PakTech Today | Pakistan's Premier Technology Magazine
Vol. 01, Issue 14 • ISSN: 3136-2729

TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

Shadow AI: The Security Risk Your Company Doesn't Know It Has

A software developer copies company code into ChatGPT to solve a problem. A marketing person puts customer information into an AI tool that is not approved. A finance manager instructs an AI chatbot to summarize notes from a meeting. They don't mean to hurt. When they do these things, they might be giving away company secrets. When the developer wants to fix the bug. He uses ChatGPT to get help. He does not think about sharing the code. So, the company needs to be careful about how it uses AI tools.

By **Hadia Zia** | University of Agriculture, Faisalabad | Published: August, 2026
hadiazia0328@gamil.com | Position: Student

Introduction

It starts in a way. An employee becomes mired in a bug. They embed a lot of internal code into ChatGPT. The problem is solved in a speedy manner within 30 seconds. That's productivity win, isn't it? Not really. The code they copied was. The code they copied was: It could contain API keys for the database, secret algorithms or even passwords. Is now on servers they cannot control. It's used to train a model they do not know. It can be viewed by individuals who they had not previously met.

Welcome to the age of Shadow AI. A decade ago, Shadow IT was all about employees using cloud apps without permission. Now Shadow AI is the use of AI tools within companies.

- It isn't controlled and isn't endorsed by anyone.
- Going at a rapid pace as a chatbot conversation.

Most companies, in Pakistan do not know that Shadow AI is already being used inside their organizations. They are unaware of Shadow AI and its usage. Shadow AI is wave.

Pakistan's tech world is indeed drastic. The freelancers in Pakistan have adapted to a culture of independence. They embrace AI tools designed for the average user. The startups in Pakistan take shortcuts and usually do not follow due process. In the meantime, they implement no data loss prevention systems. This opens the way for everything called Shadow AI. We are no longer questioning whether data leaks are happening; rather, we question to what extent. This involves tech ecosystems in Pakistan, startups, and freelance workers. The core issue is about data and how much is leaking.

> ***"Most companies in Karachi, Lahore, and Islamabad have no Shadow AI policy, no detection tools, and no employee training. That is not a gap. That is a wide-open door."***

Technology Overview

Shadow AI isn't just one thing; rather, it's a constellation of perils, many of which are not obvious. The first step toward the responsible management of Shadow AI is, therefore, understanding some of its many emergent, complex facets.

- **Pasting code into public LLMs** is very dangerous. Usually, developers normally use tools like ChatGPT, Google Bard, or Claude to make debugging faster by trying to paste source code, configuration files, and logs containing sensitive information such as passwords. The disadvantage is that data may leak permanently; anything placed in a large language model might be part of the information retained for training, security checks, or God knows, any other legal reason. Therefore, "deleted" literally does not imply that it has been obliterated from all memory. That is particularly problematic when exposing any internal documentation or even reusing passwords. Caution is required when these tools are applied. Sometimes, insouciant habits mean inadvertently disclosing sensitive information. Hence, if used occasionally, one should really ponder what code, for instance, or other sensitive information one intends to dump. It is pointless to take such information lightly. Large language models can be dangerous places, hence their naming for those savvy enough to use them.
- **These fall into the second category: unauthorized AI plugins.** Employees install browser plugins that purport to provide AI utilities for email summarization or intelligent spreadsheet support. Often, such plugins transparently request access permissions to all data on the webpage, which includes customer data, company wikis, internal emails, and management systems. The average employee clicks on "Allow" without going through the plugin privacy policy, if at all.

If employees use personal AI accounts in a business environment, it is also a major concern. Suppose an individual logs into his ChatGPT account through the corporate laptop; he transmits corporate information in an account where he is the sole owner, and there are no restrictions protecting the data from potential misuse. It is also noteworthy that the corporation does not have the right to delete the transmitted information or investigate the case. The corporation has no idea about what information has been transmitted and who has transmitted it.

