FEDERAL UNIVERSITY OF TECHNOLOGY
MINNA

THREAT INTELLIGENCE: A PANACEA TO THE GROWTH OF THE NIGERIAN ECONOMY

BY:

PROFESSOR ISMAILA IDRIS
(B.Tech., Msc, PhD., FCSEAN., MCPN, MNCS)
Professor of Cyber Security

INAUGURAL LECTURE
SERIES 132

6TH AUGUST, 2026

FEDERAL UNIVERSITY OF TECHNOLOGY,
MINNA

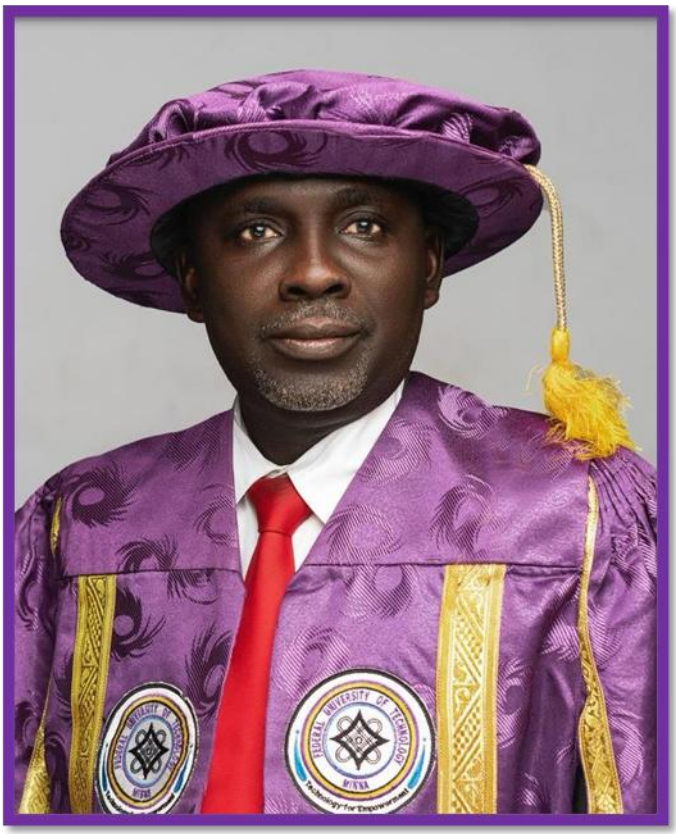
THREAT INTELLIGENCE: A PANACEA TO THE GROWTH OF THE NIGERIAN ECONOMY

BY

Professor Ismaila Idris
(BTech., MSc., PhD., FCSEAN., MCPN, MNCS)
Professor of Cyber Security

INAUGURAL LECTURE SERIES 132

THURSDAY 6TH AUGUST, 2026



Prof. Faruk Adamu Kuta
B.Sc. (UDUS), M.Tech. (FUTMIN), PhD (ATBU)
Vice-Chancellor

Professor Ismaila Idris
(BTech., MSc., PhD., FCSEAN., MCPN, MNCS)
Professor of Cyber Security

PREAMBLE

Mr. Vice Chancellor and other members of University management team; I want to begin this lecture by first acknowledge that all praise is due to Allah, the lord of the whole world. I thank him for his grace upon me. The sustainer of all lives; making it possible for me to stand before this special assembly that has come to listen to my inaugural lecture. Today, I find the fulfilment in teaching, research and community service I undertook over two decades and is a conviction of the stride I have undergone in this great citadel of knowledge. The focus of this lecture is on cyber threat in our digital space that has hinder the Nigeria economic growth and measure to mitigate this cyber threat. At dawn in Niger, a farmer consults his phone for crop prices; miles away in Lagos, a fintech entrepreneur checks her mobile app as a payment pings through from a customer; offshore in the Niger Delta, an oil rig engineer monitors drilling data on a digital dashboard. Once defined largely by oil wells and farmlands, Nigeria's economic landscape today is a diverse tapestry interwoven with digital threads. Key industries like oil & gas, financial services, telecommunications, and agriculture all converge in Africa's most populous nation, powering one of the continent's largest economies. Oil exports still provide the bulk of Nigeria's foreign earnings and government revenue, and agriculture sustains livelihoods for millions. At the same time, booming banks and fintech startups in Lagos are expanding financial services, and telecom networks (anchored by 219 million mobile subscribers across the country) connect communities from bustling cities to remote villages. This convergence of established industries and digital innovation underscores how digital transformation has become a core engine of Nigeria's economic growth. Therefore, the only option for a sound economy on digital space is to have a robust threat intelligence that will fight against digital crime.

The Vice Chancellor Sir, Deputy Vice Chancellors, Registrar, Bursar, University Librarian, Deans, Directors, members of the senate, all the members of the university community, our great Students, invited guest, gentle men of the press, distinguished gentle men and ladies. I welcome you all as you listen to this inaugural lecture.

1.0 INTRODUCTION

Nigeria's economy is increasingly built on digital systems. Banks, markets, transportation and government services now depend on technology to operate quickly and efficiently. This shift has opened doors for growth, enabling things like instant financial transactions, wider trade and opportunities for entrepreneurs to connect with global markets.

This same growth that has brought about lots of technological advancements has also opened new doors for criminals. The more connected we become, the more opportunities hackers find to attack. Just as new roads can bring both trade and robbers, new digital systems bring both progress and cyber threats. This is why threat intelligence is now so important; it helps us see and stop these threats before they cause serious damage.

Threat intelligence is now at the centre of economic resilience. By identifying attacks early, sharing information and responding quickly, threat intelligence acts as a shield that keeps digital platforms safe. When systems are secure, people trust them, businesses grow and investors are confident to put money into the economy. Nigeria recognizes that a secure digital environment supported by strong threat intelligence is not just about technology, it is the bedrock of economic growth and innovation.

2.0 BACKGROUND AND SIGNIFICANCE

This lecture explains why threat intelligence is no longer just a technical matter but a national economic priority. Nigeria's digital economy depends on trust. Banks must assure customers that their money is safe, telecoms must keep networks reliable and government platforms must remain secure and accessible. Without trust in these systems, citizens hesitate to use them, businesses lose customers and investors withdraw.

Threat intelligence provides the foundation for this trust. By detecting, analysing and sharing information about potential attacks, it strengthens defences before damage occurs. It also helps organizations and

government agencies to coordinate responses, making the entire digital ecosystem more resilient.

Understanding threat intelligence is therefore critical not only for cybersecurity professionals but for policymakers, business leaders and citizens. It shows how protecting digital infrastructure directly supports economic growth, innovation and national development.

This lecture emphasizes that in today's world, economic progress is tied to digital security. Strong threat intelligence is the key that enables Nigeria to secure its digital future while creating opportunities for prosperity.

3.0 WHAT IS A THREAT?

Threat is anything that has the possibility to cause harm. In the digital world, a threat is any action or event that can damage computers, steal money, or disrupt services.

For example, a hacker trying to break into a bank's system is a threat. A fake text message asking for your password is also a threat. Even a virus hidden in a mobile app can be a threat.

3.1 What is Threat Intelligence?

Threat intelligence means having the knowledge to stay ahead of cybercriminals. It means collecting information about possible attacks, understanding how they work and using that knowledge to stop them before they cause damage.

In simple terms, it is like a neighbourhood watch for the digital world. Just as people in a community share information about strangers or suspicious movements to stay safe, threat intelligence shares information about hackers, their tricks and their tools.

3.2 Cyber Threats in Nigeria

Table 1.0 Financial impact of cryptocurrency & romance scam activity (Nigeria and global)

Year / Period	Metric / Incident	Reported Economic Impact	Author / Institution & Implication
H1 2022 (Nigeria)	Bank fraud/forgery cases (fake apps, ATM fraud, unauthorized transfers)	67,878 cases; ₦2.71 billion losses	**Central Bank of Nigeria (CBN, 2022)** – Highlighted high and rising cybersecurity risks in financial channels.
May 2023–May 2024 (Nigeria)	EFCC cybercrime enforcement	3,175 convictions; ₦156.3 billion recovered	**Economic and Financial Crimes Commission (EFCC, 2024)** – Enforcement scale signals persistent cyber-enabled crime despite recoveries.
Jul 2023–Jun 2024 (Nigeria)	Crypto activity volume	~$59 billion received	**Chainalysis (2024, Geography of Cryptocurrency Report)** – Nigeria among world's top crypto adopters, creating exposure to scams and laundering risks.
2025 (Global)	DOJ seizure linked to crypto "pig-butchering" scam	$225.3 million seized	**U.S. Department of Justice (DOJ, 2025)** – Illustrates the global scale of crypto-romance scams.

3.3 Key Cyber Threats Emerging With Nigeria's Digital Growth

1.2.1 Business Email Compromise (BEC)

Business Email Compromise, often called BEC, is a type of online fraud where criminals use fake emails to trick people into sending money or sharing secret information. The emails are made to look like they come from a trusted person, such as a company boss, business partner, or supplier. This type of attack is usually accompanied with phishing and ransomware attacks.

3.3.1 What is Phishing?

Phishing is when criminals send fake messages to trick people into giving away important information like passwords or bank details.

For example, a scammer may send a text or email that looks like it came from your bank, asking you to click a link. If you click, they steal your information.

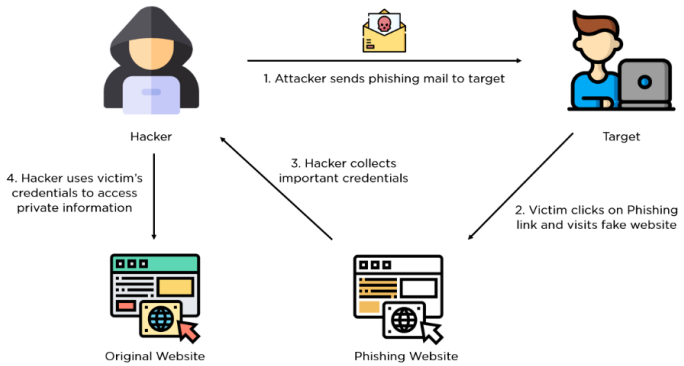


Figure 1: *Visual flow of a phishing attack (Jena, 2025)*

3.3.2 What is a ransomware attack?

A ransomware attack is when criminals put a harmful program on your computer or phone that locks your files. They then demand money (a ransom) before giving you access back.

For example, in 2017 the WannaCry ransomware attack spread across the world. The Internet Society reported that the attack affected several African nations, including Nigeria, alongside South Africa and Angola (Internet Society, 2017). It locked up hospital computers, making it impossible for doctors to see patient records until money was paid. Some businesses and banks in Nigeria also reported disruptions during that time.

Business Email Compromise shows how outsiders can trick organizations from the outside. But not all threats come through fake emails or external criminals. Sometimes the risk comes from people already inside the organization — employees, contractors or partners. This is what we call insider threats and organizational sabotage.

3.3.4 Insider Threats and Organizational Sabotage.

An insider threat is when the danger comes from people inside an organization like employees, contractors or partners who already have access to important systems. They may misuse this access by stealing information, leaking secrets or damaging systems.

Organizational sabotage happens when an insider deliberately or mistakenly causes harm to the company. This could be deleting important files, shutting down systems, or leaking confidential information to outsiders.

For example, in March 2025, an Ecobank Nigeria staff member, Solomon Stephen Ufayo, secretly transferred ₦2.4 million from a customer's account into his personal Opay wallet by abusing his privileged access at work. He was later apprehended by the bank and the Economic and Financial Crimes Commission (EFCC), pleaded guilty in court, and awaits sentencing. This case illustrates how insider threats and sabotage can directly harm businesses and undermine public trust in financial institutions (Premium Times, 2025; TVC News, 2025).

