Securing the digital future in the age of AI

CYBER SECURITY

SARAH AHURA

Sarah Ahura

Artificial Intelligence (AI) is redefining how societies operate, shaping how citizens access services, how governments plan, how businesses function, and how economies grow. Uganda is no exception.

Through the expansion of e-government platforms, mobile money, digital health systems, and a vibrant fintech ecosystem, AI has become an important driver of the country's socio-economic development. However, as Uganda advances along its digitization journey, a critical challenge emerges: how to secure a world where machines think, learn, and increasingly operate faster than humans.

AI offers immense promise. It enables faster and more efficient decision-making in public service, improves fraud detection in banking, strengthens disease surveillance in healthcare, and supports farmers with real-time advisory services.

These innovations support Uganda's ambition to build a modern, efficient, and globally competitive economy.

Yet the same technology is also reshaping the cyber threat landscape. Around the world, cybercriminals are using AI to generate deepfake voices and videos that impersonate senior leaders, craft highly convincing phishing messages that bypass traditional security filters, deploy self-learning malware that adapts to evade detection, and automate attacks at unprecedented speed and scale.

Cybercrime is no longer slow or visible; it is intelligent, automated, and increasingly difficult to detect.

Uganda's digital transformation has also expanded its risk exposure. As more services move online, from tax systems and land registries to Sacco platforms, mobile banking, and digital payments, the nation's digital footprint continues to grow.

While this expansion improves access and efficiency, it also creates more entry points for attackers.

Amplified

"AI will amplify everything the good, the bad, and the dangerous. Security must keep up.'

Across the region, cyber incidents affecting governments, financial institutions, and critical infrastructure are on the rise.

Uganda is not immune. A single cyber breach can disrupt essential services, undermine public confidence, compromise sensitive national data, and result in significant financial losses. In a digitally connected economy, cybersecurity failures quickly become national security and economic stability concerns.

Despite advances in technology, human behaviour remains one of the most significant vulnerabilities. Weak passwords, careless clicks on malicious links, and the use of unsecured personal devices for official work can compromise even the most sophisticated systems. In the AI era, cybersecurity is no longer just a technical challenge; it is a cultural one.

Uganda's digital safety depends as much on informed and vigilant users as it does on advanced security technologies. Uganda has made important progress in building a cybersecurity foundation, including the enactment of the Data Protection and Privacy Act (2019), the National Information Security Framework, and regulatory oversight by NITA-U.

However, the AI age demands faster, more adaptive, and more intelligent responses. Manual monitoring alone can no longer keep pace with AI-driven attacks.

Government agencies and critical sectors such as finance, energy, health, security, and ICT must adopt AI-enabled security tools capable of detecting and responding to threats in real time.

Equally important is developing a skilled cybersecurity workforce. Uganda faces a significant talent gap in areas such as machine learning, security, digital forensics, cloud security, and AI ethics.

Addressing this gap requires sustained investment in education, training, and professional development through universities, technical institutions, and national programs.

Cybersecurity compliance must also be treated as a governance priority rather than an IT afterthought. Regulators should ensure that banks, telecoms, Saccos, health facilities, and technology firms adhere to established security standards.

At the same time, AI systems used in public services must be ethical, transparent, auditable, and free from bias to maintain public trust and protect citizens' rights.

Ultimately, cybersecurity is a shared national responsibility. Government, the private sector, academia, civil society, and citizens all have a role to play.

Simple actions, such as using strong and unique passwords, enabling two-factor authentication, verifying information before sharing, reporting suspicious activity, and exercising caution with unsolicited messages, collectively form the country's first line of defence.

In the AI era, securing Uganda's digital future is about more than protecting data. It is about safeguarding national sovereignty, strengthening public trust, and ensuring that technology remains a force for inclusive growth and sustainable development.

The writer is a risk analyst at NITA-U