November 5, 2025

Faculty Search Committee
Department of Electrical and Computer Engineering
Iowa State University

Dear Faculty Search Committee Members:

Please accept my application for the **tenure-track Assistant Professor position in Cybersecurity** in the College of Computing at **Michigan Technological University**. I am a Ph.D. candidate in the School of Computing at Clemson University, and my research spans **Security & Privacy compliance in IoT/app ecosystems** and using **Large Language Models and Vision-Language Models for security defenses**. I am currently pursuing my Ph.D. in the School of Computing at Clemson University, and I expect to complete my Ph.D. dissertation by Aug 2026. I am very excited to submit my application with the potential of joining your well known college with excellent researchers and education programs.

Over the past three years, my research has made important contributions to the following broad areas: policy compliance, usable privacy in voice/mobile ecosystems, Internet of Things, Computer network, AI-for-security with LLMs/VLMs, privacy-preserving, and security and privacy in cyber-physical/connected systems. My research results have led to **18 peer-reviewed publications** in venues such as WWW, NDSS, USENIX Security, UbiComp/IMWUT, and IEEE TDSC, along with one **co-authored book chapter** on AI for Zero Trust. I also have mentoring experience and have built labs for students. I received the prestigious Talford Endowed Fellowship from Clemson University in 2022 and 2023. Throughout my academic journey, I have gained independent research experience, along with collaborations with multiple universities, and proposal-writing experience, and I am confident that my background and research record will make me a valuable asset to the university.

I am drawn to Michigan Tech because its R1 profile within the College of Computing, which is an ideal home for my passion towards research and take my professional career to a higher level. I see immediate collaboration with Professor Bo Chen, whose work in AI and systems security aligns with my audits of real apps and connected systems. I am also excited to bring a new research area to the College of Computing on large-scale policy compliance measurement for open ecosystems and the digital safety of children. I would be really honored to plant long-term roots at Michigan Tech and become part of the outstanding faculty department.

My application includes a CV, Research Statement, and Teaching Statement. I would be delighted to provide any additional materials upon request. The best way to reach me is at mshujaa@clemson.edu or by cellphone at 864-765-4323.

Thanks in advance for your consideration!

Sincerely,
Mohammed Aldeen
Ph.D. Candidate, School of Computing
Clemson University, SC, USA

