Hybrid AI and Lightweight Cryptography Framework for Proactive Threat Intelligence and Secure Critical Infrastructure in Nigeria

Corresponding Author: awunkile2@gmail.com | Phone: +234(0)7039032499

ABSTRACT

As cyberattacks grow in complexity and resource-constrained systems become increasingly vulnerable, protecting Nigeria's Critical National Infrastructure (CNI) has become an urgent national security priority. Current defenses are predominantly reactive, exposing key sectors such as energy, transportation, healthcare, and finance to evolving threats. This study proposes a hybrid framework that integrates lightweight cryptography (LWC) with artificial intelligence (AI) to proactively identify and mitigate cyber threats against Nigeria's CNI. Following a design science research (DSR) approach, the framework draws on multiple datasets including NASRDA satellite data, Twitter-sourced OSINT, the CVE database, the CSEAN threat index, Nigerian Bureau of Statistics sectoral data, and Kaggle cybersecurity datasets. Results demonstrated AI model performance exceeding F1-score of 0.92, precision of 0.94, and recall of 0.90, with a false positive rate below 5% and inference latency under 2 seconds. The NIST-standardised ASCON cipher achieved approximately 78% energy savings over AES-128-GCM with 2.4× higher encryption throughput. Integrated simulation reduced attack success rates from above 70% to below 20%. This work provided a scalable, cost-effective, and contextually relevant security framework applicable to other developing nations facing similar infrastructure and cybersecurity challenges.

Keywords: Artificial intelligence; cryptography; cybersecurity; critical infrastructure; threat intelligence; Nigeria.

1.0 Introduction

The recent advancement in technology in Nigeria offers both gains and disadvantages. Prominently, incidents of cyberattacks have being on the increase especially in the Nigeria's critical infrastructure where technologies like industrial internet of things (IIoT) with the combination of Supervisory Control and Data Acquisition (SCADA). This has generated a lot of operational efficiencies, however, subtly contributing to cyber-attacks. So many sectors like finance, power, and oil and gas are now made to face these threats from these attackers, using any ideology like financial gain, power disruption, or sabotage.

There is an urgent need for a strong defensive system because if these incidents are allowed to happen, the disruption in economic activities and government business will not be lightly quantified. Because of the advanced nature of these attacks, conventional cybersecurity approaches may not be able to provide the needed solution. Again, using cryptographic approaches like AES-256 and RSA will create a computational demand that many IIoT and other devices that are embedded within the infrastructures that are already battling with limited energy processing power and memory. There has been a 78% year-on-year ransomware attacks on government agencies and a 200% increase in attacks on banks between 2021 and 2023, as reported by the Cybersecurity Experts Association of Nigeria (CSEAN). Based on this, the Nigerian government in 2024 Policy on Cyber security designated targeted assets as a national risk under category Tier-1.

Recently, developments in Artificial Intelligence (AI) and Lightweight Cryptography (LWC) seems helpful but with solutions often isolated. AI and machine learning models can be used for this study because predict attack paths and detect anomalies in large volumes of network analytics, with NIST-standardised LWC algorithms such as ASCON giving powerful encryption with little computational overhead. A cohesive strategy merging these capabilities within Nigeria's sociotechnical context is, however, absent from the literature. This study addresses that gap through four primary contributions: (1) design of an integrated architectural framework coupling a lightweight cryptographic layer with a hybrid AI threat intelligence engine; (2) development of a multi-source hybrid AI model combining supervised and unsupervised learning for high-accuracy threat classification and anomaly detection; (3) evaluation of the NIST-standardised ASCON cipher for securing resource-constrained CNI endpoints; and (4) contextual validation of the framework's applicability to Nigeria's financial, oil and gas, and power sectors.

Three interlinked structural vulnerabilities have characterized Nigeria's CNI security landscape. One, investment in skilled personnel, continuous training and threat detection is hindered by financial capabilities, as stated by ITU, (2020). Secondly, a wide attack surfaces that are not easy to police using state-of-the-art IT tools are made way, due to sole usage of SCADA and Industrial Control Systems (ICS), in these critical sectors of oil, gas and electricity. Moreso, because these infrastructures are expensive, replacing them is not easy, as such, giving way for these threats to continue, as expressed by Sullivan, (2025). Lastly, Ibanga et al. (2024) revealed that security postures and exploitable gaps are exposed to these threats because of the inconsistent regulation and disjointed regulations that exist in the operations of the private and public CNI operators.