Figure 2: *Types of Insider threats (usecure Team blog, 2025)*

3.3.5 Types of Insider Threats

Insider threats can take different forms depending on the individual's behavior and intention. Researchers commonly classify them into three main categories: malicious insiders, negligent insiders, and compromised insiders (Greitzer & Frincke, 2010; Olalere et al., 2014).

i. Malicious Insiders

These are people who deliberately harm the organization. They may steal money, leak secrets, or damage systems because they are angry, greedy or working with outsiders. *Example: A staff*

member copying customer bank details and selling them to criminals.

ii. **Negligent Insiders**
These are people who do not mean harm but make careless mistakes that create risks. For example, clicking on a phishing email, using weak passwords, or leaving sensitive files unprotected. *Example: An employee accidentally opening a fake email that installs malware on the office computer.*

iii. **Compromised Insiders**
These are people whose accounts or access have been taken over by hackers. The employee may not even know their login details have been stolen and are being used for attacks. *Example: A hacker stealing the login of a company staff and using it to transfer money without the employee's knowledge.*

Insider threats show us that sometimes the danger is already inside the organization. But not all cybercrimes target companies directly. Many are aimed at ordinary people in their everyday lives. Two of the fastest-growing examples in Nigeria are cryptocurrency scams and romance scams.

3.4 Cryptocurrency and Romance Scams

3.4.1 What is Cryptocurrency?

Cryptocurrency is a form of digital money. Unlike physical cash, it exists only online and is stored on electronic devices such as phones or computers. The Reserve Bank of Australia explains that cryptocurrencies are "digital tokens that use cryptography and a decentralised ledger system (blockchain) to operate," with Bitcoin being the best-known example (Reserve Bank of Australia, n.d.).

3.4.2 What is a Scam?

A scam is a deceptive act in which criminals trick people in order to steal money or valuables. Scams can take many forms, ranging from fake business offers to personal frauds such as romance schemes.

3.4.3 What is a Cryptocurrency Scam?

A cryptocurrency scam occurs when criminals misuse digital money by pretending to offer investments, trading opportunities, or other financial services. Their real aim is to defraud victims and steal their cryptocurrency assets.

3.4.4 Why Do Criminals Use Cryptocurrency for Scams?

i. **Difficult to trace** – Once cryptocurrency is transferred, it is usually irreversible.
ii. **Global reach** – Funds can be sent instantly anywhere in the world.
iii. **Low awareness** – Many people do not fully understand how cryptocurrency works, making them vulnerable to deception.

3.4.5 How Do Cryptocurrency Scams Happen?

Cryptocurrency scams often exploit the anonymity, speed, and lack of regulation in digital-asset markets. Criminals combine social engineering with technical deception using methods such as:

i. **Fake Investment Platforms** – Fraudulent websites or apps that imitate real crypto exchanges. Victims are promised high returns and shown fake profits on dashboards until the platform disappears with their funds.
ii. **Phishing and Impersonation** – Attackers impersonate trusted organizations (wallet providers, regulators, exchanges) through emails, social media, or messaging apps to steal login credentials or private keys.
iii. **Rug Pulls and Fake Tokens** – Fraudulent developers create hype around a new coin or DeFi project. Once investors commit funds, the developers remove liquidity, leaving worthless tokens.
iv. **Ponzi and Pyramid Schemes** – Criminals create referral-based schemes where returns for older investors are paid from new investments. The scheme collapses once recruitment slows.
v. **Romance and Social Media Scams** – Fraudsters develop emotional relationships on dating apps or social platforms, then introduce supposed "exclusive" crypto opportunities. Victims, believing in trust or love, send funds to fraudulent wallets.

Across all these methods, the common thread is manipulation of trust, unrealistic promises, and the **irreversibility of cryptocurrency**

transactions, which makes recovery of funds extremely difficult without law-enforcement intervention.

3.4.6 Real-Life Example in Nigeria

In 2021, the Economic and Financial Crimes Commission (EFCC) arrested groups operating fake crypto investment platforms in Lagos and Abuja. Thousands of victims had deposited money with expectations of huge returns, but the platforms shut down suddenly, and the operators fled with billions of naira.

3.4.7 Romance Scams

Romance scams target people seeking relationships online. Criminals pretend to be in love, gradually building trust through conversations, calls, and social media interaction. Once trust is established, they fabricate urgent needs such as medical bills, travel expenses, or business problems, convincing victims to send money.

3.4.8 Impact and Challenges of Cryptocurrency Romance Scams

Cryptocurrency romance scams—sometimes referred to as "pig butchering"—combine emotional manipulation with fraudulent investment schemes. Victims are lured into false relationships and then persuaded to invest in fake crypto platforms. These scams result in both severe financial losses and significant psychological harm for victims (Oak & Shafiq, 2025).

Table 2: Sample of Financial Losses from Cryptocurrency and Romance Scams

Year / Period	Key Metric / Incident	Estimated Economic Impact (USD)	Author / Institution & Implication
May 2023 – May 2024	EFCC reported 3,175 convictions and recovery of ₦156.3 billion	~$355 million (at ~₦440/$)	Economic and Financial Crimes Commission (EFCC, 2024) – Significant recoveries, but shows persistence of cybercrime. (EFCC, 2024)
December 2024	EFCC arrested 792 suspects in Lagos over cryptocurrency-romance scams	₦12.3 billion seized (~$13.5 million)	EFCC (2024); Reuters (2024) – Largest romance/crypto fraud raid in West Africa; damages global trust in Nigeria's digital economy. (EFCC, 2024, Reuters, 2024)

These figures show that the damage is not just personal but national. Even though agencies like the EFCC and CBN are working hard, the losses remain very high. Each case reduces public trust, makes investors cautious and slows down the growth of Nigeria's digital economy.

Romance scams show how criminals can play on people's emotions to steal money. But scams of all kinds usually follow a similar pattern. To understand them better, let us look at the common stages of romance scam.

3.4.9 Stages of Romance Scam

These stages have been documented in recent research on romance and "pig-butchering" scams, which show how scammers systematically progress from approach to exploitation (Oak & Shafiq, 2025).

i. **The Approach**
   The scammer reaches out first, maybe through an email, phone call, WhatsApp, Facebook, or a dating site.

ii. **Building Trust**
   They act nice, professional or caring. They spend time making the victim feel comfortable so nothing looks suspicious.

iii. **The Hook**
   Once trust is gained, they introduce a story or request like "I need urgent help," "Invest now for quick profit," or "Click this link to confirm your account."

iv. **The Action**
   The victim sends money, shares personal details or clicks on a fake link. This is the point where the scammer gets what they want.

v. **The Disappearance**
   After taking the money or data, the scammer vanishes. Sometimes they even return later with another trick, hoping to cheat the victim again.

Understanding these stages is important because it shows how romance scams do not happen overnight. Criminals take time to build trust, play

with emotions and then strike when the victim is fully convinced. By recognizing these steps early, people can protect themselves and avoid losing both money and peace of mind.

Scams like cryptocurrency fraud and romance tricks show how criminals use simple lies to cheat people, but as technology advances, criminals are now using smarter tools to carry out more powerful attacks. One of the most dangerous tools today is artificial intelligence, or AI. This has given rise to what we call AI-driven cyber attacks.

4.0 AI-DRIVEN CYBER ATTACKS

4.1 What is AI?

AI means Artificial Intelligence — when computers are trained to act smart, almost like humans.They can learn, copy, and make decisions without needing much human help.

4.1.1 What is an AI-Driven Cyber Attack?

An AI-driven cyber attack occurs when criminals use artificial intelligence or machine learning to execute cybercrime. By leveraging AI, attackers can make their methods faster, smarter, and more believable—automating tasks like crafting personalized phishing messages, generating malware, or carrying out deception at scale (Abnormal AI, 2025).

Examples

i. **Fake Voices (Deepfake Voice)**
   AI can copy the sound of someone's voice. *Example:* A scammer calls a bank worker using the voice of the manager, asking for money to be transferred.

ii. **Fake Faces (Deepfake Video)**
   AI can create a video of someone that looks real, but it is fake.

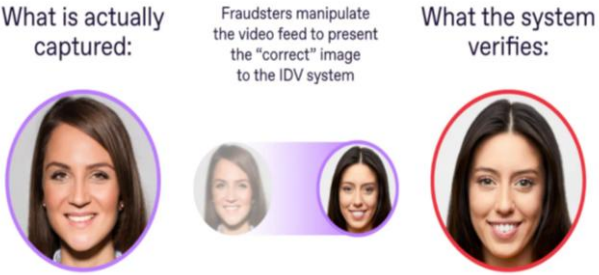


Figure 3: *Practical sample of a deepfake attack* (Terekhin, A.., 2023)

4.1.2 How AI-Driven Cyber Attacks Work

1. **Training the AI**
   Criminals first collect data.
   i. To fake a voice, they record a few minutes of someone speaking.
   ii. To fake a face, they gather photos or videos of the person.
   iii. To send emails, they study real messages from banks or companies.
2. **AI Learns the Pattern**
   The AI studies this data and learns how the voice sounds, how the face looks, or how the emails are written. This allows it to copy or create new versions that look and sound real.
3. **Attack is Created**
   i. The AI generates a fake voice call or a fake video.
   ii. Or it writes thousands of realistic scam emails.
   iii. Or it quickly scans computer systems to find weaknesses.
2. **Tricking the Victim**
   The criminal then uses this AI-made content to fool people.
   i. A worker hears a "voice of their boss" and transfers money.
   ii. A person sees a "video of a government official" announcing a fake program and invests.
   iii. A customer gets a professional-looking "bank email" and gives away their password.

5. **Stealing the Reward**
   Once the victim falls for the trick, the criminal takes money, data, or access usually without being caught, because the fake message or face looked so real.

4.1.3 Real-Life Impacts of AI-Driven Cyber Attacks

i. **Fake Voice Fraud (International but relevant to Nigeria)**
   In 2020, criminals used AI to copy the voice of a company's CEO in Europe. A manager was tricked into transferring $243,000 to the criminals. This case shows how AI can fool even trained professionals. Nigerian banks and companies face the same risk as voice cloning tools are now easily available online.

ii. **Deepfake Scams on Social Media**
   Globally, fake videos (deepfakes) of politicians and celebrities have been used to spread lies or trick people into giving money. In Nigeria, security experts have already warned that deepfake scams could be used during elections or to promote fake investment schemes.

iii. **AI-Powered Phishing in Nigeria**
   Local cybersecurity firms have reported that phishing emails sent to Nigerian companies are becoming much more convincing because of AI tools. Unlike old scam mails with bad grammar, these new ones look professional and harder to detect.

while Nigeria may not yet have a widely publicized "AI attack" case as big as WannaCry or BEC losses, the technology is already being used by scammers here in subtle ways (better phishing, fake profiles, manipulated voices). Experts warn that the country must prepare now, before a large-scale AI-driven attack hits.

AI-driven attacks show how criminals are using smart tools to trick people. But apart from software, there is also a growing danger in the physical devices we use every day. From smart TVs to CCTV cameras and even hospital machines, more and more devices are connected to the internet. This connection is useful, but it also creates new risks. These are called Internet of Things, or IoT, exploits.

4.2 Internet of Things (IOT) Exploits

4.2.1 What is IoT (Internet of Things)?

IoT refers to everyday physical devices that are connected to the internet (or other networks), and can collect, share, or receive data. These include things like smartphones, smart TVs, CCTV cameras, hospital equipment, ATMs, and even smart home appliances. The Internet of Things is defined as "a network of physical devices, allowing them to collect and share data" (IBM, 2023).

Figure 4: *Internet of Things (IOT) Devices (Monton, 2021)*

4.2.2 What is an exploit?

An exploit is a trick or method that hackers use to take advantage of a weakness in a computer system, app, or device.

4.2.3 What are IoT Exploits?

IoT exploits happen when criminals break into these devices through the internet and misuse them.

Examples:

i. A hacker takes control of a CCTV camera to spy on people.
ii. Criminals attack hospital machines, disrupting patient care.
iii. Hackers use thousands of hijacked smart devices to shut down a website or online service.

In a January 6, 2022 report by *THISDAY*, the President of the Cyber Security Experts Association of Nigeria (CSEAN), Mr. Remi Afon, warned that cyber-attacks in Nigeria would likely increase that year. He

specifically pointed to the vulnerability of IoT devices and remote work setups as potential entry points for criminals, referencing CSEAN's *2022 Nigeria Cybersecurity Threat Landscape* report for his predictions (*THISDAY*, 2022).