MOHAMMED SHUJAA ALDEEN

mshujaa@clemson.edu

School of Computing, Clemson University, Clemson, SC |

Education

Clemson University, Clemson, SC *Aug 2022 – Present*

- *Ph.D. Candidate in Computer Science*
- **Advisor:** Dr. Long Cheng

University of Jinan, China *Sep 2019 – Jun 2022*

- *M.S. in Computer Science and Technology*
- **Advisor:** Dr. Chuan Zhao

Zhejiang University of Technology, China *Sep 2015 – Jun 2019*

- *B.E.in Electrical Engineering and Automation*

Publications

1. J. Anderson, **M. Aldeen**, S. Zhang, S. Liao, H. Hu, M. Chowdhury, and L. Cheng, "Zero Trust Security – Technologies, Applications, and Adoption Challenges," EAI International Conference on Security and Privacy in Cyber-Physical Systems and Smart Vehicles, ***(SmartSP 2025)***.
2. A. York, **M. Aldeen**, J. Yan, P. Silimkhan, S. Liao, M. D. Pesé, and L. Cheng, "A First Look at Privacy Compliance of Zoom Apps," IEEE Secure Development Conference, ***(SecDev 2025)***.
3. J. Ma, **M. S. Aldeen**, F. Luo, and L. Cheng, "Few-Shot Detection of Hate Videos Using Multi-Modal Large Language Models," in *Proceedings of the 1st ACM Workshop on Deepfake, Deception, and Disinformation Security*, October 2025, pp. 32–35. (**3D-Sec 2025**)
4. J. Yan, S. Liao, J. Ma, **M. Aldeen**, S. Kumar, and L. Cheng, "No Way to Sign Out? Unpacking {Non-Compliance} with Google Play's App Account Deletion Requirements," in *34th USENIX Security Symposium*, 2025, pp. 3277–3296. **(USENIX Security 2025)**
5. J. Yan, S. Liao, **M. Aldeen**, L. Xing, D. D. Yao, L. Cheng, and V. Tech, "SKILLPOV: Towards Accessible and Effective Privacy Notice for Amazon Alexa Skills," in *Network and Distributed System Security Symposium* **(NDSS 2025)**.
6. S. Zhang, **M. Aldeen**, S. Liao, J. Young, and L. Cheng, "AcousticScope: Understanding Biases in Voice Interaction via Automated Acoustic Testing," In *International Conference on Security and Privacy in Cyber-Physical Systems and Smart Vehicles*, November 2024, pp. 26–53. Cham: Springer Nature Switzerland **(SmartSP 2024)**.
7. **M. Aldeen**, J. Young, S. Liao, T. Chang, L. Cheng, H. Cai, and H. Hu, "End-Users Know Best: Identifying Undesired Behavior of Alexa Skills Through User Review Analysis," Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, vol. 8, no. 3, article 89, September 2024, doi: 10.1145/3678517 **(Ubicomp 2024)**.
8. **M. Aldeen**, C. Zhao, Z. Chen, L. Fang, and Z. Liu, "Privacy-Preserving Collaborative Learning for Genome Analysis via Secure XGBoost," IEEE Transactions on Dependable and Secure Computing, 2024 **(TDSC 2024)**.
9. S. Liao, **M. Aldeen**, J. Yan, L. Cheng, X. Luo, H. Cai, and H. Hu, "Understanding GDPR Non-Compliance in Privacy Policies of Alexa Skills in European Marketplaces," Proceedings of the ACM on Web Conference, pp. 1081–1091 **(WWW 2024)**.
10. **M. Aldeen**, P. MohajerAnsari, J. Ma, M. Chowdhury, L. Cheng, and M.D. Pesé, "An Initial Exploration of Employing Large Multimodal Models in Defending Against Autonomous Vehicles Attacks," in IEEE Intelligent Vehicles Symposium, June 2024, pp. 3334–3341. IEEE **(IV 2024)**.
11. **M. Aldeen**, P. MohajerAnsari, J. Ma, M. Chowdhury, L. Cheng, and M.D. Pesé, "WIP: A First Look at Employing Large Multimodal Models Against Autonomous Vehicle Attacks," in ISOC Symposium on Vehicle Security and Privacy **(VehicleSec 2024)**.

12. **M. Aldeen**, P. Silimkhan, E. Anderson, T. Kavuru, T.Y. Chang, J. Ma, F. Luo, H. Hu, and L. Cheng, “An Integrated Platform for Online Abuse Research," in 5th International Workshop on Cyber Social Threats **(CySoc 2024)**.
13. **M. Aldeen**, S. Liang, Z. Zhang, L. Guo, Z. Song, and L. Cheng, “EMMasker: EM Obfuscation Against Website Fingerprinting," in Workshop on Measurements, Attacks, and Defenses for the Web **(MADWeb 2024)**.
14. **M. Aldeen**, J. Luo, A. Lian, V. Zheng, A. Hong, P. Yetukuri, and L. Cheng, “ChatGPT vs. Human Annotators: A Comprehensive Analysis of ChatGPT for Text Annotation," in International Conference on Machine Learning and Applications, December 2023, pp. 602–609. IEEE **(ICMLA 2023)**.
15. H. Jia, **M. Aldeen**, S. Jing, Z. Chen, and C. Zhao, “Flexible Privacy-Preserving Machine Learning: When Searchable Encryption Meets Homomorphic Encryption," International Journal of Intelligent Systems 37.11 (2022): 9173–9191.
16. **M. Aldeen** and C. Zhao, “Rare Variants Analysis in Genetic Association Studies with Privacy Protection via Hybrid System," International Conference on Information and Communications Security, doi: 10.1007/978-3-030-88052-1_11 **(ICICS 2021)**.
17. A. Bomai, **M. Aldeen** and C. Zhao, “Privacy-Preserving GWAS Computation on Outsourced Data Encrypted under Multiple Keys Through Hybrid System," International Conference on Data Science and Advanced Analytics, doi: 10.1109/DSAA49011.2020.00078 **(DSAA 2020)**.