Our information regarding the country can take another route. In this case, one of our staff members makes use of a computer program from an external agency to view the images and document says. The designer could be using a computer program to manipulate an image of a product that our client has not put on the market yet. It is worth noting that once we submit these documents, we lose control over them. As per the terms and conditions of the computer programs, they have the right to use the uploads to enhance their software. Consequently, the documents and images uploaded into computer programs such as the unreleased product become subject to modification through the computer program.

Lahore-based fintech startup faced a scare recently. This happened because three employees had pasted parts of the transaction processing code in ChatGPT to improve it. The issue here is that this code contained valid credentials used for testing purposes, and which remained untouched after deployment. The

company was not even aware of this issue for six months, when it came up during a third-party security audit. Fortunately, there was no evidence of any kind of data breach.

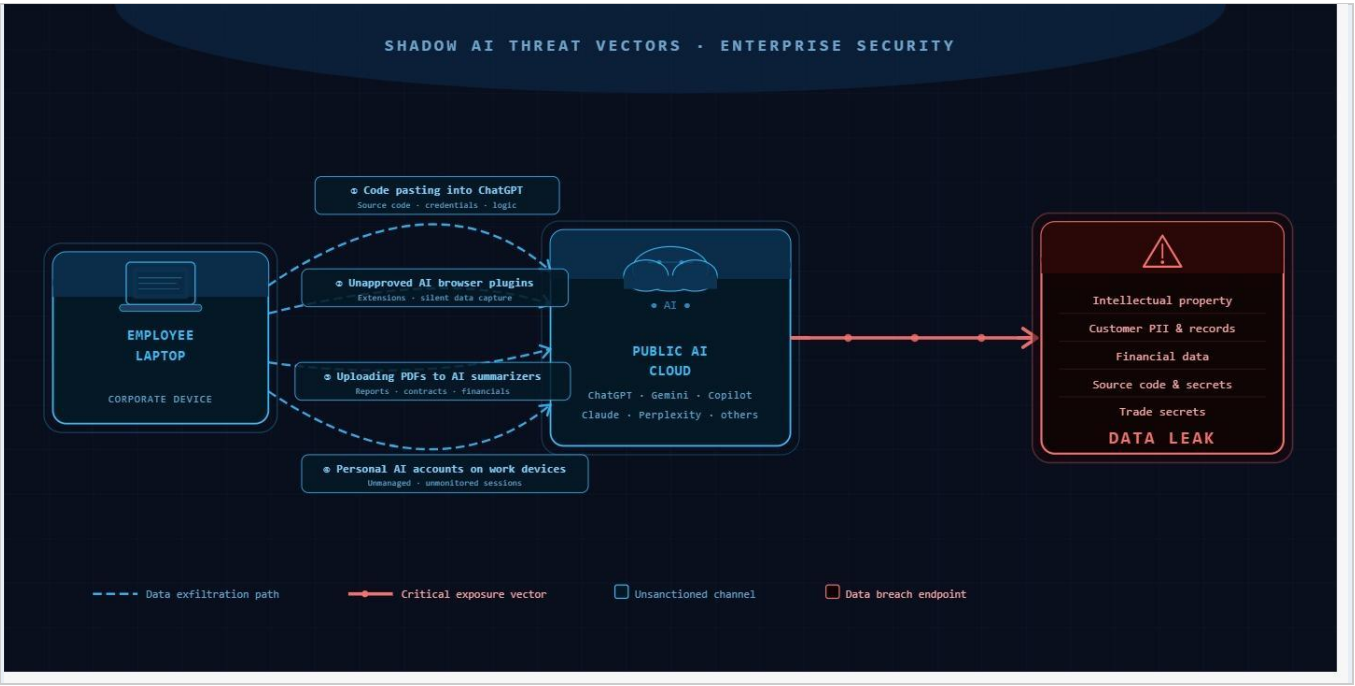

Figure 1: Shadow AI threat in enterprise security- code pasting, unproved plugins, personal AI accounts, and unsanctioned tools create data leakage pathways from employee laptops to public AI clods, resulting in exposure of IP, source code, and trade secrets.