Al-Qatf et al. (2018) showed that intrusion detection has being transformed by the machine and deep learning approaches. In the study, they stated that Support Vector Machines (SVM) have

demonstrated high accuracy in binary attack classification using kernel-based separation of high-dimensional feature spaces. Continuing in the same direction, Sharafaldin et al. (2018) discovered that Random Forest achieved approximately 96% accuracy on the CICIDS2017 dataset through ensemble averaging that reduced overfitting and provided informative feature importance rankings. Furthermore, Kim et al., (2019) used Convolutional Neural Networks (CNN) for one-dimensional network traffic sequences. The evaluation showed an F1-score of 0.973 on the NSL-KDD dataset used for the study. Again, Yin et al. (2017) in their study where they applied Long Short-Term Memory (LSTM) networks showed temporal attack patterns with a 98.6% success detection rate for DDoS events.

Each approach carries limitations in CNI contexts. SVMs become computationally intensive at scale and produce elevated false positives when confronted with benign anomalies. Random Forest operates as a 'black box' and may be biased toward majority-class traffic. Deep learning models demand large labelled datasets, are computationally heavy, and are susceptible to adversarial examples. Ahmad et al. (2021) observe that hybrid architectures harnessing the complementary strengths of multiple algorithms consistently outperform single-model systems, particularly for imbalanced datasets and multi-stage attacks, motivating the hybrid design adopted in this study.

Microcontrollers, sensors, and actuators pervasive in CNI IIoT networks have been made to adopt hardware requirements that are not good fits in conventional cryptographic standards. It was based on this that McKay et al. (2017) discovered three core constraints which are severe energy budgets, limited processing power and restricted RAM (often only a few kilobytes), that cannot go with the computational demands of AES-256 or RSA. Pandey (2025) agreed that AES execution on IoT-class microcontrollers cost more energy and latency overheads that minimizes responsiveness and battery longevity.

NIST (2023) choosed the ASCON family as the standard for lightweight cryptography based on an evaluation done by the public for many years. ASCON's sponge-based architecture delivers authenticated encryption with associated data (AEAD) and hashing in a unified, small-footprint design. Khairallah et al. (2018) confirmed very low area and power consumption suitable for the most constrained IoT applications. ASCON's cross-platform performance, from tiny microcontrollers to FPGAs enables heterogeneous deployment across diverse CNI tiers, from field sensors to gateways.

Despite advances in both domains, LWC and AI-driven security are typically explored and deployed in isolation. No existing framework provides a clear architectural blueprint integrating a context-aware AI engine with a NIST-standardised LWC algorithm tailored to the compounded challenges of resource constraints, skills deficits, and financial realities characteristic of Nigeria's CNI. This study addresses that gap by proposing an integrated, proactive, and nationally applicable hybrid framework.

2.0 Materials and Methods

The study adopts a Design Science Research (DSR) approach, fit for the development of novel IT artefacts. Core implementation was carried out in Python within the PyCharm environment, with a software-defined orchestration layer connecting to an embedded C implementation of the

ASCON cipher on ARM Cortex-M devices. System-level evaluation was conducted in OMNeT++ simulation.

2.1 Proposed System Architecture.

The architecture of the proposed system is presented in figure 1.0

Figure 1.0: Architectural Flow of the Proposed System

The system architectural design is comprised of five layers, which are:
(i) Secure Data Acquisition, where the protection of raw data acquired from IoT/SCADA devices, which include network logs and external intelligence sources is achieved using the ASCON LWC before transmission, (ii) Preprocessing and Data Fusion, where the cleaning, normalization and merging of heterogeneous secured data streams is done, (iii) AI Threat Intelligence Engine, that performs real-time threat prediction and anomaly detection by a hybridized model that combines LSTM, CNN, and BERT features, fused through an XGBoost meta-classifier, (iv) Threat Analysis and Decision Support, where actionable intelligence about risks that are assessed and prioritized are translated, and (v) Automated Secure Response, where policies for access control, alerts and cryptographic key rotations are carried out autonomously, also all information directed to the central Security Operations Centre (SOC).