Under Review

1. **M. Aldeen**, J. Yan, J. Ma and L. Cheng, “Sign2Alexa: Enhancing Accessibility of Voice Personal Assistants for Deaf and Hard-of-Hearing Users”,Conference on Mobile Computing and Networking, ***UbiComp 2025***.
2. J. Ma, **M. Aldeen**, F. Luo, M. Chowdhury and L. Cheng, "DisPatch: Disarming Adversarial Patches in Object Detection with Diffusion Models", International Conference on Dependable Systems and Networks. ***DSN 2025***.
3. J. Ma, **M. Aldeen**, K. Guo, F. Luo, H. Hu, and L. Cheng, "HateShield: Employing Multi-Modal Large Language Models for Hate Video Detection", Proceedings of the ACM on Web Conference, ***WWW 2025***.
4. Y. Nong, G. Yi, **M. Aldeen**, L. Cheng, H. Hu, and H. Cai, "Assessing and Improving Prompting Large Language Models for Software Vulnerability Analysis", ACM Transactions on Software Engineering and Methodology 2025 ***SEC 2025***.
5. J. M. Tine, **M. Aldeen**, A. Enan, M. S. Salek, L. Cheng, and M. Chowdhury, “Real-World Evaluation of Protocol-Compliant Denial-of-Service Attacks on C-V2X-based Forward Collision Warning Systems,” arXiv preprint arXiv:2508.02805, 2025.

Posters

- J. Ma, A. Enan, **M. Aldeen**, and L. Cheng, Mashrur Chowdhury “Potential Risks of Asphalts Arts on the Reality of Perception System” *(SecDev 2025)*.
- **M. Aldeen**, P. Silimkhan, E. Anderson, T. Kavuru, T.Y. Chang, J. Ma, F. Luo, H. Hu, and L. Cheng, “An Integrated Platform for Online Abuse Research,” *(SecDev 2023)*.
- **M. Aldeen**, S. Liang, Z. Zhang, L. Guo, and L. Cheng, “A Defense Against EM Side-Channel Attacks on Website Fingerprinting", IEEE Secure Development Conference (SecDev), 2023.
- S. Liao, **M. Aldeen**, J. Yan and L. Cheng, “Poster: On GDPR Compliance of Amazon Alexa’s Privacy Policies in European Marketplaces”, IEEE Secure Development Conference (SecDev), 2023.

Awards

- Travel grant from NDSS (2024), VehicleSec (2024), IEEE SecDev (2023), Clemson GTG (2024)
- Talford Endowed Fellowship Award *January 2023*
- Talford Endowed Fellowship Award *August 2022*
- Fully Funded Scholarship to pursue Master’s Program from CSC *2019 – 2022*
- Outstanding Student Awards for Three Years *2015 – 2018*
- Fully Funded Scholarship to pursue Bachelor’s Program from Republic of Yemen *2014 – 2019*

Teaching Assistant

- CS 8570 Network Technologies Security *Spring 2024*
- CS 6240/4240 System Administration and Security *Spring 2023*

Mentoring Experience

- Mentored Ethan Anderson, Taran Kavuru (Clemson, undergraduate, 2023) and Parnav Silimkhan in building an Integrated Platform for Online Abuse Research (ICOAR).
- Mentored Joshua Luo (from The Westminster Schools), Ashley Lian, and Venus Zheng (from the SC Governor's School for Science and Mathematics), and Allen Hong (from D.W. Daniel High School) in 2023 to conduct a comprehensive analysis of ChatGPT's text annotation capabilities, led to publication in (ICMLA 2023)
- Mentored Arpan Bansal, MacKenna Baum, and Dalton Smith (from the SC Governor's School for Science and Mathematics, Class of 2024) in AI-Generated Text Detection: Limitations and Opportunities.
- Mentored Matthew Weathers, Cindy Qiu (from the SC Governor's School for Science and Mathematics, Class of 2024) in Understanding Users' Security and Privacy Concerns Towards VR Apps.