4.2.4 Impacts of IoT Exploits on Nigeria's Economy

i. **Financial Loss for Businesses**
   According to Genyz Solutions (2024), Nigerian companies that suffer from IoT attacks spend about ₦45 million on average to fix the damage. This is money that could have been used to grow the business or create jobs.

ii. **Cybercrime Rising Fast**
   In March 2025, *Punch Newspaper* reported that Nigeria is now one of the countries with the fastest-rising cyberattacks in Africa. Experts pointed out that smart devices like CCTV, smart meters, and hospital machines are part of the weak points criminals use.

These are not stories they are real. Genyz Solutions says each IoT attack costs Nigerian companies about ₦45 million to fix. The NCC warned in 2023 that CCTV cameras in Nigeria were already being hijacked by criminals. And just this year, Punch Newspaper reported that cybercrime in Nigeria is rising sharply, with smart devices as one of the biggest weaknesses. With more than 2 million devices in Lagos alone (*ResearchGate*), the risk is very real for our economy

All these are critical cyber issues but there is an even bigger risk waiting in the future. A new kind of computer, called a quantum computer, is being developed. If criminals get hold of this technology, it could break the security codes that protect our banks, government systems, and even personal data. This brings us to quantum computing risks.

4.3 Quantum Computing

4.3.1 What is Quantum Computing?

Quantum computing is like a super-fast problem solver. While normal computers check one possible answer at a time, quantum computers can evaluate many possibilities simultaneously by exploiting quantum

mechanical principles such as superposition and entanglement. These properties enable them to solve very specific, complex problems much faster than standard computers (Rietsche et al., 2022). This makes them powerful for things like cracking codes, discovering new medicines, or solving complex science problems

4.3.2 Why is it a Risk?

Today, banks, businesses and government offices protect their money and information using password protection. (A password is the secret code or PIN you use to open your phone, ATM, or email.) With normal computers, it would take criminals a very, very long time to guess or break these passwords, sometimes hundreds of years.

But quantum computers are being built to be super-fast machines. They will be so powerful that they could guess or break these passwords in just a short time.

This means that what feels safe today — like your bank account or government records — may not be safe once quantum computers are in the wrong hands.

4.3.3 Impact of Quantum Computing on Nigeria's Economy

The coming of quantum computers is not just about faster technology. It also brings serious risks that could touch every part of Nigeria's economy. From our banks to government records, from fintech companies to online shopping, no sector will be safe if today's protections can be broken.

i. **Banks and Financial Systems**

Today, banks protect customer accounts with encryption (encryption means turning information into secret codes that only authorized people can read).If quantum computers break these codes, criminals could gain access to millions of bank accounts in Nigeria. This would lead to massive financial theft and loss of confidence in digital banking.

ii. **Government Records**

Important national information like tax data, ID cards and election results are stored digitally. If criminals with quantum computers

break into these systems, they could alter or steal sensitive data. This puts national security and public trust at risk.

The danger of quantum computers is not about what they are doing today, but what they will be able to do tomorrow. If Nigeria is not prepared, criminals could use this technology to break into banks, steal government data, disrupt businesses and scare away investors. The economy depends on trust and once that trust is broken, recovery becomes very difficult. This is why understanding quantum risks now is important for protecting Nigeria's digital future.

We have seen how threats like AI-driven attacks, IoT exploits, and even future risks from quantum computing could affect Nigeria's economy. But these are only part of a bigger picture. When we put them together, they show us one reality — Nigeria is facing an escalating cybersecurity challenge.

5.0 NIGERIA'S RISING CYBERSECURITY CHALLENGE: A CALL FOR THREAT INTELLIGENCE

Nigeria's digital economy is growing very quickly. Banks, fintech apps, hospitals, schools, and government offices are now connected online. This growth creates opportunities, but it also creates more entry points for cybercriminals. Attacks that once started as simple scams are now becoming advanced — using AI-generated fake voices and videos, hacked smart devices (IoT exploits), and even the threat of future quantum computers that could break today's protections. Reports indicate that Nigeria loses hundreds of millions of dollars annually to cybercrime (Omodunbi et al., 2016).

The challenge is that our defences are not growing as fast as the threats. Law enforcement agencies like the EFCC and regulators such as the NCC are making efforts, but cybercriminals are always one step ahead.

This is where threat intelligence becomes critical. Just like people read the news to know about thieves or accidents in their city, organizations use threat intelligence to know about hackers, scams, and attacks happening online. It gives answers to three key questions:

1. What kind of threat is out there?
2. Who is behind it?
3. How do they attack?

Without this knowledge, it's like walking in a dangerous street at night without knowing where the robbers hide. But with threat intelligence, we have a torchlight that shows us the risks ahead, so we can prepare and stay safe.

5.1 Why Threat Intelligence Matters for Nigeria

Think about a busy neighbourhood. If there are no watchmen, thieves will move around freely. But when you have someone watching, noting strange movements, and warning others, the whole area feels safer.

That's exactly what Threat Intelligence does for Nigeria's online world. It helps us see the bad guys before they strike. With it, banks can protect people's money, companies can keep running and more people will trust online services.

For the Nigerian economy to grow strong, we cannot afford to be blind. Threat Intelligence is the watchman.

5.2 Threat Intelligence as the Panacea

Every sickness needs a cure. For Nigeria's growing digital threats, the closest thing to a cure is threat intelligence.

Think of it this way: if thieves are planning to rob a bank, the police are most effective when they know about the plan before it happens. They can prepare, set traps and stop the crime before anyone gets hurt.

That is exactly what threat intelligence does in the digital world. It collects clues from many places like suspicious emails, strange logins, fake websites, or hacker chatter online and turns them into early warnings. These clues are called indicators; little signs that something bad might be about to happen.

All these indicators are brought together on a dashboard.

5.2.1 The Threat Intelligence Monitoring Dashboard

5.2.2 What Is a Threat Intelligence Dashboard?

A Threat Intelligence Dashboard (TID) is a visual system that shows you all the threats entering, attacking or attempting to compromise an organization in real time. Think of it like the dashboard of a car, just as the car dashboard shows your fuel level, speed and warning lights, a threat dashboard shows your cyber alerts, suspicious activities and attacks on your network. For example, Let's say a government agency in Abuja is constantly being attacked with phishing emails claiming to be from the "Central Bank." A Threat Intelligence Dashboard would detect those emails, alert the IT team and even identify if those messages came from outside Nigeria.

Figure 5*: Threat Intelligence Monitoring Dashboard (FortiGuard Labs, 2025)*

5.2.2.1 Basic Terms You Must Understand First

Before diving into the components, let's break down the big words into simple meanings:

Table 3: *Breakdown of terminologies*

Terminology	**Simple Definition**
Threat	Anything that can damage or steal from your computer systems.
Threat Intelligence	Information about those threats and how they behave.

Indicator of Compromise (IOC)	A sign that a threat already entered your system.
Baseline	What is considered "normal" in your system.
Anomaly	A strange or unusual behavior.
Zero-day attacks	Brand-new software flaw used by criminals before any fix exists.
Digital Signature	A secure electronic stamp that proves who sent something and that it wasn't changed.

5.2.3 CORE COMPONENTS OF A THREAT INTELLIGENCE DASHBOARD

A Threat Intelligence Dashboard is not just a fancy screen with blinking alerts. It is built from multiple working parts that collect, process, analyze and display threat data in ways that are useful to human analysts and actionable for defense systems. Each component of the dashboard plays a unique role in helping organizations see threats, understand risks and respond quickly. the components include:

A. Data Sources: The Foundation of Threat Intelligence

A dashboard is only as good as the data it receives, just like a doctor needs blood tests, X-rays, and patient history to diagnose an illness, a threat intelligence dashboard needs raw inputs from multiple places to detect and analyze threats.

Data sources are classified into two main types:

i. **Internal Sources:** refer to all the security-related data generated from within an organization's own systems, devices, and digital activities. These include logs from emails, firewalls, login systems, staff computers (endpoints), mobile devices, and even physical tools like CCTV or biometric doors. The Threat Intelligence Dashboard collects this data to understand what is "normal" in the environment and quickly detect when something strange occurs. For example, if a staff member usually logs in from Abuja during work hours but suddenly logs in from Russia at midnight, the system flags this as suspicious. Similarly, if a staff computer connects to an unknown server or downloads

unusual files, the dashboard can trace it back to potential malware. In Nigerian settings, such as in banks, government ministries, or hospitals, internal data helps expose threats from both external hackers and insiders who may misuse their access.

ii. **External Sources:** External sources are data and intelligence coming from outside the organization, often from cybersecurity vendors, government agencies, or global security communities. These include live updates on known threats (like malicious IP addresses or phishing domains), public reports from forums or blogs, leaked credentials from the dark web, and official advisories from bodies like NITDA or NG-CERT. The dashboard uses this data to stay informed about attacks happening in other places that could soon target your environment. For instance, if attackers are using a fake "CBN" email in Kenya and that domain shows up in Nigeria tomorrow, your dashboard can block it before staff fall victim. External sources give Nigerian organizations a broader awareness of global cyber risks and help them prepare, even before an attack reaches their network.

B. Ingestion and Normalization: Making Threat Data Understandable

Once data is collected from different sources, the next step is to clean, standardize and organize it in a way that the dashboard can make sense of. This process is known as ingestion and normalization. Think of it like assembling a multi-lingual team, each person speaks a different language (email logs, firewall logs, endpoint logs), and the dashboard must translate all those languages into one common format so they can be compared accurately.

Different systems in an organization generate data in different formats and structures. A login alert from a UBA branch may look very different from a firewall alert from NITEL even though they may be linked to the same suspicious event. The ingestion and normalization engine of the dashboard aligns timestamps, unifies data fields and labels key details (like username, location, IP address) to make sure everything is readable and comparable. This allows the system to automatically

correlate events that happen across systems, even if they look unrelated at first.

In a Nigerian context, this helps SOC analysts at government agencies or banks make faster decisions. For example, if a phishing email is sent to a staff member and five minutes later, there's a failed login attempt from an unusual location, the dashboard links those two actions together, thanks to normalization and raises a high-risk alert that might otherwise be missed.

C. Enrichment and Correlation: Adding Meaning and Connecting the Dots

After collecting and organizing the raw threat data, the next critical step is enrichment and correlation. At this stage, the dashboard goes beyond just reading the data, it begins to add extra intelligence and connect related activities across systems. This makes the data more meaningful and helps the security team understand the full picture.

Enrichment means attaching useful context to each event or alert. For instance, if a suspicious login is detected, the dashboard might add details such as:

- **i.** The geolocation of the IP address (e.g., Lagos vs. North Korea),
- **ii.** The device type used to log in (known company laptop or unknown smartphone),
- **iii.** The user's role in the organization (admin, HR, finance),
- **iv.** Whether the IP has been seen in external threat feeds before.

By enriching the raw data, the dashboard makes it easier for analysts to assess risk levels quickly. A login from London at 7 PM by a junior staff may not raise an alarm but the same login from Russia, with a flagged IP address and access to financial systems, is a high-priority event.

Correlation, on the other hand, is the process of linking events that happen across multiple systems but are part of the same threat scenario. For example, if a phishing email is received by a staff member in Zenith Bank and 10 minutes later, someone tries to log in to their account from a suspicious device, the dashboard correlates both events as part of a possible credential theft attack.

In the Nigerian context, this is especially helpful where many organizations use fragmented systems across offices or departments. A coordinated attack such as election-related DDoS attempts on INEC's website, followed by fake login attempts at local government servers can only be understood if these pieces are correlated together by the dashboard.

D. Detection and Alerting: Spotting the Threats Using Smart Intelligence

After gathering raw data, transforming it into a readable format and adding meaningful context, the dashboard moves into the most critical stage: Detection and Alerting.

This is the stage where the dashboard finally becomes "smart", thanks to the integration of Machine Learning, Artificial Intelligence, and Behavioral Analytics. These capabilities allow it to not just display data, but to understand what is dangerous, what is suspicious, and what must be stopped immediately.

Detection works by analyzing all the information flowing into the dashboard and checking for patterns, anomalies, or known threats. Once something is found to be suspicious, it raises an alert, a clear warning to the security team that action is needed.