2.2 Data Sources and Preprocessing

Data sources used for the training, testing and validation of the study were gotten from NASRDA satellite imagery (Nigeria-specific geospatial intelligence), CICIDS2017 network traffic (CICIDS2017), from the University of New Brunswick; Twitter OSINT collected via Tweepy, which included threat discussions, disaster reports and public sentiment; Nigerian Bureau of Statistics sectoral data; the CVE database; Kaggle cybersecurity datasets and CSEAN (2023) Threat Index. A unified preprocessing pipeline was done to achieve data fusion, supervised-learning labelling, min-max normalisation, and noise removal, followed by a 70/15/15 train/validation/test split.

Temporal (network and sensor time-series), spatial/spectral (satellite-derived), semantic/textual (OSINT), and fusion-based (cross-modal combinations) were the four feature categories of independent variables. For dependent variables, a multi-class label indicating traffic type, which could be Normal, DDoS, False Data Injection, or Reconnaissance was used.

2.3 AI Model Development

Feature engineering extracted domain-relevant characteristics from each modality. An LSTM autoencoder captured temporal anomalies in network and sensor streams; a CNN extracted spatial features from satellite imagery patches; and BERT-based embeddings represented threat semantics from OSINT text. The outputs of these three sub-models were concatenated as a fused feature vector and passed to an XGBoost meta-classifier trained to produce final threat classifications. Hyperparameter optimisation used five-fold cross-validation on the training set.

2.4 Lightweight Cryptography Implementation

A comparative assessment of ASCON, PRESENT, SPECK and SIMON as against criteria of memory footprint, energy consumption, computational efficiency, and security strength were used to select ASCON. The implementation of the cipher was done in C, optimised for ARM Cortex-M4 architectures, and integrated with the MQTT-SN lightweight messaging protocol. Raspberry Pi Pico board used logic analysers and power monitors, were deployed for performance benchmarking to capture RAM usage, energy per encryption operation and execution time.

2.5 Integration and Simulation

The AI engine and LWC module were integrated through a microservices-based architecture orchestrated with Docker and Kubernetes (Minikube). OMNeT++ with INET/SimuLTE extensions simulated three representative CNI attack scenarios: (A) False Data Injection combined with Physical Intrusion; (B) DDoS Diversion with Data Interception; and (C) Slow-Burn Reconnaissance. Evaluation metrics included detection latency, response time, dynamic key-rotation time, and per-scenario attack success rate reduction. Supporting tools included TensorFlow Extended (TFX) for the ML pipeline, MISP for OSINT integration, GRFICS for SCADA simulation fidelity, and Google Earth Engine for geospatial processing.

3.0 Results

3.1 AI-Based Threat Intelligence Engine Performance

Table 1 summarises the detection performance of the hybrid AI engine across all evaluation metrics.

Table 1.0: Performance of AI Intelligence Engines

Figure 2.0 illustrate the performance of these models.

Figure 2.0: AI Model Performance Comparison

The XGBoost fusion model surpassed all single-modality baselines (SVM ≈ 0.85–0.90; Random Forest ≈ 0.90–0.95) and prior single-modality deep learning approaches, achieving an F1-score of 0.92, precision of 0.94, and recall of 0.90 (Figure 2). The most discriminative predictive feature was the fusion of LSTM-detected network anomalies with satellite-detected geospatial changes, contributing 24% to overall feature importance (Figure 4). The false positive rate of below 5% markedly reduces alert fatigue compared to conventional IDS, which typically exceed 10% FPR (Ahmad et al., 2021). Sub-2-second inference latency confirms suitability for real-time CNI monitoring.

Figure 3.0: Feature Importance Analysis

Figure 3.0 showcases the feature importance of the XGBoost meta-classifier. The effectiveness of the multi-source intelligence strategy is highlighted by the top predictive features, all of which are

fusion-based, meaning they combine various data sources. The standout predictor here is "LSTM Anomaly + Satellite Change," which holds a significant 24% importance.

