. "Differential privacy". In: *International colloquium on automata, languages, and programming*. Springer. 2006, pp. 1–12.

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

[14] 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: *2023 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. IEEE. 2023, pp. 494–500.

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

[16] 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.

[17] 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.

[18] W. U. Hassan, S. Hussain, and A. Bates. "Analysis of Privacy Protections in Fitness Tracking Social Networks -or- You can run, but can you hide?" In: *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 497–512. ISBN: 978-1-939133-04-5. URL: https://www.usenix.org/conference/usenixsecurity18/presentation/hassan.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

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

[24] L. Mokry, P. Slife, P. Bishop, J. Quiroz, C. Guzzi, Z. Chen, A. Crainiceanu, and D. Needham. "Efficient and privacy-preserving collaborative intrusion detection using additive secret sharing and differential privacy". In: *IEEE Big Data*. 2021.

[25] *MSSPs Among Hardest Hit by Cyberattacks Targeting*. https://www.msspalert.com/cybersecurity-research/mssps-among-hardest-hit-by-cyberattacks-targeting-backup-vulnerabilities/.

[26] Z. Pan, W. Yu, X. Yi, A. Khan, F. Yuan, and Y. Zheng. "Recent progress on generative adversarial networks (GANs): A survey". In: *IEEE access* 7 (2019), pp. 36322–36333.

[27] A. M. Pinto. "An introduction to the use of zk-SNARKs in blockchains". In: *Mathematical Research for Blockchain Economy: 1st International Conference MARBLE 2019, Santorini, Greece*. Springer. 2020, pp. 233–249.

[28] 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.

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

[30] 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).

[31] 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.

[32] C. Wu, F. Wu, L. Lyu, T. Qi, Y. Huang, and X. Xie. "A federated graph neural network framework for privacy-preserving personalization". In: *Nature Communications* 13.1 (2022), p. 3091.

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

[34] 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.

[35] 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, Auditing, Threat Detection, 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.