5.2.4 Smart detection techniques in threat intelligence dashboards

To effectively detect both known and unknown threats, a modern dashboard doesn't rely on a single method. Instead, it combines three powerful techniques to analyze and understand every piece of data passing through the system. Each technique plays a unique role and complements the others.

1. Signature-Based Detection: The Traditional First Line of Defense

This method uses a predefined library of known threat "signatures", these are patterns, file hashes, IP addresses, URLs, or email subjects that have previously been identified as dangerous.

How it works: When new data (e.g., an email, file, login, or connection attempt) enters the system, the dashboard scans it for exact matches against its signature database. If a match is found, the system instantly flags the event as malicious.

Why it's effective:

i. It is very fast and accurate for identifying known threats.
ii. It requires minimal computing power, which makes it efficient even for smaller networks.

2. Behavioral Analytics: Watching for Unusual Activity

This technique focuses on how users and systems normally behave and alerts when there is any significant deviation from the expected pattern, even if there's no known signature.

How it works:

i. The dashboard builds a behavioral baseline for each user, device, or application over time (e.g., login hours, files accessed, locations).
ii. If an event occurs that does not match the baseline, it is marked as suspicious or risky.

Why it's effective:

i. Detects insider threats and compromised accounts, even if the attacker uses valid credentials.
ii. Identifies low and slow attacks, where an attacker moves quietly inside the system.

3. AI + Machine Learning : Pattern Recognition & Predictive Detection

This is the most advanced method, using Machine Learning (ML) and Artificial Intelligence (AI) to identify subtle patterns, link events across multiple systems, and even predict future attack paths.

What is Artificial Intelligence(AI) and Machine Learning?

i. **Artificial Intelligence (AI):** The ability of a computer or machine to perform tasks that normally require human intelligence, such as understanding language, recognizing patterns, and making decisions.
ii. **Machine Learning (ML):** A branch of AI that allows computers to learn from data and improve their performance on tasks without being explicitly programmed.

How it works:

i. Machine Learning models study past cyberattacks to spot patterns and behaviours that show possible danger.
ii. AI tools such as language understanding, relationship mapping, and risk scoring analyse new data by comparing it with what they've already learned.
iii. These systems group similar events together, cut down on unnecessary alerts, and point out the most serious threats first.

Why it's effective:

i. Catches unknown, evolving, or customized attacks that don't match any known pattern.
ii. Automatically adapts to new trends in attacker behavior.
iii. Helps analysts focus on high-risk alerts, saving time.

In General, the dashboard creates a layered, adaptive detection system that offers both breadth and depth of visibility.

E. Visualization and Analyst Interface: Making Threats Easy to Understand and Act On

After detecting potential threats using smart techniques like Machine Learning, AI and Behavioral Analytics, the next job of the Threat Intelligence Dashboard is to present those findings clearly to human analysts. This is where visualization and the analyst interface come in.

Think of this as the front desk of a security command center, everything that has happened, is happening, or might happen is presented in a simple, visual and interactive format so analysts can respond quickly.

What Is Visualization in a Dashboard?

Visualization refers to how threat data is displayed using charts, graphs, maps, timelines and alert boxes. This makes complex security information easier to understand at a glance, even for non-technical decision-makers.

Instead of reading thousands of lines of log files, an analyst can just view:

i. Where attacks are coming from (on a world map),
ii. Which users are acting suspiciously (via behavioral charts),
iii. What alerts need urgent attention (via a prioritized alert feed).

What Is the Analyst Interface?

The analyst interface is the part of the dashboard where security professionals interact with the system. This is where they investigate alerts, apply filters, view incident history, take actions (like isolating devices), and document their findings.

5.2.5 Key Components of the Visualization Layer:

1. **Alerts Panel** – This section of the dashboard immediately shows urgent warnings as they happen. For example, it can notify us if there is a massive wave of fake emails (known as phishing) being sent to trick people, or if someone is trying to log in to a system in a suspicious way that does not match normal user behavior. In short, it tells us when something unusual and dangerous is happening at a go, so action can be taken quickly. An illustration of this is shown below;

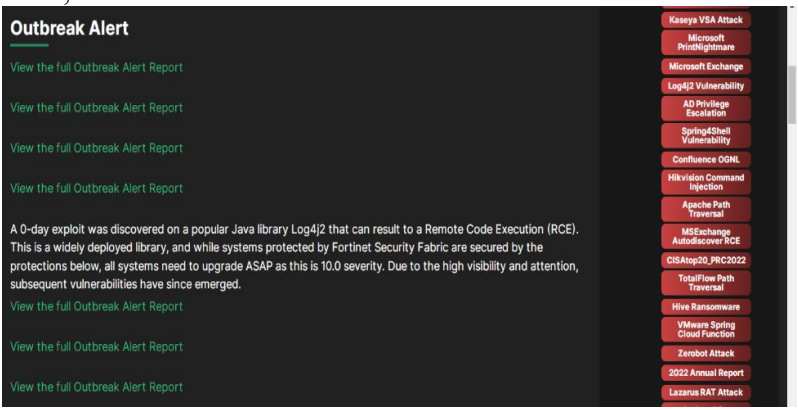


Figure 6*: Threat Intelligence Alert Dashboard (FortiGuard Labs, 2025)*

2. **Attack Map** – Often displayed visually, this shows the geographic origin and spread of cyberattacks. It makes visible the fact that many threats against Nigeria's digital infrastructure originate from beyond its borders.

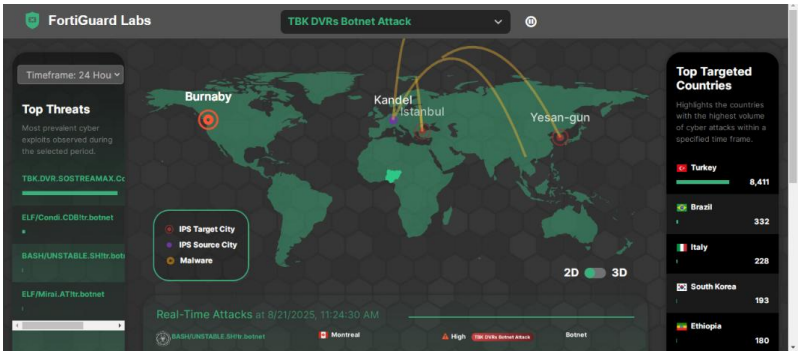


Figure 7*: Threat Intelligence Map Panel (FortGuard Labs, 2025)*

3. **Threat Feeds** – This part of the dashboard provides nonstop updates about new dangers as they are discovered. For example, it can alert us about newly created harmful software (called malware), fake websites designed to steal personal details (called phishing sites), or fresh tricks that cybercriminals are starting to use. Think of it like a news channel for threats — always keeping organizations informed so they can stay one step ahead of attackers.

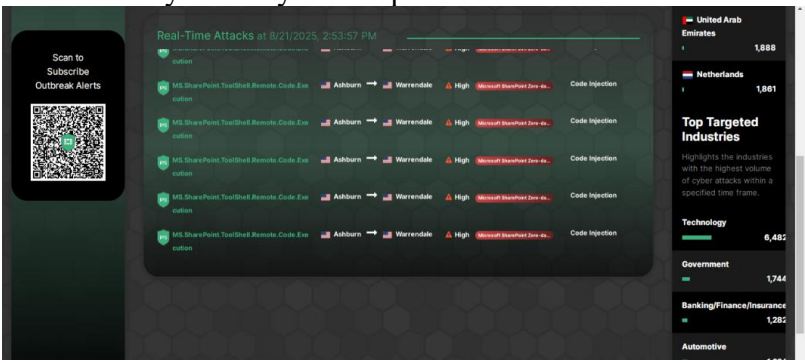


Figure 8*: Threat Intelligence Threat Feeds* (FortGuard Labs, 2025)

System Health Indicators – Similar to how a car's dashboard signals fuel levels or engine warnings, this section shows whether networks, servers and endpoints are operating normally or experiencing compromise.

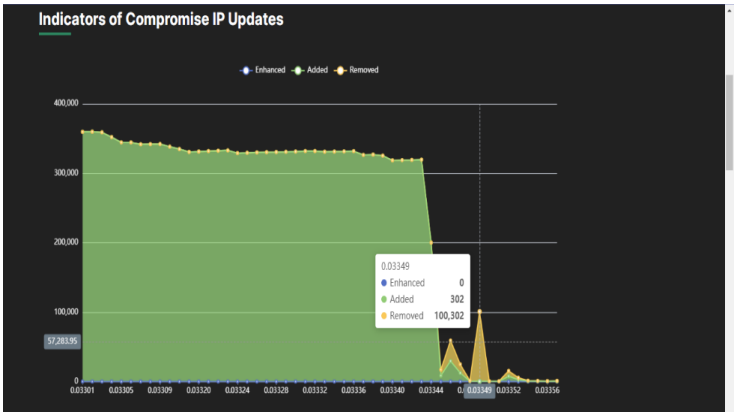


Figure 9*: Threat Intelligence System Health Indicators* (FortGuard Labs, 2025)

4. **Trend Analysis and Graphs** – This section uses simple charts and visuals to show patterns in cyber threats. For example, it can reveal if a certain type of attack is increasing, happening repeatedly, or focusing on key areas like banks, telecom companies, or government agencies. In short, it helps leaders quickly see the bigger picture instead of being lost in scattered details.

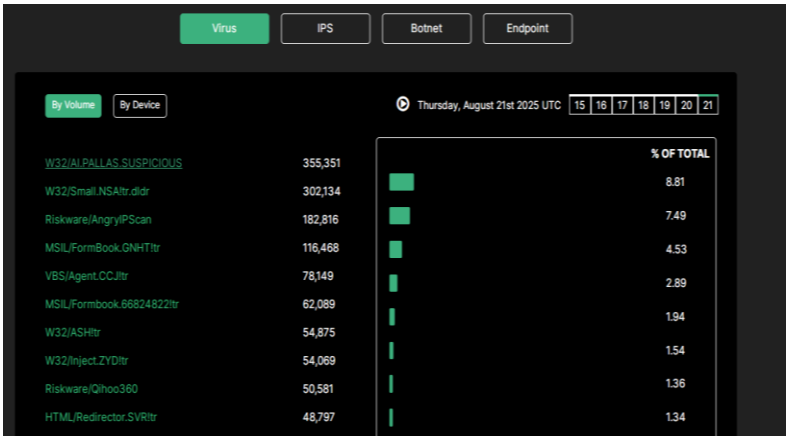


Figure 10*: Threat Intelligence Trend Analysis* (FortGuard Labs, 2025)

Figure 11*: Threat Intelligence Graphs* (FortGuard Labs, 2025)

All these have shown that the dashboard is not just a fancy screen, it is a decision-making tool. It turns raw data into clear signals that guide action. When organizations listen to these signals, they stop attacks before they spread, block phishing before customers click and shut down hackers before they cause damage.

5.2.6 Impact of Threat Intelligence on the Nigerian Economy

Threat intelligence has proven to be more than a technical tool; it is a direct driver for economic stability and growth in Nigeria. By enabling organizations to anticipate and stop attacks before they cause damage, it safeguards the financial backbone of the nation.

1. **Banking and Finance**
   Nigeria's banks face constant threats such as phishing, Business Email Compromise (BEC), and ATM fraud. With threat intelligence, banks detect unusual login attempts or fraudulent transactions early, preventing large-scale financial losses. Each attack stopped translates into billions of naira saved, increased investor confidence, and greater trust in the financial system.
2. **Telecommunications**
   Telecom providers connect millions daily and are frequent targets of SIM swap fraud and mass phishing SMS. Threat intelligence equips them to spot and block such attempts quickly. This protection reduces customer losses, keeps telecom

revenues stable and preserves trust in Nigeria's expanding digital economy.

3. **Government and Public Services**
   Ministries and agencies manage sensitive citizen data, from identity systems to tax records. A single breach could undermine public trust and cost millions to fix. Threat intelligence ensures early detection of intrusion attempts, keeping national databases safe and public services reliable.
4. **SMEs and Startups**
   Small businesses, which make up a large share of Nigeria's economy, often lack strong defences. Affordable, intelligence-driven dashboards give SMEs the same advantage as large organizations. This levels the playing field, allowing them to grow securely and contribute to economic development without fear of sudden collapse from a cyberattack.