Paper Review

- Security and Privacy in Cyber-Physical Systems and Smart Vehicle *SmartSP 2025*
- Digital Threats: Research and Practice *DTRAP 2025*
- Transportation Research Board *TRB 2025*
- IEEE Transactions on Dependable and Secure Computing *TDSC 2025*
- Annual IEEE International Computer Software and Applications Conference *COMPSAC 2025*
- International Conference on Distributed Computing Systems *ICDCS 2025*
- SAE International *SAE 2024*
- Great Lakes Symposium on VLSI *GLSVLSI 2024*
- International Conference on Information and Communications Security *ICICS 2023*
- IEEE International Conference on Machine Learning and Applications *ICMLA 2023*
- International Conference on Computer Communications and Networks *ICCCN 2023*

Talks

- "A First Look at Privacy Compliance of Zoom Apps" in IEEE Secure Development Conference, Indianapolis, 2025.
- "An Integrated Platform for Online Abuse Research" in 5th International Workshop on Cyber Social Threats, Buffalo, 2024.
- "EMMasker: EM Obfuscation Against Website Fingerprinting" in Workshop on Measurements, Attacks, and Defenses for the Web, San Diego, 2023.
- "Rare Variants Analysis in Genetic Association Studies with Privacy Protection via Hybrid System" in International Conference on Information and Communications Security, Virtual (Chongqing, China), 2021.

Professional Service

- **Session Chair**, SecDev 2025.

Teaching for me is not an obligation, but an opportunity to work with students to to build technical skills and connect ideas to real systems, reason about security and privacy, and work in teams. Teaching and mentoring students have been my favorite parts of my academic journey because they let me share the core problem, the risks, "why" behind our methods and where they matter in the world. I also strive to ensure that CS is a place where every student feels at home, respected, encouraged, and given equal opportunities to succeed.

Teaching Philosophy: My teaching philosophy is built around three principles: explaining why each topic matters with real-world examples before teaching it, breaking materials into small chunks followed by a practice, and giving students opportunities to work on research problems alongside graduate/PhD students.

Purpose-Driven Instruction: During my mentoring experience, I noticed that when I started by having discussions about privacy and security of IoT or a system, students tend to asked more thoughtful general questions. I believe students may engage fully with technical materials if they do not understand why it matters in the first place. I like begin every topic by establishing why it matters, what real-world problem it solves, what vulnerabilities it addresses, or what system it enables. This will build solid foundation how concepts being taught are directly related to research or industry applications.

For course work, computer science field in general evolves rapidly, and newer and more robust elements are being introduced frequently. To keep my courses aligned with emerging developments, I will incorporate recent studies from top tier conferences into the course materials. Rather than just presenting them in lectures, I would structure group projects where students reproduce published results and understand why the approach work and how is that related to traditional methods. This approach helps the students to build the skills necessary to read, understand and implement robust architectures, which is essential for any computer science career.

Continues Practice: One thing I observed during my TA is that, usually students have short attention span and lose focus during long technical lectures. I structure my teaching to break concepts into smaller segments, each followed by mini-practices or questions that students work through before moving to the subsequent sections. Although this approach sound challenging and time consuming, it became more practical with modern AI tools, which would allow us to provide these practices. The goal is not just keeping students, but avoiding misconceptions before they compound. I also use anonymous surveys throughout the semester to understand what is working. Students do not always know what they need, but their feedback helps me adapt for them to receive the teaching quality for their growth.