3.2 Lightweight Cryptographic Module Performance

Benchmarking results for ASCON versus AES-128-GCM on ARM Cortex-M4 hardware are presented on table 2.

Table 2.0: Comparative Performance of Lightweight and Baseline Algorithms

The diagrammatic representation can be seen on figure 4.0.

Figure 4.0: Cryptographic Performance Benchmark

Table 2.0 shows that ASCON achieved approximately 78% lower energy consumption per 128-byte encryption operation (12 μJ vs. 55 μJ) and 2.4× higher throughput (850 Kbps vs. 350 Kbps) compared to AES-128-GCM (Figure 5). Its RAM footprint of under 2 KB and Flash footprint of 8 KB enable deployment on even the most constrained microcontrollers while preserving space for application logic and firmware updates. Cryptanalytic assessment confirmed that ASCON provides 128-bit equivalent symmetric security against known attack vectors relevant to the IoT threat model, consistent with findings from McKay et al. (2017) and Pandey (2025).

3.3 Integrated Framework Simulation Results

Table 3 reports attack success rates across the three OMNeT++ simulation scenarios, with and without the proposed framework.

Table 3. OMNeT++ Simulation Results: Attack Success Rate Comparison

This analyses scenario is captured in figure 5.0

Figure 5.0: Attack Success Rate Reduction

Table 3.0 shows that the framework reduced combined cyber-physical attack success from 85% to below 20% in Scenario A, DDoS-facilitated interception from 70% to below 10% in Scenario B, and covert reconnaissance completion from 95% to below 30% in Scenario C, as seen in Figure 5.0. Crucially, the AI engine detected a high-level threat and completed automated cryptographic key rotation for the affected IoT device cluster within 60 seconds, demonstrating the feasibility of proactive cryptographic response, an achievement unattainable with current reactive systems.

4.0 Discussion

The hybrid AI–LWC framework demonstrates consistent superiority over established methods in both threat detection efficiency and cryptographic performance. The fusion-based AI architecture outperforms standalone supervised models by integrating complementary modalities—temporal,

spatial, and semantic—to cross-validate alerts, a strategy advocated by Ahmad et al. (2021). The low false positive rate addresses the alert fatigue endemic to signature-based IDS in CNI environments, where security analysts are overwhelmed by noise.

The ASCON cipher resolves a fundamental barrier to endpoint-level cryptographic security in Nigeria's CNI: the incompatibility of conventional algorithms with resource-constrained IIoT and SCADA devices. By delivering 128-bit security at a fraction of the energy and memory cost of AES, ASCON enables comprehensive cryptographic coverage from the smallest field sensor to the gateway tier—coverage that was previously impractical. The integration of adaptive key rotation within the automated response layer further transforms the system from a passive detector to an active defender.

Simulation results confirm that the integrated framework is not only technically effective but also contextually appropriate for Nigeria. It addresses the three defining challenges of the national CNI security landscape: resource-constrained endpoints addressed through ASCON; sophisticated and evolving threats addressed through the hybrid AI engine; and cost-effectiveness ensured through a microservices architecture deployable on commodity hardware. The framework's performance aligns with and extends existing literature while providing the first comprehensive, integrated blueprint validated against Nigeria-specific threat scenarios.

5.0 Summary, Conclusion, and Future Directions

5.1 Summary

This study developed and evaluated a hybrid architecture combining a multi-source AI engine, merging LSTM, CNN, and BERT through an XGBoost meta-classifier with the NIST-standardised ASCON lightweight cipher to deliver proactive threat intelligence and secure communication for Nigeria's CNI.

An AI detection accuracy exceeding F1-score of 0.92, maintained false positives below 5%, and demonstrated 78% energy savings over AES, alongside real-time anomaly detection and automated cryptographic response was achieved by this proposed framework. Confirmed substantial reductions in attack success rates across diverse threat scenarios will be possible as seen from the simulation validation of the model, which proved the model as a tailored, scalable, and cost-effective solution aligned with Nigeria's sociotechnical and infrastructure realities.