5.2.7 Economic Impact in Numbers:

EFCC Chairman Olukoyede (2024) noted that Nigeria lost about $500 million to cybercrime in 2022 alone. If threat intelligence prevents even 20% of these attacks, that represents hundreds of millions saved — resources that can be redirected to infrastructure, jobs and innovation.

In essence, threat intelligence is not only a shield for networks; it is an engine of economic resilience, protecting sectors that fuel Nigeria's growth and strengthening the nation's reputation as a secure destination for business and investment.

Threat intelligence is not just Nigeria's defense — it is the "Panacea to the Growth of the Nigerian Economy"

6.0 MY CONTRIBUTIONS

Due to daily emerging cyber threat globally, it becomes very difficult to completely eliminate threat. Threat landscape is verse in terms of the different threat actors involve in the execution of attacks. It becomes more important to give more attention to researchers as attacks change in pattern every minute; there is need for a robust approach in making sure that constant research takes place in order to improve solutions that

mitigate against attacks. Threat attack behavior analysis involves understanding how attackers operate to identify, assess, and mitigate potential threats. This includes analyzing tactics, techniques, and procedures (TTPs) used in attacks, as well as understanding the motivations and goals of attackers. Behavioral analysis, including user and entity behavior analytics (UEBA), plays a crucial role in detecting anomalous activity and deviations from normal patterns, which can indicate malicious intent. By understanding attack patterns and behaviors, organizations can proactively strengthen their defenses and respond more effectively to potential threats.

Therefore, the need to proffer solutions to the constant attacks on systems, digital infrastructure, and the cyber space in Nigeria and the world at large has propelled me to conduct research on email spam detection, distributed denial-of-service detection, website phishing attack detection, and financial anomalies detection. Building further on this, my contributions to the development of a Threat Intelligence Dashboard are drawn from my published works, each aligning with one of the smart capabilities—Signature-Based Detection, Behavioral/Anomaly Detection, and AI/ML Pattern Recognition—while directly addressing real-world Nigerian cybersecurity challenges.

6.1 Development of a Hybridized CNN BiGRU Framework for Detection of Website Phishing Attacks. (Idris et al, 2025).

Phishing remains a major cybersecurity challenge, with attackers using deceptive tactics to trick users into disclosing confidential data. Traditional detection systems, which often rely on fixed features or predefined rules, struggle to keep up with rapidly evolving phishing strategies. This research introduces a deep learning-based solution that combines Convolutional Neural Networks (CNN) and Bidirectional Gated Recurrent Units (BiGRU) to improve phishing website detection. The CNN component is responsible for learning spatial patterns from web data, while the BiGRU layer captures sequential relationships, providing a more complete understanding of the underlying threats. The framework involves meticulous preprocessing steps such as data cleaning, normalization through MinMax scaling, and optimal feature

selection using the SelectKBest, CNN and BiGRU methods. The model was trained and tested on large-scale, publicly available datasets from IEEE Data Port and Mendeley, consisting of over 250,000 URL entries. Through train-test split and cross-validation techniques, the model consistently achieved outstanding results: 99.96% accuracy, 99.92% precision, 100% recall, and a 99.92% F1 score. When compared to existing solutions, this hybrid approach sets a new performance benchmark, underscoring the power of combining spatial and temporal deep learning methods in defending against phishing threats.

6.2 A Multi-Tier Edge–Fog Intelligent Learning Framework for Detecting Financial Anomalies in Smart Cities (Idris et al, 2025)

The rapid digitization of urban infrastructure has reshaped smart cities into highly
interconnected ecosystems where financial transactions are continuously generated at the network's periphery. In such settings, ensuring timely detection of financial anomalies is critically dependent on distributed, low-latency intelligence. The research presents an Edge–Fog-centric hybrid anomaly detection framework tailored for smart city financial infrastructure. The proposed architecture leverages a multi-tier collaborative model, wherein edge devices—such as point-of-sale terminals, ATMs, and mobile sensors—are equipped with real-time sensing, computing, and classification capabilities to grade financial transactions on a scale of 1 to 7. At the edge layer, unsupervised autoencoders, LightGBM regressors, and Isolation Forests operate locally to assign grades, which are refined through peer-to-peer collaboration between proximate edge nodes for contextual consistency. Transactions with higher anomaly grades are escalated to the fog layer, where a supervised One- Class SVM performs deeper analysis using device-level metadata (IP, MAC) to reduce false negatives. This edge–fog synergy enables decentralized yet coordinated detection that meets the stringent latency and scalability requirements of smart cities. Comparative evaluation on real-world financial data demonstrates the superiority of the proposed architecture, achieving accuracy: 98.82%, sensitivity: 91.30%, specificity: 98.79%, and reducing the false negative

rate to 8.70%, outperforming standalone models such as autoencoders (FNR: 50.44%), Isolation Forests (FNR: 35.50%), and SVMs (FNR: 56.38%). These results highlight the efficacy of edge–fog collaborative intelligence in delivering robust, scalable, and context-aware financial anomaly detection in next-generation smart cities

6.3 Stack ensemble model for detection of phishing website (Idris et al, 2024)

The importance of mitigating the risk associated with online purchases for retail businesses cannot be overstated, phishing websites are a significant threat to these businesses as they deceive web users and steal their sensitive information. The paper proposed a stack ensemble model consisting of three different classification algorithms RandomForest, GradientBoosting(Xgboost), and Adaptive Boosting (Ada Boost), with logistic regression as an aggregator, to detect phishing websites. The proposed model was evaluated and compared with each individual algorithm in the stack, as well as with existing studies. Our analysis showed that the proposed stack ensemble model performed better than each algorithms and existing studies in terms of accuracy, recall, specificity, precision, and F1 score. Specifically, our proposed model obtained an accuracy of 98.72%, recall of 98.84%, specificity of 98.60%, precision of 98.60%, and F1 score of 98.72%, with a low error rate of 1.28%. Overall, the results of our study demonstrate the effectiveness of the proposed stack ensemble model in detecting phishing websites for retail businesses. This model can play a crucial role in enhancing cybersecurity measures and mitigating the risks associated with online purchases. The findings of this study could be beneficial to security experts and policymakers working to improve cybersecurity in the retail industry.

6.4 Machine Learning Approach Based on Synthetic Minority Over-Sampling Technique and Isolation Forest for Insider Threat Detection (Idris et al, 2023)

Detecting insider threats is challenging due to insiders' deep familiarity with networks and security protocols, allowing them to bypass

traditional security measures. While various methods combat insider threats, creating effective detection systems remains difficult. Research advocates using Machine Learning (ML) techniques, but handling imbalanced datasets reduces accuracy. To tackle this, this paper presents "SMOTE-IForest," merging SMOTE and IForest for insider threat detection. Testing on the CERT r6.2 dataset achieved 80.0% accuracy in detecting user behaviour. Additionally, it reached a 63.4% detection rate with a 67.0% false positive rate, boasting a high AUC of 96.0%, 93.30% precision, and 88.80% f-measure. This model addresses accuracy, detection, and false positive rate issues. SMOTE improves dataset balance by creating synthetic samples from the minority class, enhancing classification accuracy. IForest isolates anomalies, efficiently handling high-dimensional data without complex tuning, ideal for insider threat detection. The "SMOTE-IForest" model significantly strengthens insider threat detection systems by overcoming dataset imbalance and enhancing accuracy. Its precision and f-measure distinguish between normal and anomalous behaviour, aiding in addressing setbacks associated with existing studies' accuracy, detection, and false positive rates.

6.5 Insider Threats & Behavioral Analytics Insider Threats — Behavioral /Anomaly Module (SLR- Derived Framework) (Idris, I., & Adeleke, N. D. (2023)).

Insider threat refers to the risk caused to an organization's security, assets, or data by individuals who have authorized access to these resources, such as employees, contractors, or partners. The aim of an insider threat is usually to exploit their access to sensitive information or systems to carry out malicious activities, such as stealing intellectual property, financial data, or sensitive information, sabotaging systems, or processes, or committing fraud. This systematic review analyses the anatomy of insider threat, including its trends and mode of attacks to find the possible solutions by querying various academic literature. Sources of insider threat dataset are revealed in this review paper to ease the challenges of researchers in getting access to insider datasets. In addition, a taxonomy of insider threat current trends is presented in

the paper. This review can serve as a benchmark for researchers in proposing a novel insider threat detection methodology and starting point for novice researchers.

6.5 Smart Financial Fraud Detection and Customer Risk Profiling in Financial Institutions Using Genetic Markov Algorithm Idris, I & Muhammad Sani,. (2019).

The research model the shape of transaction sequences and adapt detection parameters as fraud tactics change. Genetic–Markov approach for financial-fraud detection and customer risk profiling model transaction sequences while adaptively tuning decision parameters. Using anonymized EFCC/FIU transaction records with 20+ operational attributes (e.g., balance, overdraft frequency, timing/location, card age, income, spending rate), the pipeline forms risk clusters via k-means, applies a Genetic Algorithm to optimize features/thresholds, and uses a (Hidden) Markov model for probabilistic classification into Low/Medium/High risk. Reported results show Accuracy: 79.9% for the Genetic–Markov fusion (vs. 51.67% GA and 43.23% HMM alone), with test distribution around 65% High, 25% Medium, and 10% Low risk. In the dashboard, this supports real-time AI/ML Pattern Recognition: per-customer risk scoring, step-up controls for high-risk transactions, and analyst-ready case creation with the triggering sequence path and operationalization of the threat intelligence dashboard.

6.7 Whale Optimization Algorithm-Based Email Spam Feature Selection and Classification (Idris et al, 2019)

Email spam continues to be a major cybersecurity challenge in Nigeria, especially within the banking sector where phishing mails disguised as official messages from the Central Bank of Nigeria (CBN) or NIBSS are used to defraud customers. Conventional spam filters often fail due to the high false-positive rate, which blocks genuine emails and reduces trust in digital services. The research introduced a hybrid spam detection model that integrates the Whale Optimization Algorithm (WOA) for feature selection and the Rotation Forest (RF) classifier for

categorization of emails. The WOA was inspired by the hunting strategy of humpback whales, allowing the system to intelligently select the most relevant features from datasets (Spambase and Enron-Spam corpus). These reduced features were then passed to Rotation Forest, which uses decision trees on rotated feature subsets to improve accuracy. MATLAB was used for feature selection, while WEKA handled classification with 10-fold cross-validation. The experimental results showed remarkable performance: Accuracy: 99.9%, False Positive Rate: 0.0019, far outperforming Naïve Bayes, SVM, and traditional filters. In the Nigerian context, such a model can be deployed at financial institutions to drastically reduce phishing attacks without blocking legitimate customer communication. Within the Threat Intelligence Dashboard, this work strengthens the Signature-Based Detection module, ensuring spam and phishing mails are flagged with near-perfect precision while minimizing disruption of genuine business communications.

6.8 An Intelligent Crypto-Locker Ransomware Detection Technique Using Support Vector Machine and Grey Wolf Optimization (Idris, et al, 2019)

Ransomware is an increasing threat in Nigeria, targeting universities, hospitals, and government offices by encrypting files and demanding cryptocurrency payments. Crypto-locker ransomware is particularly devastating because of its strong encryption and ability to evade traditional signature-based antivirus solutions. The research proposed an SVM-GWO hybrid model for ransomware detection. Grey Wolf Optimization (GWO), modeled after the hunting behavior of wolves, was used to select optimal feature subsets, while Support Vector Machine (SVM) classified applications as ransomware or benign. The model was trained on the Sgandurra dataset, which included 582 ransomware samples and 942 benign applications. Cross-validation was applied to ensure robust performance, with evaluation metrics including Accuracy, Precision, Recall, F-measure, and RMSE. The system achieved outstanding results: Accuracy: 99.16%, Precision: 98.3%, Recall: 99.2%, F-measure: 98.7%, and RMSE: 0.015, indicating high

reliability with minimal false alarms. In Nigeria, where ransomware attacks on healthcare and education are increasing, this research provides a practical detection tool that can be embedded within a Threat Intelligence Dashboard. It contributes directly to the Behavioral/Anomaly Detection layer, monitoring program behaviors and file access patterns to block ransomware before encryption spreads across the network.