Technical Engagement: After working with undergraduates on semester-long research projects during my PhD, several told me they learned more from that single project than from multiple courses. This is because during our research we exposed students to the full research lifecycle, where they get to read about a concept, implement it from scratch, and work through troubleshooting when things did not work. This approach not only sharpens their technical skills for industry careers, but also have the opportunity to have their names as authors/co-authors on many papers if they are considering research careers. I will create these opportunities in my teaching and encourage students to participate in workshop publications to build both their technical skills and professional portfolios.

Teaching and Mentoring Experience: During my Ph.D. program, I was a TA for three semesters for classes CPSC-8570 Network Technologies Security (graduate level) and CPSC- 6240/4240 System Administration and Security Spring (undergraduate level). I mentored 9 high school students, 4 undergraduates, 1 graduate. During the summer of 2023, 4 high school students I mentored step by step, got a paper published in ICMLA conference, with one of them went to present our work at the venue. I am pleased that two high school students from summer 2024, are pursuing studies in CS/CE at Clemson University, with one of them Arban is currently doing research in our lab about computer vision. I believe I have put in the work to be the kind of advisor I wanted to be, and I genuinely love helping students figure out their diverse talents.

Teaching Preferences I have developed my teaching skills and interests through teaching some classes, mentoring undergraduate and high school students. I am qualified to teach graduate courses on cybersecurity and networking, such as computer network, computer security principles and applied data science. I would also be glad to teach fundamental courses such as introductory programming. In addition, I would be enthusiastic to develop graduate-level seminars on emerging security research. These seminars would allow graduate students to explore a variety of state-of-the-art research projects in a specific field and help them to explore new research ideas.

My research lies on two threads: (1) Security & Privacy in IoT platforms and app ecosystems and (2) Using Large Language Models and Vision Language Models for security. On the IoT side, my research focused on security and privacy compliance in IoT ecosystems, such as detecting policy violations in voice and mobile apps, designing privacy notices that work inside constrained interfaces, and run audits to check whether these systems really follow the corresponding regulations. On the AI-for-security side, my focus was on how Large Language Models (LLM)/Vision Language Models (VLM) can serve as defensive components in deployed systems such as detecting adversarial inputs in autonomous-vehicle perception, software vulnerability discovery/repair. I also led and participated in building Integrative Cyberinfrastructure for Online Abuse Research (ICOAR) and helped in creating labs for students on cyberbully detection as part of SaTC-EDU labs.

1 Research Overview

Topic 1: Security & Privacy in IoT platforms and app ecosystems

Voice personal assistants (VPAs) such as Amazon Alexa and Google Assistant are now common in homes and workplaces. Their ecosystems have grown by opening marketplaces where third-party developers publish voice apps. Platform providers define policies those apps must follow. In my first work, published at **UbiComp'24** [**1**], I led a measurement and dynamic-testing pipeline that mines user reviews of Alexa voice apps to surface policy violations and behavior complaints. We then used a large language model to interact with Alexa and probe those complaints, identifying **228** policy-violating apps and deeper understandings on root cause of undesired behaviors. To connect "what users experience" with what the law requires, I helped as a co-author in testing European-marketplace Alexa voice apps for GDPR compliance, which was published at **WWW'24** [**2**]. In this work, we analyzed 23,927 privacy policies and testing 65,577 skills in different marketplaces and languages, we found that 67% of privacy policies fail to comply with GDPR and 95% of the skills with data collection have GDPR non-compliance issues.

Beyond compliance, when users interact with VPA, they can't view data collection disclosures, so they need to visit the voice app web page and read the privacy policy. Building on that insight, as a co-author, we proposed a short, automatically generated privacy notices delivered in voice when users interact with the Alexa, published at **NDSS'25** [**3**]. I contributed to system evaluation and user study. We also extended beyond Alexa to mobile apps, where we evaluate if the mobile apps follow Google account deletion policy, where we found that only 8.5% of sampled apps actually provided how to delete the account paths. In this work, I helped validate and annotate during the evaluation phase of our tool, in which was published at **USENIX'25** [**4**].

