AI IN CYBER SECURITY & FORENSICS

Cyber security refers to measures put in place to deter, detect and counter threats to data and systems in networks. Forensics is what's done after a successful attack to understand the loopholes that made it possible for the attack, the parties responsible, and reflect on measures to be put in place to prevent future attacks. Attacks like malware, phishing and spam emails, hacking, data espionage, Denial of Service, Fraud, Identity theft, etc. are some examples of cyber threats organizations with networked computers (whether local network or internet) might want to protect their data and systems against, and AI is a very vital tool to put up strong defenses against such attacks. We will now discuss how AI can be used in cybersecurity and forensics

How AI Can Help in Cybersecurity and Forensics at Ufanisi Bank

Let's imagine a fictional bank in Kenya, let's call it *Ufanisi Bank*. Hackers, fraudsters, and even dishonest employees might try to steal money, access customer data, or disrupt services. To stay ahead, Ufanisi Bank decides to use Artificial Intelligence (AI) to keep their systems secure.

This discussion will look at three areas:

1. How AI helps to prevent attacks before they happen.
2. How AI helps in investigating and solving cybercrimes.
3. How AI helps the bank plan ahead and improve security for the future.

1. How AI Prevents Cyberattacks

Before any hacker tries their tricks, AI is already working in the background to stop them.

a. AI Detecting Suspicious Activity

The first job AI does is **monitoring everything** in the bank's system to catch anything unusual. It looks at customer transactions, employee logins, and how the bank's computers and servers are being used.

For example, if a customer always withdraws Ksh 5,000 at an ATM but suddenly takes out Ksh 200,000 in another town at 2 AM, AI will flag this as suspicious. The system can **pause the transaction** and **send an alert** to confirm if it's really the customer.

The bank uses **open-source tools** like **Suricata and Snort** to monitor all network traffic in real-time. AI makes these tools smarter by teaching them what normal behavior looks like, so they can easily catch anything strange.

b. Stopping Phishing and Fake Emails

Many cybercriminals don't break into the system directly—they **trick employees** into giving them passwords or bank details through fake emails or messages (phishing).

AI tools like **SpamAssassin and PhishTank** scan emails to detect fraud. They check for things like:

✔ Emails pretending to be from the bank's IT department.
✔ Links that lead to fake websites.
✔ Urgent messages asking employees to send their passwords.

If AI sees something suspicious, it warns the employee **before they click** the fake link.

c. AI Preventing Fraud and Theft

AI also protects customer accounts by checking transactions for fraud. It uses **H2O.ai and FraudGuard** to analyze how people usually spend money. If it sees anything unusual, it **blocks the transaction immediately**.

For example, if a customer's account is suddenly used in Mombasa, yet their phone is in Nairobi, AI will suspect fraud and temporarily freeze the account.

The bank also uses **biometric security**, where AI checks fingerprints or facial recognition to verify users. This way, even if a hacker steals a password, they **can't access the account without the customer's face or fingerprint**.

d. AI Responding to Attacks in Real-Time

If AI detects that someone is trying to break into the bank's system, it doesn't wait for humans—it **acts immediately**.

✔ **AI Firewalls like Wazuh** automatically block suspicious connections.
✔ **Multi-Factor Authentication (MFA)** makes it harder for hackers to log in without extra security checks.
✔ **Automatic Account Locking**—if AI sees too many failed logins, it locks the account to prevent hacking.

For example, if someone tries to log into an administrator account from China using stolen passwords, AI **instantly blocks** the attempt before damage is done.

2. AI in Investigating a Cyberattack

Even with strong security, let's say hackers **still manage to break in** and steal money from customer accounts. AI is now used to investigate, find out how it happened, and catch the criminals.

a. Tracking the Hacker's Digital Footprint

The cybersecurity team starts by looking at logs (records of all activity in the system). AI helps analyze thousands of logs in minutes instead of hours.

✔ **Wireshark and Zeek** trace where the attack started.
✔ **ELK Stack (Elasticsearch, Logstash, Kibana)** helps to go through logs to find clues.
✔ AI detects whether the hacker used **a VPN or a proxy** to hide their location.

In this case, AI finds that **an employee's email was hacked**, and the attacker used it to log into the bank's system.

b. Checking for Viruses or Malicious Software

Sometimes hackers install malware (bad software) in the system to steal passwords or corrupt files. AI scans all files and computers for malware.

✔ **YARA and VirusTotal** scan the system for hidden viruses.
✔ **Volatility** checks if hackers left behind spying software.

Here, AI finds that the hacker installed a **keylogger** on an employee's computer to record their password. The cybersecurity team then removes it.

c. Recovering Stolen or Deleted Data

Hackers usually delete logs and files to **hide evidence**. AI helps recover this lost data.

✔ **Autopsy** is used to find deleted files.
✔ AI reconstructs logs that were wiped out.

For example, if the hacker deleted records of where stolen money was sent, AI **restores those logs**, allowing the bank to track the stolen cash.

d. Tracing the Cybercriminals

Once the bank knows how the attack happened, the next step is to **find out who was responsible**.

✔ **Maltego and MITRE ATT&CK** scan online data to find connections between hackers.
✔ AI checks dark web forums where stolen bank data is sold.
✔ **Facial Recognition and Voice Analysis** can check CCTV footage or phone calls for clues.

In this case, AI finds that the stolen money was sent to **fake accounts registered by a cybercriminal group operating from Nigeria**. The case is now handed over to law enforcement.

3. AI in Planning for the Future

Now that the bank has stopped the attack and caught the criminals, it must **strengthen its security** to prevent future incidents. AI helps with this in several ways.

a. Simulating Future Attacks

✔ **MITRE Caldera** runs **fake cyberattacks** to test if the bank's security is strong enough.
✔ AI detects **which employees need more cybersecurity training** based on their mistakes.

For example, AI simulates a phishing attack, and 5 employees fall for it. The bank now knows **who needs extra training**.

b. AI Keeping the System Updated

✔ AI regularly **updates firewalls and antivirus software** to stay ahead of hackers.
✔ It also **learns from new threats** reported globally and **adapts security measures** automatically.

For example, if AI notices that banks in Kenya are being targeted by ransomware, it **strengthens Ufanisi Bank's defenses** before an attack happens.

What we have learnt:

By using AI in cybersecurity and forensics, Ufanisi Bank:

- Prevents most cyberattacks before they happen.
- Investigates and recovers from attacks quickly.
- Continuously improves security to stay ahead of cybercriminals.

With AI, the bank protects its customers, secures their money, and ensures trust in its services.