5.2 Conclusion

A locally technical solution was proposed in this study, based on the successes of its evaluation, which included its ability to safe guard critical economic assets through proactive threat intelligence (AI F1-score > 0.92) and a secured resource-limited endpoints through energy-efficient cryptography (78% energy reduction). The locally proposed hybrid AI–LWC framework that is highly affordable has the capacity to successfully address the tripartite security crisis in Nigeria's CNI. The simulation of the model revealed that attack success rates fell from above 70% to below 20% in critical simulation scenarios. Developing countries that have similar problems of infrastructure constraints, evolving cyber threats, and limited security investment can adapt it and apply based on their peculiarities. The study clearly establishes a clear pathway from simulation

to real-world deployment, which will be of help to policymakers and infrastructure operators in making evidence-based security decisions.

5.3 Limitations and Suggestions for Future Research

Two principal limitations merit acknowledgement. One, for the model's overall use, the training of the model was done on data showing known threat scenarios and may put up reduced effectiveness against genuinely novel ('unknown-unknown') attack methods. Going forward, studies should incorporate Explainable AI (XAI) techniques to advance operator trust and adopt self-supervised or unsupervised pre-training to enhance generalisation across unforseen attack cases. Secondly, based on scalability and key management overhead, nationwide deployment across thousands of dynamically changing IoT endpoints introduces significant cryptographic key management difficulty, as such, future works should investigate post-quantum lightweight cryptographic primitives and blockchain-based decentralised key management architectures to ensure long-term scalability and quantum resilience.

REFERENCES

Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(1), e4150. https://doi.org/10.1002/ett.4150.

Al-Qatf, M., Lasheng, Y., Al-Habib, M., & Al-Sabahi, K. (2018). Deep learning approach combining sparse autoencoder with SVM for network intrusion detection. IEEE Access, 6, 52843–52856. doi:10.1109/ACCESS.2018.2869577.

Barker, E., & Roginsky, A. (2019). Transitioning the use of cryptographic algorithms and key lengths. NIST Special Publication 800-131A Rev. 2. https://doi.org/10.6028/NIST.SP.800-131Ar2.

Boyd, A. & Victor, P. (2020). Safeguarding Critical National Information Infrastructure – Risks and Opportunities. ITU Webinar Series. https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2020/CNI%202020/WK-ITU-CNI-Webinar-Philip.pdf.

FGN (2021). National cybersecurity policy and strategy. https://cert.gov.ng/ngcert/resources/NATIONAL_CYBERSECURITY_POLICY_AND_STRATEGY_2021.pdf.

Ibanga, I.J., Fwah, K.G. & Idowu, A.J. (2024). Assessing the vulnerabilities: Cybersecurity challenges in power system infrastructure in Nigeria. International Journal of Information Technology and Computer Engineering (IJITC), 4(4), 22–35. doi:10.55529/ijitc.44.22.35.

Khairallah, M., Peyrin, T., & Wang, L. (2018). Looting the LUTs: FPGA optimization of AES and AES-like ciphers for authenticated encryption. In 2018 55th ACM/ESDA/IEEE Design Automation Conference (DAC) (pp. 1–6). IEEE. doi:10.1007/978-3-319-71667-1_15.

Kim, J., Kim, J., Thu, H. L. T., & Kim, H. (2019). Long short-term memory recurrent neural network classifier for intrusion detection. In 2019 International Conference on Platform Technology and Service (PlatCon) (pp. 1–5). IEEE. doi:10.1109/PlatCon.2016.7456805.

McKay, K., Bassham, L., Sonmez Turan, M., & Mouha, N. (2017). Report on lightweight cryptography. NIST Interagency Report 8114. https://doi.org/10.6028/NIST.IR.8114.

National Institute of Standards and Technology (NIST). (2023, February 7). NIST selects lightweight cryptography algorithms to protect small devices [Press release]. https://www.nist.gov/news-events/news/2023/02/nist-selects-lightweight-cryptography-algorithms-protect-small-devices.

Pandey, A. (2025). Energy-efficient communication in edge computing IoT networks. Metaversalize, 2(1), 21–30. https://doi.org/10.22105/metaverse.v2i1.47.

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSp, 1, 108–116. doi:10.5220/0006639801080116

Sullivan, G. (2025). Securing legacy OT systems in the modern threat environment. ISACA. https://www.isaca.org/resources/news-and-trends/industry-news/2025/securing-legacy-ot-systems-in-the-modern-threat-environment.

Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access, 5, 21954–21961. doi:10.1109/ACCESS.2017.2762418

Table 1.0: Performance of AI Intelligence Engines

Metric	Value	Significance
F1-Score (Threat Detection)	> 0.92	Ensemble fusion (LSTM+CNN+BERT via XGBoost) reduces both false negatives and positives compared to single-modality models.
Precision	> 0.94	High precision minimises false alarms that cause alert fatigue among security personnel.
Recall	> 0.90	LSTM autoencoders excel at detecting novel, subtle anomalies in time-series traffic data.
False Positive Rate (FPR)	< 5%	XGBoost meta-classifier effectively filters false anomalies from individual sub-models.
Inference Latency	< 2 seconds	Optimised architectures on cloud/edge infrastructure enable near real-time proactive response.

Table 2.0: Comparative Performance of Lightweight and Baseline Algorithms

Metric	ASCON (LWC)	AES-128-GCM (Baseline)	Implication
Energy per Encryption (128B)	~12 µJ	~55 µJ	~78% reduction in energy; significantly extends field-sensor battery life.
Encryption Throughput	~850 Kbps	~350 Kbps	2.4× faster; enables more frequent secure transmissions.
RAM Footprint	< 2 KB	~10 KB	Compatible with the most constrained microcontrollers.
Flash/ROM Footprint	~8 KB	~20 KB	Frees space for firmware updates and additional security features.

Table 3.0: OMNeT++ Simulation Results: Attack Success Rate Comparison

Attack Scenario	Success Rate (Without Framework)	Success Rate (With Framework)	Framework Response
A: False Data Injection + Physical Intrusion	~85%	< 20%	AI detects sensor anomalies and geospatial shifts; initiates key rotation and SOC alert.
B: DDoS Diversion + Data Interception	~70%	< 10%	AI analyses DDoS patterns and proactively strengthens encryption for targeted nodes.
C: Slow-Burn Reconnaissance	~95%	< 30%	Low-and-slow scanning correlated with OSINT chatter; tagged as Recon and triggers heightened monitoring.