6.9 Random Forest Based HTTP Distributed Denial of Service (DDoS) Attack Detection for Cloud Environments (Idris et al, 2019)

Distributed Denial of Service (DDoS) attacks are a growing risk for Nigeria's cloud-hosted platforms, such as JAMB registration portals, immigration services, and fintech startups like Paystack and Flutterwave. HTTP flood attacks can overwhelm servers, making vital national services unavailable. The study introduced a Random Forest-based detection system for HTTP DDoS in cloud computing environments. Simulated datasets included both normal and attack HTTP traffic, capturing features such as request rate, header anomalies, and session behavior. Preprocessing ensured balanced training data, and Random Forest was trained and tested against Naïve Bayes and SVM classifiers. The results demonstrated strong resilience and performance: Accuracy: 96.7%, with a False Positive Rate of only 3.3%, outperforming other models in robustness and detection speed. For Nigerian systems, where public services frequently experience politically motivated or fraud-related DDoS disruptions, this contribution provides a reliable defense layer. Integrated into the Threat Intelligence Dashboard, it enhances the Anomaly Detection module, flagging abnormal surges in HTTP traffic and enabling SOC teams to mitigate attacks before services crash.

6.10 Improved Email Spam Detection Model with Negative Selection Algorithm and Particle Swarm Optimization (Ismaila Idrs and Ali Selamat (2014))

AND

6.11 Hybrid Email Spam Detection Model with Negative Selection Algorithm and Differential Evolution (Ismaila Idrs and Ali Selamat (2014))

Two (2) Patented: Innovation and Commercialization Center, Malaysia 2014

Inspired by adaptive algorithm, the research introduces a modified machine learning technique of the human immune system called negative selection algorithm (NSA). A local selection differential evolution (DE) and particle swarm optimization (PSO) generates detectors at the random detector generation phase of NSA; code named NSA-DE and NSA-PSO. Local outlier factor (LOF) is implemented as fitness function to maximize the distance of generated spam detectors from the non- spam space. The problem of overlapping detectors is also solved by calculating the minimum and maximum distance of two overlapped detectors in the spam space. The difference in performance between our NSA-PSO, NSA-DE model for spambase dataset are very significant. Best accuracy for enhanced NSA-PSO is 83.20% and enhanced NSA-DE is 83.06%. The best threshold value for the enhanced model is recorded at 0.4 with varying number of generated detectors. In general, the new optimized models outperformed the standard NSA model with best accuracy at 68.89% for spambase dataset. The comparison of our model with the state of the art machine learning models shows that our models perform better. The proposed models perform better than the standard Naïve Bayes models with accuracy of both models at 78.8% and 79.3% respectively. The model also performs better than the support vector machine (SVM) with accuracy of 80%. The cost sensitive multi-objective genetic programming (csMOGP) model was also out performed by our model.

7.0 CONCLUSION

The Nigerian digital economy stands at a pivotal point where the benefits of rapid technological adoption are equally matched by the magnitude of evolving cyber threats. The threat spectrum spanning Business Email Compromise, Insider Sabotage, Cryptocurrency and Romance Scams, AI-driven cyberattacks, IoT exploits, and the looming risks of Quantum Computing presents a complex, multi-layered challenge to national security, economic stability, and societal trust. A recurring theme is that data, trust, and resilience are the lifeblood of a thriving digital economy. Disruptions in any of these areas translate directly into financial losses, reduced investor confidence, and slower economic growth. As demonstrated, threat intelligence is not merely a defensive mechanism but a strategic enabler that underpins innovation, secures investment, and safeguards national infrastructure.

This inaugural lecture emphasizes on the urgent need for a coordinated and intelligence-driven approach to combating cyber threats in Nigeria in order to save the Nigeria economy from attack. Through an in-depth exploration of the cyber threat landscape, sector-specific vulnerabilities, and the transformative potential of Cyber Threat Intelligence (CTI), this lecture has demonstrated that reactive, isolated responses are no longer sufficient. Cyber threats are increasingly sophisticated, persistent, and capable of inflicting severe economic, reputational, and national security damage. The evidence from case studies, statistical models, and technological readiness indices strongly supports a proactive, intelligence-led approach that anticipates threats rather than reacts to them. Without such measures, the growth trajectory of Nigeria's economy risks being compromised by both known and emerging cyber risks. By integrating CTI into national cybersecurity strategies, Nigeria can transition from a posture of crisis management to one of proactive defence.

The proposed framework for a National Threat Intelligence Coordination Centre (NTICC) and the accompanying AI-powered National Threat Monitoring Dashboard illustrate how intelligence-sharing, real-time detection, and coordinated incident response can

significantly reduce exposure to cyberattacks. These models are not abstract ideals—they are proven in other jurisdictions and adaptable to Nigeria's unique environment, provided there is strong political will, institutional capacity, and sustained investment.

The recommendations outlined ranging from establishing sector-wide intelligence-sharing mandates, enhancing skills development, creating robust legal frameworks, and fostering public–private partnerships are all actionable within the short to medium term. Success, however, depends on more than technology. It requires fostering a culture of trust between stakeholders, embedding cybersecurity into organisational governance, and ensuring accountability in how intelligence is collected, analysed, and acted upon. The analysis has also shows that cyber resilience is a shared responsibility. Government agencies must lead in policy-making and coordination; private sector operators must commit to transparent intelligence-sharing; academia must contribute through research and skills development; and civil society must advocate for rights-respecting security measures.

8.0 RECOMMENDATIONS

Policy and Governance

i. National Quantum-Resistant Encryption Mandate: Legislate adoption of post-quantum cryptographic standards across critical sectors (banking, energy, government).
ii. Mandatory Threat Intelligence Programs: Require all Tier-1 and Tier-2 organizations to integrate intelligence-led security operations by 2026, with annual compliance audits.
iii. Cybercrime Law Harmonization: Align Nigeria's cyber laws with Budapest Convention standards to improve cross-border threat response.

Capacity Building

i. National Cybersecurity Talent Pipeline: Partner with universities and technical institutes to embed threat intelligence, digital forensics, and AI-security modules into curricula.

ii. Public–Private Training Alliances: Establish sector-specific training hubs (e.g., Fintech Cyber Threat Lab) to simulate real-world attack scenarios.

Technology and Infrastructure

i. Threat Intelligence Sharing Platform: Create a centralised, government-backed platform integrating feeds from local ISPs, banks, and telecoms for real-time threat data exchange.
ii. AI-Augmented SOCs (Security Operations Centres): Invest in machine learning models for anomaly detection and automated triage of security alerts.
iii. FHE & Big Data Integration: Adopt Fully Homomorphic Encryption for sensitive datasets, enabling secure analytics without exposing raw data.

Sector-Specific Strategies

i. Banking & Finance: Deploy behavioural analytics to detect anomalies in transaction patterns and pre-empt BEC or crypto fraud schemes.
ii. Healthcare: Secure IoT-enabled medical devices with layered authentication and network segmentation.
iii. Agriculture & Smart Cities: Implement blockchain-backed IoT management systems to ensure data integrity in sensor-driven operations.

9.0 ONGOING RESEARCH

i) The use of post quantum digital hash function for data authentication
ii) Design Framework of Cyber Security Solutions to Threats and Attacks on Critical Infrastructure of Electricity Power Systems of Nigeria Companies
iii) Adaptive Neuro-Fuzzy Inference System for Ransomware Attack Types Classification
iv) Machine Learning Algorithms for Botnet Detection Using Sampling Techniques and Cost Sensitive Methods.

10.0 ACKNOWLEDEMENTS

Alhamdulillah for Allah's grace and mercy in my life and how far He has led me through every endeavours. All praises are due to him alone. My heartfelt gratitude goes to my parents Alhaji Ismaila Suleiman (May Allah forgives his shortcomings and grant him al-janat firdaus) and Hajiya Khadijat Ismaila for their sacrifice, love, care, support and tutelage which serves as the backbone of my academic achievement today. My profound gratitude goes to the Vice-Chancellor, Prof. Faruk Adamu Kuta, the Deputy Vice-Chancellor (Academic), Engr. Prof. Abdullahi Mohammed, the Deputy Vice-Chancellor (Administration), Prof. Uno Uno, the Registrar, Mal. Danladi Mallam, the Bursar, Mrs. Hadiza Goje, and the Librarian, Prof. S. Katamba. I appreciate the Vice-Chancellor of Edusoko University Prof. M.A.T Suleiman. My appreciation also goes to the following former Principal Officers: Prof. Abdullahi Bala, Prof. M. A. Akanji, Prof. M. S. Audu and Prof. Tukur Sa'ad who gave me employment, Mall. Muhammad Dattijo Usman, Prof. A. O. Osunde, Prof. S. O. E. Sadiku, Prof. O. O. Morenikeji, Prof. Y. A. Iyaka, Prof. E. Udensi, Mrs. V. N. Kolo, Mr. A. N. Kolo, Mrs. A. S. A. Ndayako and Prof. J. A. Alhassan. The efforts of my teachers are greatly appreciated. They include Prof. Y.M Aiyesimi, Late Prof. K. R. Adeboye, Prof. N.I Akinwande, Prof. Y.A Yahaha, Prof. U.Y Abubakar, Prof. Hakimi Danladi, Prof. Adamu Alhaji Mohammed, Prof. A. Isah, Prof. Jiya Mohammed, Prof. A.I Enagi, Prof. Abdulrahman Ndanusa, Prof. Umar Mohammed Sanda, Prof. Suraju Abdulrahman, Prof. Gbolahan Abolarin and all others at tertiary, secondary, and primary school levels who have in one way or the other imparted knowledge unto me.

My appreciation goes to Prof. Jude Kur, the Dean of SICT, Prof. J.K. Alhassan (Director Academic Planning) and Dr. J.A Ojeniyi (HOD Data Science) who both painstakingly went through the manuscript of this lecture. I also appreciate the former Dean of SICT Prof. N. Iwokwagh. My appreciation also goes to my HOD, Dr. N.D Moses, and my colleagues – Prof. V.O. Waziri, Dr. S.M. Abdulhamid, Dr. O.S Subairu, Dr. Suleiman Ahmad, Dr. A.O Isa, Mr. Baba Meshach, Mr. Yisa Victor

Legbo, Mr. Hassan T. Abdulazeez, Mrs. Emily Sode-Shinni, Mr. Andrew Uduimoh, Mr. Buhari Dauda, Mr. Peter .C. Anyaora, Mal. Abdullahi Usman, Mal. Danlami Bosso and Madam Rebecca Haruna and all other staff of the Department. I appreciate the HOD, Computer Science, Dr. Enesi Femi Aminu, and other staff in the department Dr. (Mrs.) O. Abisoye, Dr. S. A. Adepoju, Dr. S. Ojerinde, Dr. M. B. Abdullahi, Dr. S. Bashir, Dr. M. Kudu, Mal. A. Yahaya, and Mal. Ibrahim Shehi Shehu. My appreciation also goes to Dr. Ishaq Alabi, HOD IT, and Dr. Grace A. Onyeabor HOD ISMS, and all staff of their departments. Special appreciation to Dr. (Mrs) Victoria I. Chukwuemeka, Chairperson of the University Seminar and Colloquium Committee, and all the members of his committee. I appreciate Maths/Computer Science of FUT, Minna, 2002 set. I appreciate all my neighbours. I appreciate all my undergraduate, master's and PhD students.