Topic 2: Using LLMs/VLMs as defensive components in deployed systems

In autonomous-vehicle perception, I evaluated VLMs against two attack surfaces:(i) diffusion-generated "non-signs", which are artistic images look like traffic signs but they are not, and (ii) attacks that target Automated Lane Centering (ALC) by manipulating lane-keeping inputs. we find that VLMs flag the diffusion-generated "non-signs" far more reliably than standard TSR baselines (i.e, 84.06% accuracy vs 18.67%). For ALC, it was correctly inferred the lane/action 100% of the time across lane and weather settings. This work was published as work under progress in **VehicleSec'24**[**5**] and the complete work published in **IEEE IV'24** [**6**].

In software security, we introduced vulnerability semantics guided prompting (VSP) chain-of-thought prompting approach that unifies three tasks: vulnerability identification, open-world discovery, and patch generation. Across two datasets and three LLMs, VSP outperformed five prompting baselines, improving F1 by 53.3% for identification, 36.5% for discovery, and 30.8% for patching on CVE benchmarks. As a co-author, I led the patch-generation track, where I designed the repair prompts steps, built the evaluation method, and conducted the failure analysis. Although the paper is currently under review for **SEC'25** [**7**], the arXiv preprint has already been cited nearly 70 times. Also, when ChatGPT was first released, I led a study comparing ChatGPT with human annotators across diverse datasets, this work

was conducted with help of high-school students I mentored over the summer, which later published at **ICMLA'23** [**8**].

Outside the two research topics, I led and built the Integrative Cyberinfrastructure for Online Abuse Research (ICOAR), which is targeted for researchers studying online abuse from data collection from across social media platforms to analyze cyberbully types to visualization of the results, presented at **CySo'2024** [**9**]. Also, participated in SaTC-EDU (Learning Platform and Education Curriculum for AI-Driven Socially-Relevant Cybersecurity) [**?**], where I built Lab 5 on Hateful Meme Detection.

2 Future Research Plan

In the future, I intend to leverage my expertise in policy compliance and LLM-based security systems to extend my work to a broader range of more important areas, including children's online safety in gaming ecosystems, age-inappropriate content detection, manipulative design patterns in digital platforms. I will also focus on policy adherence across emerging app marketplaces such as AI app stores, collaboration extensions (Slack, Microsoft Teams, Zoom,..., etc), and connected vehicle applications.

AI for Social Good: Detecting and Mitigating Digital Harms: The emerging sophistication of large language models and vision language models enables automated detection of complex safety threats that traditional methods fail to capture. My research will focus on developing automated systems to detect and analyze harmful design patterns in children's games, including gambling-like mechanics such as loot boxes, gacha systems, and exploitative microtransactions. Currently, I am investigating the age rating mechanics across app stores to understand why developers may provide inappropriate age rating, undermining parental trust and regulatory frameworks. Also, I will analyze whether mobile app ecosystems actually comply with the European Commission's 14 July 2025 DSA minors' guidelines, which mandate privacy and safety by design for minors accounts. I will also work on building multimodal detectors (via VLM) to analyze manipulative designs (dark patterns) common in children's apps and games including, parasocial pressure, fabricated timers, navigation constraints, and attractive lures. On top of that, we will study the parental control protection end to end by configuring controls across operating systems, workarounds to bypass the protection and measuring real outcomes. I believe this the work will have a good position for publication in top-tier security and privacy venues. The logic is reusable across different platforms, which will result in multiple publications for different platforms in short time.

