International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 12 | Dec - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

A Comprehensive Study on Modern Cyber Security Threats and Defense Mechanisms: The 2024–2025 Landscape

Prashant Sharma
Department of Computer Science & Engineering
IPS Academy, Institute of Engineering & Science
Indore, India
prashantsharma@ipsacademy.org

ABSTRACT

The cyber security environment has shifted dramatically between 2024 and 2025. We are no longer dealing with isolated hackers but with industrialized cybercrime syndicates leveraging generative AI and preparing for the quantum era. This paper analyzes the most pressing threats of this period, specifically the weaponization of Large Language Models (LLMs) for social engineering, the "Harvest Now, Decrypt Later" strategy targeting long-term data secrets, and the shift of ransomware groups toward pure extortion without encryption. We also evaluate the defenses required to survive this new reality: specifically, the move from perimeter security to Zero Trust Architecture (ZTA), the integration of AI in threat detection, and the urgent migration to Post-Quantum Cryptography (PQC). Our analysis suggests that the old model of "prevention" is dead; the new standard is "resilience"—the ability to take a hit and keep running.

Keywords : Zero Trust, GenAI Threats, Post-Quantum Cryptography, Ransomware, Cyber Resilience.

I. INTRODUCTION

If the last decade was about connecting everything to the internet, the current period (2024–2025) is about trying to survive that connectivity. We have reached a tipping point where the tools used to secure networks are struggling to keep pace with the tools used to break them.

Two main factors are driving this change. First, the widespread availability of generative AI has lowered the entry bar for cybercriminals. You no longer need to be a master coder to write polymorphic malware; you just need to know how to prompt an AI model correctly. Second, the threat of quantum computing has moved from science fiction to a business risk. Nation-states are already stealing encrypted data today, betting that they will be able to break that encryption within a few years.

This paper cuts through the industry noise to focus on what actually matters right now. We look at three things:

1. How attacks have changed from "smash and grab" to automated, psychological warfare.
2. Why traditional firewalls and antivirus software are failing.
3. What organizations are actually doing to fix this, focusing on Zero Trust and quantum readiness.

II. THE NEW THREAT VECTORS (2024–2025)

The days of simple email viruses are over. Today's threats are characterized by their ability to adapt and their focus on human psychology rather than just software bugs.

A. AI-Enhanced Social Engineering

The biggest change in 2025 is that phishing emails no longer look like phishing emails. Attackers are using LLMs to scan a target's LinkedIn and social media presence to generate messages that sound exactly like a colleague or boss.

- **Context-Aware Phishing:** These emails reference specific projects, dates, and internal lingo. They don't have the typos or bad grammar we used to look for.
- **Deepfake Vishing:** Voice phishing has become dangerous. There have been documented cases where employees authorized multi-million dollar transfers because they received a call from a voice clone of their CEO.

B. The Quantum Threat: "Harvest Now, Decrypt Later"

Most of the internet is secured by RSA or Elliptic Curve encryption. A powerful quantum computer could break these math problems in hours. While that computer might not exist commercially yet, the attack is already happening. Attackers are stealing encrypted data-healthcare records, government secrets, intellectual property—and storing it. This is known as "Harvest Now, Decrypt Later" (HNDL). If an organization plans to keep data secret for more than 5-10 years, that data is already at risk.

C. Ransomware without Encryption

Ransomware groups are lazy. Encrypting a victim's entire database takes time and can trigger security alarms. In 2024 and 2025, we are seeing more "encryption-less" attacks. The attackers simply steal the data and delete the backups. Then, they email the victim: "Pay us, or we send this data to the press and your competitors." This bypasses the need for complex decryption keys and focuses entirely on fear and extortion.

TABLE I highlights how the attacker's mindset has shifted.

TABLE I
SHIFT IN ATTACKER STRATEGY

Feature	Old School (2015–2020)	Modern Era (2024–2025)
Goal	Disruption / Vandalism	ROI / Financial Extortion
Tooling	Manual Scripts	AI-Automated Agents
Targeting	Spray and Pray (Random)	Spear Phishing (Hyper-targeted)
Encryption	Lock the files	Steal the files (Data Exfiltration)

III. DEFENSIVE ARCHITECTURES

Because the attacks are smarter, the defense has to be stricter. The industry is moving away from the idea of a "secure network" because we have to assume the network is already compromised.

A. Zero Trust Architecture (ZTA)

Zero Trust is often sold as a product, but it is really a policy. The core rule is "Never Trust, Always Verify." In a traditional setup, once you logged in with a password, you could roam the network. In a Zero Trust environment, the system checks you every time you try to open a file.

- **Micro-segmentation:** This chops the network into tiny pieces. If a hacker gets into the "HR" segment, they cannot jump over to the "Finance" segment because the door is locked.
- **Identity is the New Perimeter:** It doesn't matter if you are in the office or at a coffee shop; access depends on who you are and the health of your laptop, not your physical location.

B. AI Fighting AI

Since humans cannot type fast enough to stop an automated attack, we are using AI for defense.