Key Findings & Impact

The impact of Shadow AI can be broken down into four areas that often overlap: data leakage, compliance violation, intellectual property theft and reputational damage.

Data Leakage is a concern. If a worker enters customer information into a publicly available AI program, the information is no longer under the company's control. For instance, in Pakistan, if a company violates customer data, they will be penalized based on the data protection laws. Likewise, if a company provides services to its clients in Europe and violates their data, it will be fined a maximum of $20 million or four percent of its income as they have violated GDPR regulations.

Compliance violations are not about privacy. Banks and healthcare providers and fintech companies must follow rules about keeping things secret. These rules say they cannot share kinds of information with other people or companies without getting permission first. Most artificial intelligence tools that are available to the public are considered companies. If an employee uses something, like ChatGPT, to work with customer transaction data they may be breaking banking secrecy laws without realizing it. This is because ChatGPT is one of those companies that banks and other places are not supposed to share information with.

When something bad happens and people find out, the company gets a bad name. If an employee leaks customer information through an AI Chatbot, the news will spread like wildfire. Regaining lost customer trust is challenging and costly. In Pakistan, where everybody in the tech industry knows each other,

information regarding a company quickly spreads to customers and investors. The tech industry in Pakistan is like a community, so when something bad happens, everybody will know about it, and the company will be damaged.

For this reason, the Pakistani tech industry is trying to become a trusted destination for international clients to outsource their work. Shadow AI is a threat in this respect. If any known Pakistani software company leaks vital data, the reputation of all Pakistani software companies will be dented regarding the safety of data.

What's Next?

The good thing about Shadow AI is that it can be handled without hurting the work that people do or making the workplace feel like it is being watched all the time.

First, we need to find out when people use Shadow AI. We can do this by watching the network to see when people use AI tools OpenAI, Anthropic, Google Gemini, Perplexity and popular AI image generators. We can also use tools to see when people copy and paste things from important programs like code editors or customer relationship management tools. For companies we use Cloud Access security brokers to automatically stop people from passing risky things from AI tools.

Second, we need to make rules about Shadow AI. We should make a policy that says what AI tools are okay to use and what people can and cannot paste. We should make it easy for people to report if they accidentally paste something they should not have. We do not want to punish people for making mistakes.

If you oversee a tech team learn in Pakistan, you should start talking about this. You need to ask your developers some questions. Ask them, “Are you using ChatGPT for your work?” You should not get angry if they tell you the truth. Thank them for being honest. Then give them a better way to do things. You can make special company accounts for intelligence that do not save any information. You can also set up a system for a type of open model. It is an idea to make a simple rule book, for artificial intelligence and share it with everyone. You should have a meeting to teach people about artificial intelligence.

Companies that do well with intelligence are not the ones that try to stop people from using it. They are the companies that use intelligence in a smart way. They know what they are doing, they have clear rules and their employees feel safe and able to use artificial intelligence without being sacred.

About the Author

I am Hadia Zia currently pursuing the degree of Bachelor of Computer Science. I can be reached at hadiazia0328@gmail.com

Keywords: Artificial Intelligence; Cybersecurity; Data Leakage; ChatGPT; Pakistan Tech; Policy framework

References

[1] Samsung (2023) Internal Investigation Report: Accidental Data Leak via ChatGPT, Samsung Electronics Internal Document.

[2] Gupta, *R.&Mehta. (2025) Shadow AI in South Asian Enterprises: Prevalence, Impact, and Mitigation, Journal of Cybersecurity Research,12(3),pp. 45-62.*

[3] *Pakistan Software House Association(2025)State of Cybersecurity in Pakistani IT Exports, Annual Industry Report, pp. 34-41.*