Noor ul ain Ibrahim

rrrr

University of eastern finland
University Documents
Mehran University of Eng. and Technology

Document Details

Submission ID
trn:oid:::1:3133309602

Submission Date
Jan 20, 2025, 4:28 PM GMT+5

Download Date
Jan 20, 2025, 4:29 PM GMT+5

File Name
Turku-cybersecurity-Updated.pdf

File Size
74.1 KB

3 Pages

796 Words

4,685 Characters

*% detected as AI

AI detection includes the possibility of false positives. Although some text in this submission is likely AI generated, scores below the 20% threshold are not surfaced because they have a higher likelihood of false positives.

Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Frequently Asked Questions

How should I interpret Turnitin's AI writing percentage and false positives?

The percentage shown in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was either likely AI-generated text from a large-language model or likely AI-generated text that was likely revised using an AI-paraphrase tool or word spinner.

False positives (incorrectly flagging human-written text as AI-generated) are a possibility in AI models.

AI detection scores under 20%, which we do not surface in new reports, have a higher likelihood of false positives. To reduce the likelihood of misinterpretation, no score or highlights are attributed and are indicated with an asterisk in the report (*%).

The AI writing percentage should not be the sole basis to determine whether misconduct has occurred. The reviewer/instructor should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in accordance with their school's policies.

What does 'qualifying text' mean?

Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be likely AI-generated will be highlighted in cyan in the submission, and likely AI-generated and then likely AI-paraphrased will be highlighted purple.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.

Track: Cybersecurity

I am applying for the Master's Degree Program in ICT at the University of Turku, I am choosing the Cybersecurity track because it perfectly aligns with my background. I have over 6 years of experience as an ATM Engineer, where I handle the software, hardware, and networking aspects of Automated Teller Machines (ATMs). My responsibilities include ensuring robust security measures for ATMs, such as implementing secure communication protocols, encryption methods, authentication protocols, and monitoring network security measures to safeguard sensitive financial transactions. This experience has increased my understanding of cyber threats, and supported my passion for strengthening security in networked systems.

Although my current job responsibilities involve working on the network security of ATMs, I am now looking for wider-ranging opportunities in cybersecurity, particularly in I**oT security and secure communication system design**. The rapid development of IoT devices has raised significant security concerns, and I wish to contribute by providing scalable and resilient security solutions. So, my career move from ATM security to **IoT security** is a natural step for me, as both fields require expertise in network security, encryption, and threat reduction.

This Information and communication technology (ICT) program, specializing in Cybersecurity at the University of Turku provides the ideal foundation for my career transition, as it emphasises hands-on learning and real-world applications. The curriculum includes Capstone which will allow me to work on a significant cybersecurity project, applying my advanced knowledge to tackle real-world security problems. In addition to this, I am excited about the opportunity to participate in a hackathon. The Hackathon will challenge me to think critically and build innovative solutions under real-world conditions. These experiences will be extremely helpful for me to make a transition in my career. Furthermore, I am impressed by the networking events, CV clinics, and projects offered by the university that support graduates in their careers. In addition to this, the diverse student community makes the University of Turku an excellent choice for me to complete this program.

During my undergraduate studies in Electronics Engineering, I studied some of the subjects related to network security like I**ntroduction to computing**, **computer communication and networking**, and **advanced communication systems**. These subjects had the content related to security applied in different communication mediums, like both wired and wireless. After graduation, I started my career as an Engineer focusing on Automated teller machines. My relevant work experience is related to applying security measures in ATM networks. It includes implementing and managing secure communication protocols, encryption methods, authentication protocols, and ensuring robust network security to safeguard sensitive financial transactions. I am also given the responsibility of monitoring network security, discovering vulnerabilities, and installing firewalls to prevent unauthorised access to ATM systems. I conduct penetration testing to detect and resolve potential security threats. Other than all these things, I have also worked on integrating AI-based security features for fraud detection in the cheque depositor module of Interactive Teller Machines (ITM), which analyzes images of signatures done on cheques and detects any forgery committed. Furthermore, I ensure secure communication between ATMs and backend servers, working with encryption protocols and ensuring compliance with industry standards, such as ISO 8583 for financial transaction messaging.

I’m really excited about this program because it emphasizes practical learning in cybersecurity, which is what I need for my career shift. The curriculum and hands-on projects, like the Capstone, will help me develop advanced skills in networking, project management, and information and communication technology. I’m also looking forward to the Hackathon project because it will challenge me to think critically in a real-world scenario, which is essential for my growth.

What I expect from this program is to deepen my knowledge of cryptography and digital forensics, and learn how digital forensics can be used to investigate security breaches. I also want to learn more about System and Application Security and how these areas can be applied to securing IoT systems. The opportunity to explore security engineering, where I’ll design and implement secure systems, fits perfectly with my goals. Along with that, the program's theoretical courses will give me a strong foundation in both the technical and strategic sides of cybersecurity.

After graduation, I want to use the skills and knowledge I’ve gained to protect IoT systems by finding vulnerabilities and implementing strong security measures. My goal is to move from my current role as an ATM Engineer to becoming a **Cyber Security Specialist**, focusing on cryptography, digital forensics, and security engineering. I aim to investigate security incidents using digital forensics, build secure systems, conduct penetration testing on secure systems and contribute to the development of effective security measures for IoT devices. In the long term, I hope to grow into a leadership role where I can oversee security architectures and policies to ensure the safety of information across industries