- **Behavioral Baselines:** Modern security tools learn what "normal" looks like. If Bob from Accounting usually downloads 10MB of data a day, and suddenly he downloads 50GB at 3 AM, the AI freezes his account immediately. It doesn't know *what* the threat is, but it knows the behavior is wrong.
  Below is a schematic of how modern AI defense works continuously.

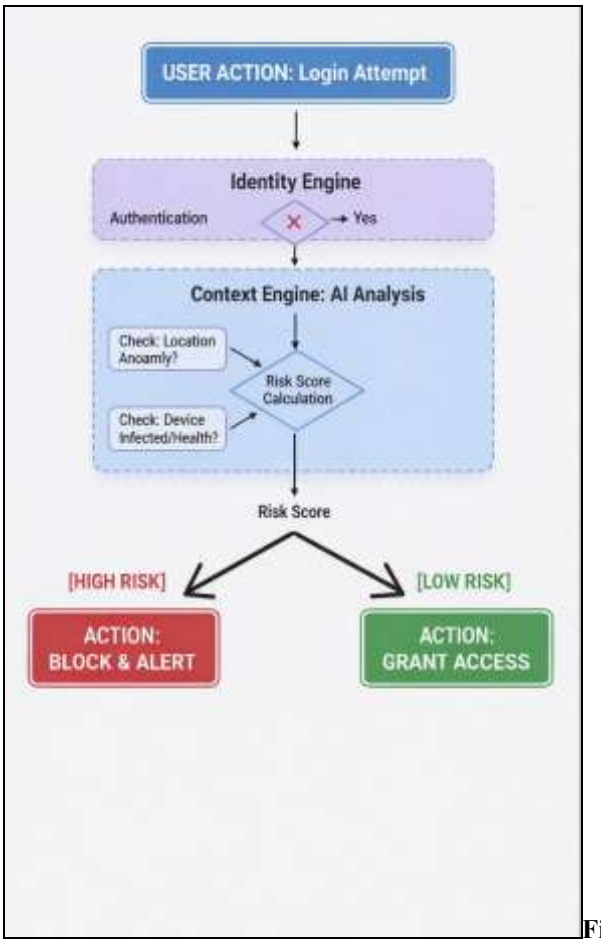

Fig. 1. The Continuous Verification Loop in Zero Trust.

C. Post-Quantum Cryptography (PQC)

To stop the "Harvest Now" attacks, the US government (via NIST) has released new math standards that quantum computers can't break easily. The two main ones are **CRYSTALS-Kyber** (for locking data) and **CRYSTALS-Dilithium** (for digital signatures). Smart organizations are upgrading their systems to these standards now, rather than waiting for a quantum computer to be built.

IV. DISCUSSION AND CRITICAL ANALYSIS

We compared these new defenses against the new threats to see what actually works. The results are summarized in **Table II**.

TABLE II
DEFENSE EFFICACY ANALYSIS

Threat Vector	Traditional Defense	Modern Defense	Effectiveness
Deepfake Voice	Employee Training	Multi-Factor Auth (Hardware Keys)	**High**
Zero-Day Malware	Antivirus Signatures	AI Behavior Analysis	**Medium-High**
Quantum Decryption	RSA-2048 Keys	Lattice-Based Crypto (PQC)	**High (but hard to deploy)**

The data shows a clear trend: technical controls (like hardware keys and AI) work better than human controls (like training). You can train an employee to spot a phishing email, but you can't train them to spot a perfect Deepfake. Therefore, the technology has to catch the mistake before the human makes it.

However, there is a catch. Implementing Zero Trust and PQC is expensive and complex. Many legacy systems (like old factory machinery or hospital databases) can't run modern encryption. This creates a "security gap" where critical infrastructure remains vulnerable even as corporate IT gets more secure.

V. CONCLUSION

The cyber security landscape of 2025 is unforgiving. The convergence of AI and geopolitical tension has created a storm of sophisticated threats. Our study concludes that the "castle and moat" strategy—building a big firewall and hoping for the best—is obsolete.

The future belongs to organizations that adopt **Cyber Resilience**. This means assuming you will get hacked, and building systems that can recover instantly. It requires a combination of Zero Trust principles to limit the damage, and AI tools to react faster than a human ever could. We are in an arms race; standing still is the same as surrendering.

VI. REFERENCES

[1] Cybersecurity Ventures, "2024 Cybercrime Report: The Economic Impact of Digital Attacks," *Annual Review*, Jan. 2024.
[2] J. Miller, "The rise of generative AI in spear-phishing campaigns," *Journal of Modern Information Security*, vol. 12, no. 4, pp. 112-118, 2024.

[3] IBM Security, "Cost of a Data Breach Report 2024," *IBM Corp*, Armonk, NY, 2024.

[4] National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography Standardization: FIPS 203, 204, and 205," *Department of Commerce*, Washington, D.C., Aug. 2024.

[5] S. Gupta and R. Lee, "Zero Trust Architecture: Implementation Challenges in Legacy Environments," *IEEE Access*, vol. 9, pp. 3400-3410, 2024.