Policy and Regulation Compliance of Open Platforms: Open platform now include mobile app stores, AI app stores (e.g., GPTs), and workplace marketplaces (e.g., Zoom, Slack), VR/AR apps as well as connected vehicles apps. Unlike established mobile app stores that have faced years of academic scrutiny, these new platforms lack systematic compliance measurement research. My research will focus on ensuring different third-party apps and extensions on these open platforms follow platform rules and regional regulations. This can be achieved leveraging my experience in our published works that combines static analysis, dynamic testing, fuzzing, and traffic analysis to examine the actual behaviors to compare with the claimed descriptions/privacy policy and the hosting platform policy. For example, I can examine OpenAI's GPT Store, where third-party GPTs can access user conversations without rigorous vetting, creating shadow AI risks that industry observers have identified but academic research has not systematically measured. I also plan to investigate connected vehicle applications, where vehicles generate vast location, biometric, and behavioral data shared across dealerships, insurers, and third-party app developers. While consumer privacy research and regulatory concern exist in this space, no systematic audit framework exists for third-party connected car apps comparable to mobile app compliance tools.
Funding Opportunities: I plan to pursue funding from multiple sources to support this research agenda. For AI-driven minor's safety and dark pattern detection, I will target NSF programs including SaTC, HCC/CHS, CPS as well as DOJ. For my research on platforms compliance, I will target federal agencies such as NSA, NIH, DOE, DOT, ARO, and ONR. I also plan to develop and submit education proposals to NSF SaTC EDU, IUSE, and REU Site programs.

References

[1] M. Aldeen, J. Young, S. Liao, T.-Y. Chang, L. Cheng, H. Cai, X. Luo, and H. Hu, "End-users know best: Identifying undesired behavior of alexa skills through user review analysis," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 8, no. 3, pp. 1–28, 2024.

[2] S. Liao, M. Aldeen, J. Yan, L. Cheng, X. Luo, H. Cai, and H. Hu, "Understanding gdpr non-compliance in privacy policies of alexa skills in european marketplaces," in *Proceedings of the ACM Web Conference 2024*, pp. 1081–1091, 2024.

[3] J. Yan, S. Liao, M. Aldeen, L. Xing, D. D. Yao, L. Cheng, and V. Tech, "Skillpov: Towards accessible and effective privacy notice for amazon alexa skills," 2025.

[4] J. Yan, S. Liao, J. Ma, M. Aldeen, S. Kumar, and L. Cheng, "No way to sign out? unpacking {Non-Compliance} with google play's app account deletion requirements," in *34th USENIX Security Symposium (USENIX Security 25)*, pp. 3277–3296, 2025.

[5] M. Aldeen, P. MohajerAnsari, J. Ma, M. Chowdhury, L. Cheng, and M. D. Pesé, "Wip: A first look at employing large multimodal models against autonomous vehicle attacks," in *ISOC Symposium on Vehicle Security and Privacy (VehicleSec'24)*, vol. 2, 2024.

[6] M. Aldeen, P. MohajerAnsari, J. Ma, M. Chowdhury, L. Cheng, and M. D. Pesé, "An initial exploration of employing large multimodal models in defending against autonomous vehicles attacks," in *2024 IEEE Intelligent Vehicles Symposium (IV)*, pp. 3334–3341, IEEE, 2024.

[7] Y. Nong, M. Aldeen, L. Cheng, H. Hu, F. Chen, and H. Cai, "Chain-of-thought prompting of large language models for discovering and fixing software vulnerabilities," *arXiv preprint arXiv:2402.17230*, 2024.

[8] M. Aldeen, J. Luo, A. Lian, V. Zheng, A. Hong, P. Yetukuri, and L. Cheng, "Chatgpt vs. human annotators: A comprehensive analysis of chatgpt for text annotation," in *2023 International Conference on Machine Learning and Applications (ICMLA)*, pp. 602–609, IEEE, 2023.

[9] M. Aldeen, P. Pradosh Silimkhan, E. Anderson, T. Kavuru, T.-Y. Chang, J. Ma, F. Luo, H. Hu, and L. Cheng, "All-in-one solution for online abuse research," in *International Conference on Security and Privacy in Cyber-Physical Systems and Smart Vehicles*, pp. 361–365, Springer, 2024.