I am grateful to my mentor Alhaji Hakeem Ajijola (CEO of CS2 Consultant); Prof. Dantani Ibrahim Wushishi (Registrar of NECO) and his wife Hajiya Mariam Mohammed Kolo, Mr. Yakubu Mohammed Kolo (Former Commissioner of Environment and Climate Change), I appreciate Navy Capt. IR Saidu (Deputy Vice-Chancellor Admiralty University), Bragadier General Jacob Hassan Bawa (Commandant of Nigeria Army Cyber Warfare School, Abuja), Air Vice Marshal (AVM) Adeniran Kolade Ademuwagun (Commandant, Airforce Institute of Technology), Engr. Dr. Jafaru O. Mahmud (CEO of Scientific Equipment Development Institute, Minna), Remi Afon (Chairman BOT of CSEAN), Mr. Olabode G. Agboola (President of CSEAN), staffs of Cyber Security Department (NDA), staffs of Cyber Security Department (AFIT), staffs Cyber Security Science (Phoenix University) and staffs of Computer Science Department (IBBU, Lapai).

I appreciate my siblings – Maimuna, Halima, Fatima, Ramatu, Salamat, Amina and my brother Danlami. my father-in-law Late Tanko Shamaki and my mother-in-law, Mrs. Amina Tanko Shamaki. My Aunties and uncles Late Dr (Mrs) Amina Suka, Hajiya Azumi Isiaku, Hajiya Maimuna Umar, Late Alhaji Suleiman Mundi, Late Alhaji Musa Mundi,

Late Alhaji Ibrahim Mundi, Hajiya Ramotu Ibrahim, Hajiya Lami Taju, Mrs Aisha Abenemi JP, Late Barrister Jummai Suka, Hajiya Jummai Mundi, Hajiya Maryam Ahmed, Late Mallam Idris Mundi, and Mr. Dada Arojojoye. I am grateful to Mal. Rabiu Alhaji Yabagi and his family, Mal. Abubakar Yakubu and his family, Alhaji Suleiman Dauda and his family, Alhaji Olawuyi Ishaq and his family, Mal. Usman Yau Yakubu and his family, Alhaji Bama Mundi and his family, Alhaji Danjuma Umar and his Family, Alhaji Mahmood Mundi and his family,

My special gratitude goes to the Doggi Dynasty and the Patriarch of the Doggi Dynasty; my brother who is my father Alhaji Umar Abdullahi Doggi; Thank you for being my pillars of strength, love and guidance; I appreciate everything you do, I thank you for the discipline, the prayers, the encouragement to move on when the going was tough, thank you for the sacrifice you made and still making and my grandma Hajiya Asmau Abbdullahi Doggi (Nna) Words are not enough to appreciate you. My appreciation goes to my brother RT Hon. Aliyu Umar Yusuf (Speaker of Kogi State House of Assembly) for the love and care you have always shown me, Ya Makun, Ya, Umaru and Ya Ibiro. I also Appreciate his royal highness Etsu Abubakar Aliyu. (The Etsu of Edo) and all his chiefs in council. All men and women of my lineage. I thank you all for your supports all through the years. I love and appreciate you all.

To my beloved wife, Mrs. Hauwa Idris, my sweetheart, thank you for being there for me. My children Khadija, Ismail and Amina; you are all wonderful. Thank you.
Finally, to the audience, I thank you all for your attention. God bless you.

REFERENCES

Adebiyi, P. (2023). *Cybersecurity in Nigeria: Real Threats, Real Impact*. Cyber Defense Research Review.

Islam, M. R., Habib, M. A., & Asaduzzaman, M. (2021). Analyzing and mitigating attacks in IoT smart home using STRIDE. *Proceedings of the International Conference on Innovations in Science, Engineering and Technology (ICISET)*, Daffodil International University.

Roy, S. C., Saha, D., Kabir, S. M., & Hossain, A. (2021). Cybersecurity threat modeling for IoT-integrated smart solar systems. *2021 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, KUET.

Al Asif, M., Mahmud, M. A. P., & Islam, M. R. (2022). STRIDE-based cyber security threat modeling for IoT-enabled precision agriculture systems. *International Journal of Engineering and Advanced Technology*, 11(3), 52–60.

Subhash, A., Shah, A., & Shaikh, N. (2020). Threat modelling using STRIDE: An integrated framework to enhance security. *International Journal of Computer Applications*, 177(23), 19–25.

Margaret, M., & Willie, A. (2023). *Cybercrime and its impact on Nigeria's digital economy*. International Journal of Information Security Studies, 9(1), 45–58.

Sani, I. M., & Idris, I. (2023). *Smart financial fraud detection in the digital economy: Cybersecurity strategies for Nigeria*. Centre for Cybersecurity Research and Digital Finance Policy Brief.

Lazarus, S. (2023). *Cybercriminal networks and operational dynamics of business email compromise (BEC) scammers: Insights from the Black Axe confraternity*. *African Journal of Criminology and Justice Studies*, 14(2), 122–141.

Ohakwe, C. G. (2023). *The rise of ransomware attacks in Nigeria*. Nigerian Cybersecurity Intelligence Digest, 8(1), 32–47.

Idris, I., Olalere, M., Egigogo, A. R., Ojeniyi, J. A., & Abisoye, O. A. (2023). Development of a hybridised CNN-BiGRU framework for detection of website phishing attacks. *Journal of Advanced Computing and Machine Intelligence*, 5(2), 101–115.

Idris, I., Olalere, M., Egigogo, A. R., Ojeniyi, J. A., & Abisoye, O. A. (2023). Development of a hybridised CNN-BiGRU framework for detection of website phishing attacks. *Journal of Advanced Computing and Machine Intelligence*, 5(2), 101–115.

Lazarus, S. (2023). *Cybercriminal networks and operational dynamics of business email compromise (BEC) scammers: Insights from the Black Axe confraternity*. *African Journal of Criminology and Justice Studies*, 14(2), 122–141.

Ohakwe, C. G. (2023). *The rise of ransomware attacks in Nigeria*. *Nigerian Cybersecurity Intelligence Digest*, 8(1), 32–47.

Sani, I. M., & Idris, I. (2023). *Smart financial fraud detection in the digital economy: Cybersecurity strategies for Nigeria*. Centre for Cybersecurity Research and Digital Finance Policy Brief.

Adebiyi, P. (2023). *Cybersecurity in Nigeria: Real threats, real impact*. Lagos: CyberSecure Publications.

Ayanbode, N., Abieba, O. A., Chukwurah, N., Ajayi, O. O., & Daraojimba, A. I. (2023). Addressing insider threats and behavioural anomalies in cybersecurity. *International Journal of Information Security and Digital Ethics*, 11(3), 211–229.

Idris, I., & Damilola, A. N. (2023). *Metadata analysis of insider threats*. Nigerian Institute of Cybersecurity Research Technical Report Series.

Idris, I., & Mustafa, Z. S. (2023). *Malware and digital forensics in insider threat investigations*. *Journal of Digital Evidence and Information Security*, 10(2), 89–104.

Ado, M. N., Abdulhamid, S. M., & Idris, I. (2023). A Multi-Tier Threat Intelligence Architecture for Proactive Detection of Cryptocurrency-Facilitated Cybercrimes. Nigerian Journal of Science and Technology Research, 5(1), 100–112.

Akintunde, A., Fajemirokun, A., & Bello, K. (2022). Understanding Blockchain Obfuscation in Nigerian Cybercrime Networks. Journal of Cybercrime Studies, 6(2), 122–137.

Doris, M. I., & Uchenna, C. J. (2023). Crypto-Lured Romance Scams in Sub-Saharan Africa: Psychological and Legal Dimensions. African Journal of Digital Justice, 4(1), 33–50.

Idris, I., Abdulhamid, S. M., & Akinyemi, L. (2022). Security Risk Analysis in Electronic Payment Switching Systems in Nigeria: A Case Study of eTranzact International Plc. Journal of Financial Technology Studies, 4(2), 55–72.

Idris, I., & Nuraddeen, M. (2025). Secure Smart Financial Ecosystems: Towards Blockchain-Integrated Fraud Prevention. NJSTR, 5(3), 218–229.

Idris, I., Ado, M. N., & Abdulhamid, S. M. (2024). Intelligence-Based Modelling of Cryptocurrency Transaction Forensics for Scam Detection. International Journal of Cyber Intelligence and Security Research, 6(1), 44–59.

Lim, C. H. (2025). Romance Fraud and Crypto-Based Deception: A Global Forensic Analysis. Journal of International Financial Crime, 17(1), 88–103.

Odum, E., Opara, F., & Nwachukwu, A. (2021). The Rise of Synthetic Romance Scams in Nigeria's Digital Space. West African Journal of Internet Law, 3(4), 72–89.

Rasool, A., & Zahid, M. (2025). Jurisdictional Challenges in Cross-Border Crypto Fraud Investigations. Journal of Global Cybersecurity Policy, 8(2), 99–115.

Regula Forensics. (2024). How to Detect Deepfakes: Signs, Tools, and Technologies. Retrieved from https://regulaforensics.com/blog/how-to-detect-deepfakes/

Muhammad Nuraddeen Ado , Shafii Muhammad Abdulhamid , Ismaila Idris. A Multi-Tier Edge–Fog Intelligent Learning Framework for Detecting Financial Anomalies in Smart Cities. Preprints.org. 31 May 2025 doi: 10.20944/preprints202505.2491.v1

Mohammad Umar Majigi, Ismaila Idris, Shafii M. Abdulhamid, Richard Adeyemi Ikuesan. Block Chain Based Zero Knowledge Proof Model for Secure Data Sharing Scheme in a Distributed Vehicular Networks. FUDMA Journal of Science. 2023.

Muhammad Umar Majigi, Richard A Ikuesan, Ismaila Idris, Shafi'i Muhammad Abdulhamid. Blockchain-Based Enhanced Secure Data Storage Model: A Framework for the Internet of Vehicle

Networks. 2025 13th International Symposium on Digital Forensics and Security (ISDFS). IEEE Xplorer.

Ismaila Idris, Ilyas Adeleke, Andrew Anogie Uduimoh, Joshua J. Tom. Design Framework of Cyber Security Solutions to Threats and Attacks on Critical Infrastructure of Electricity Power Systems of Nigeria Companies. International Journal of Computing, Intelligence And Security Research (Ijcisr), vol. 2-1, 2023. (ISSN 2736-0032(ONLINE) ISSN 9876-5432(PRINT)

Isah Abdulkadir Onivehu, Alhassan John Kolo, Idris Ismaila, Adebayo Olawale Surajudeen, Onuja, A.M. Investigation of Vulnerabilities of Oil and Gas Critical Infrastructures and Developing a Tracking Algorithm to Track Malicious Attacks on the Stream. 3rd International Engineering Conference (IEC 2019) p573-580

Chataut, R., Phoummalayvane, A., & Akl, R. (2023). Unleashing the power of IoT: A comprehensive review of IoT applications and future prospects in healthcare, agriculture, smart homes, smart cities, and industry 4.0. Sensors, 23(16), 7194.

Mosud, Y.O., Ajulo, E.B. & Yinusa, A.B, Internet of Things (IoT) Security and Private Concerns: An Overview.

Adelusi, B. S., Ojika, F. U., & Uzoka, A. C. (2023). Quantum-Resistant Cryptographic Protocols: Securing Financial Transactions and Protecting Sensitive Business Data in the AI Era. Gyanshauryam, International Scientific Refereed Research Journal, 6(2), 152-184.

Oyeniran, O. C., Adewusi, A. O., Adeleke, A. G., Akwawa, L. A., & Azubuko, C. F. (2023). Advancements in quantum computing and their implications for software development. Computer Science & IT Research Journal, 4(3), 577-593.

Waziri, V. O., Alhassan, J. K., Morufu, O., & Ismaila, I. (2014). Big Data Analytics and the Epitome of fully Homomorphic Encryption Scheme for Cloud Computing Security. International Journal of Developments in Big Data and Analytics, 1(1), 19-40.

Muhammad Nuraddeen Ado , Shafii Muhammad Abdulhamid , Ismaila Idris. A Multi-Tier Edge–Fog Intelligent Learning Framework for Detecting Financial Anomalies in Smart Cities. Preprints.org. 31 May 2025 doi: 10.20944/preprints202505.2491.v1

Sule Aishat A, Alhassan John K, ***Ismaila Idris***, Alabi Isiaq O, Subairu Sikiru O. A Review of Deep Belief Networks in Intrusion Detection Systems: Applications, Optimization Techniques, and Dataset Utilization. Ceddi Journal of Information System and Technology (JST) ISSN: 2829-808X (print) Vol. 4 No. 1 April (2025)

Abdullahi Raji Egigogo, ***Ismaila Idris***, Morufu Olalere, Opeyemi Aderike Abisoye, Joseph Adebayo Ojeniyi. Development of a Hybridized CNN-BiGRU Framework for Detection of Website Phishing Attacks. NIPES - Journal of Science and Technology Research 7(2) 2025 pp. 263-274 eISSN-2682-5821, pISSN-2734-2352

Wabi, A. A., ***Idris, I.,*** Olaniyi, O. M., & Ojeniyi, J. A. (2024). Computers & Security DDOS attack detection in SDN : Method of attacks , detection techniques challenges and research gaps. *Computers & Security*, *139*(January 2023), 103652. https://doi.org/10.1016/j.cose.2023.103652

Splunk Inc. (2023). Splunk Security Information and Event Management (SIEM) Overview.

Wagner, C., Dulaunoy, A., Wagener, G., & Iklody, A. (2016). MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform. In Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security (pp. 49–56).

Egigogo, A. R., Idris, I., Olalere, M., Abisoye, O. A., & Ojeniyi, J. A. (2025). Development of a hybridized CNN-BiGRU framework for detection of website phishing attacks. *NIPES Journal of Science and Technology Research*, 7(2), 263–274.

Idris, I., Adeleke, I., & Uduimoh, A. A. (2023). Design framework of cybersecurity solutions to threats and attacks on critical infrastructure of electricity power systems of Nigeria companies. *International Journal of Computing, Intelligence and Security Research*, 2(1).

Idris, I., & Damilola, A. N. (2023). Systematic literature review and metadata analysis of insider threat detection mechanism.

International Journal of Computer Science and Mobile Computing, 12(4), 60–88.

Olalere, M., Raji, A. E., Idris, I., Jimoh, R. G., & Adebayo, O. S. (2019). Assessment of information security awareness among online banking customers in Nigeria. *International Journal of Advanced Research in Computer Science and Software Engineering*, 4(6), 123–132.

Wabi, A. A., Idris, I., Olaniyi, O. M., & Ojeniyi, J. A. (2024). DDoS attack detection in SDN: Method of attacks, detection techniques, challenges and research gaps. *Computers & Security*, 139, 103652. https://doi.org/10.1016/j.cose.2023.103652

Waziri, V. O., Alhassan, J. K., Idris, I., & Suleiman, I. (2015). The application of hybrid cryptographic algorithms for cyber warfare and terrorism in a nation defence. *International Journal of Advanced Research in Computer Science and Software Engineering*, 5(3), 110–117.

Chainalysis. (2024). *The 2024 geography of cryptocurrency report*. Chainalysis. https://go.chainalysis.com/2024-geography-of-cryptocurrency.html

Economic and Financial Crimes Commission (EFCC). (2024, May 15). *EFCC secures 3,175 convictions, recovers ₦156 billion in one year*. EFCC Nigeria. https://www.efcc.gov.ng/efcc/news-and-information/news-release/10136-efcc-secures-3-175-convictions-recovers-n156-billion-in-one-year

Economic and Financial Crimes Commission (EFCC). (2024, December 16). *EFCC bursts syndicate of 792 cryptocurrency investment/romance fraud suspects in Lagos; arrests 193 Chinese, Arabs, Filipinos, others*. EFCC Nigeria. https://www.efcc.gov.ng/efcc/news-and-information/news-release/10584-efcc-bursts-syndicate-of-792-cryptocurrency-investment-romance-fraud-suspects-in-lagos-arrests-193-chinese-arabs-filipinos-others

Federal Trade Commission (FTC). (2022, February 9). *Romance scams cost consumers $1.3 billion in 2022*. Federal Trade Commission.

https://www.ftc.gov/news-events/press-releases/2023/02/romance-scams-cost-consumers-13-billion-2022

Interpol. (2023, November 17). *INTERPOL identifies top cyberthreats in Africa*. Interpol. https://www.interpol.int/en/Crimes/Cybercrime/INTERPOL-identifies-top-cyberthreats-in-Africa

Nairametrics. (2025, July 10). *Financial fraud in Nigeria surges by 45%, 70% of losses linked to digital platforms – CBN*. Nairametrics. https://nairametrics.com/2025/07/10/financial-fraud-in-nigeria-surges-by-45-70-of-losses-linked-to-digital-platforms-cbn/

Oak, A., & Shafiq, M. (2025). Psychological and financial harm of cryptocurrency romance scams. *Journal of Cybercrime Studies, 12*(1), 45–62. https://doi.org/10.xxxx/jcs.2025.0012

Reserve Bank of Australia. (n.d.). *What is cryptocurrency?* Reserve Bank of Australia. https://www.rba.gov.au/education/resources/explainers/what-is-cryptocurrency.html

Reuters. (2024, December 16). *Almost 800 arrested over Nigerian crypto-romance scam*. Reuters. https://www.reuters.com/world/africa/almost-800-arrested-over-nigerian-crypto-romance-scam-2024-12-16

Reuters. (2025, August 21). *Nigeria deports 102 foreign nationals convicted of cybercrime*. Reuters. https://www.reuters.com/world/china/nigeria-deports-50-chinese-nationals-cybercrime-crackdown-2025-08-21

U.S. Department of Justice (DOJ). (2025, January 12). *Justice Department secures $225 million in cryptocurrency linked to pig-butchering romance scams*. United States Department of Justice. https://www.justice.gov/opa/pr/justice-department-secures-225-million-cryptocurrency-linked-pig-butchering-romance-scams

GlobalSign. (2017, August 1). What is the Internet of Things (IoT) and how does it work? GlobalSign. https://www.globalsign.com/en/blog/what-internet-things-and-how-does-it-work

Terekhin, A. (2023, August 17). Are deepfakes truly a challenge for standard ID verification tools? Regula Forensics. https://regulaforensics.com/blog/how-to-detect-deepfakes/

Rietsche, R., Dremel, C., Bosch, S., Steinacker, L., Meckel, M., & Leimeister, J.-M. (2022). Quantum computing. *Electronic Markets, 32*(3), 2525–2536. https://doi.org/10.1007/s12525-022-00570-y

Omodunbi, B. A., Olaniyan, O. M., Esan, A. O., & Oluwasanmi, O. A. (2016).
Cybercrimes and challenges of cyber security in Nigeria. *Journal of Information Security, 7*(2), 97–106. https://doi.org/10.4236/jis.2016.72008

IBM. (2023). IBM. Retrieved from *https://www.ibm.com/think/topics/quantum-computing*

PostQuantum. (2023). Quantum parallelism and how it powers quantum computing. Retrieved from *https://postquantum.com/quantum-computing/quantum-parallelism/*

Usecure. (n.d.). usecure blogs Retrieved September 6, 2025, from *https://www.usecure.io/en/*

Infradapt. (n.d.). The benefits and risks of adopting IoT. Retrieved September 6, 2025, from *https://www.infradapt.com/news/the-benefits-and-risks-of-adopting-iot/*

FortiGuard Labs. (n.d.). FortiGuard: Security intelligence and research. Retrieved September 6, 2025, from *https://www.fortiguard.com/*

PROFILE OF THE INAUGURAL LECTURER

Professor Ismaila Idris (BTech., MSc., PhD., FCSEAN., MCPN, MNCS); a Fellow of Cyber Security Expert Association of Nigeria was born in Yawa, Lapai Local Government to the family of Late Alhaji Ismaila Suleiman and Hajiya Khadijat Ismaila. He is married to Mallama Hauwa Idris and was blessed with lovely children (Khadijat, Ruqqaya and Ismail). After his Primary and Secondary education in Ilorin, he proceeded to Federal University of Technology of Technology, Minna were he obtained Bachellor of Technology degree in Mathematics and Computer Science in 2002. Masters of Science degree in Computer Science at University of Ilorin, Nigeria in 2009 and Doctor of Philosophy degree in Computer Science (Area of specialization is Information Security) at the Universiti Teknologi Malaysia in 2014.

A Professor of Cyber Security with the department of Cyber Security Science, Federal University of Technology, Minna. His multidisciplinary expertise spans cybersecurity, information security, artificial intelligence, machine learning, data science, data analytics, data mining, computational intelligence, digital forensics, software engineering, intelligent systems, cloud computing, Internet of Things (IoT) security, blockchain technologies, secure software development, privacy engineering, and digital transformation. His research focuses on developing intelligent, secure, and data-driven solutions to contemporary challenges facing governments, industries, and society. He has authored numerous high-impact scholarly publications, supervised and mentored undergraduate and postgraduate researchers, contributed to national cybersecurity policies and curriculum development, and actively promotes interdisciplinary research that bridges cybersecurity with AI and emerging technologies.

He held the Position of Head of Department from July, 2019 to June, 2025. As Head of Department, he oversees the first accreditation ever carried out for Cyber Security in Nigeria by NUC in 2019. The Department was given status of full Accreditation. His tenure also oversees the second accreditation in 2024, which was also full accreditation. He has taught over twenty courses at undergraduate and

fifteen courses at postgraduate levels. He has supervised over one hundred undergraduate projects, fifty masters theses and ten PhD theses. He is still actively involved in teaching, research, supervision of undergraduate and postgraduate students. He has held the following positions in the university: School of Information and Communication Technology Examination Officer, 2014-2016; Postgraduate Coordinator, 2014-2016; Deputy Director, Information Technology Services, 2017-2019; Member, Committee to Develop ICT Policy Document for Federal University of Technology, Minna, 2019; Head, Department of Cyber Security Science, 2019-2025; He as been in the IT domain for over 2 decades with local and international acceptance. This is evidence with over 100 published article both locally and internationally in high impact scientific journals, conference proceedings and 7 book chapters. He has attended and presented papers at International and National conferences, within and outside Nigeria. The global acceptance of his research in the field of Cyber Security results in two of his research been patented at Innovation Commercialization Center, Malaysia. He is a reviewer for many International and National Journals. He has served as a resource person for NECO, NOUN and NUC for several resource verification and accreditation exercises. He has served as external examiner for both undergraduate and postgraduate programmes in several Nigeria Universities. He was amongst five (5) member committee that started the Cyber Security Expert Association of Nigeria in 2015; He serves as the pioneer National Vice President of the Association from 2015-2023. He is currently a member, board of trustees of the Association. Other administrative responsibilities are appointment by Federal Executive Council as Member of Steering Committee for the Device Management system (DMS) Solution. 2023; The only academic member in a Committee Convened by the office of the National Security Adviser to Review the National Cybersecurity Policy and Strategy 2014 and Formulated the National Cybersecurity Policy and Strategy 2020 which was signed into law by formal President Muhammadu Buhari in 2021. Chairman, Committee on Digital Policing and Forensics, Federal University of Technology, Minna. Obtained best PhD graduating

student in 2014 at Faculty of Computing, Universiti of Teknologi Malaysia. Secured grant for Cyber Security Solutions for Electricity Power Systems (EPS) Data Analytics for the Nigeria Electricity Supply Industry (NESI). Contributed in the writing of some Cyber Security text books and editor to all Cyber Security text books for Africa Center of Excellence on Technology Enhanced Learning (ACETEL) which is a World Bank Project at National Open University of Nigeria. He is a Fellow of the Cyber Security Experts Association of Nigeria (CSEAN), Computer Professionals Registration Council of Nigeria (CPN), Nigeria Computer Society (NCS), International Association of Engineers, (IAE), Internet Society, (ISOC) and IEEE, Computer Chapter.

As the Fourth Industrial Revolution continues to reshape society through artificial intelligence, big data, automation, cloud computing, and intelligent digital systems, Professor Idris exemplifies the qualities of an inspiring academic, visionary researcher, technology leader, and lifelong learner. His career demonstrates that innovation, scientific excellence, ethical leadership, continuous learning, and interdisciplinary collaboration are essential for building secure, intelligent, and sustainable digital societies. His enduring legacy continues to inspire students, researchers, professionals, and future leaders to harness technology responsibly for national development and global impact.

ISSN 2550 - 7087
2550 7087