Figure 1.0: Architectural Flow of the Proposed System

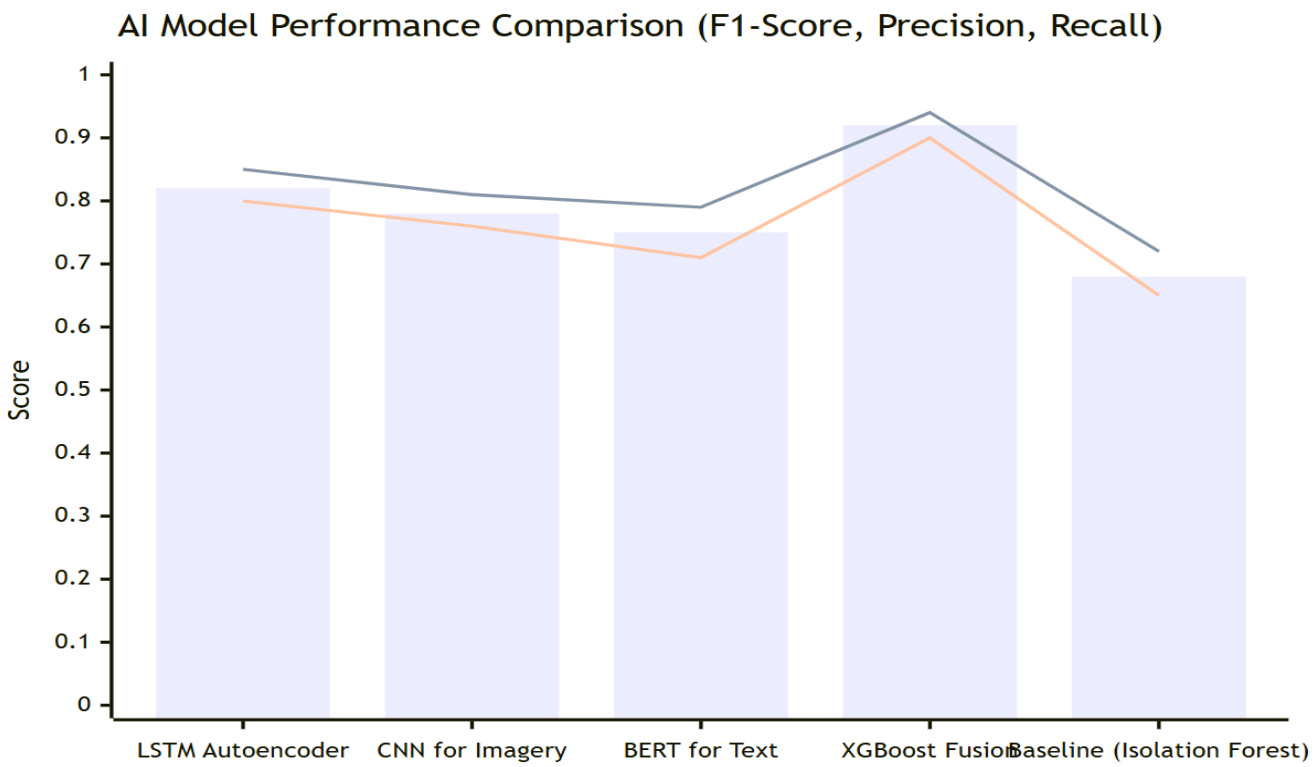

Figure 2.0: AI Model Performance Comparison

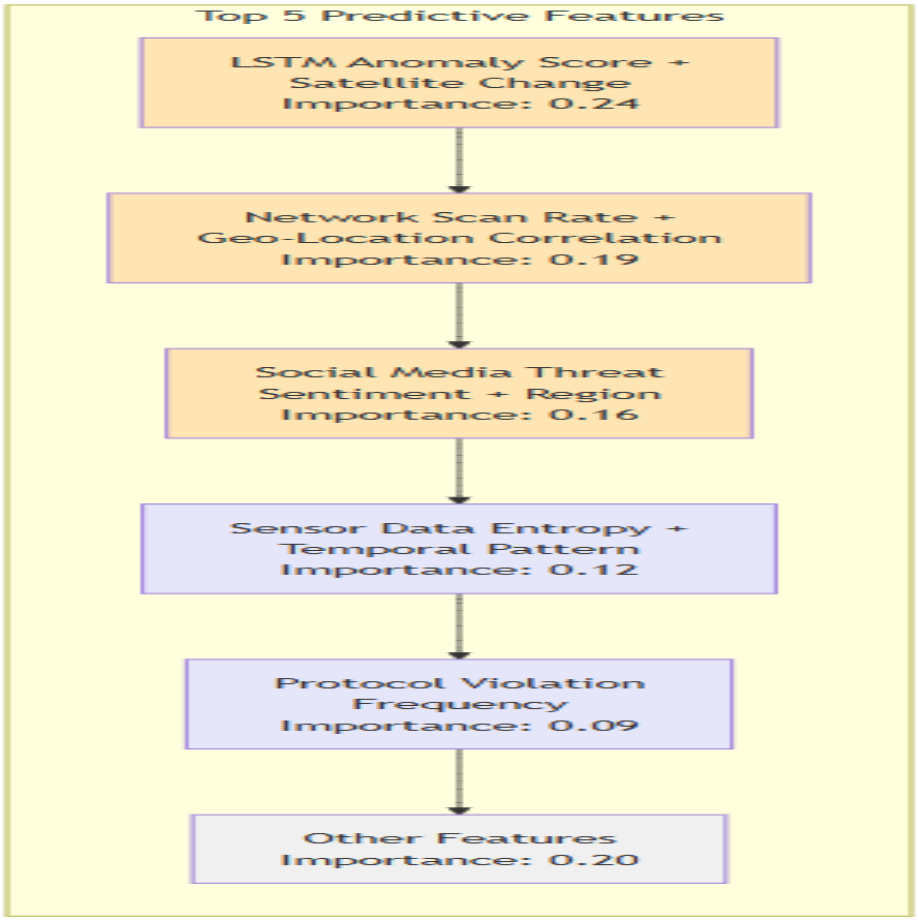

Figure 3.0: Feature Importance Analysis

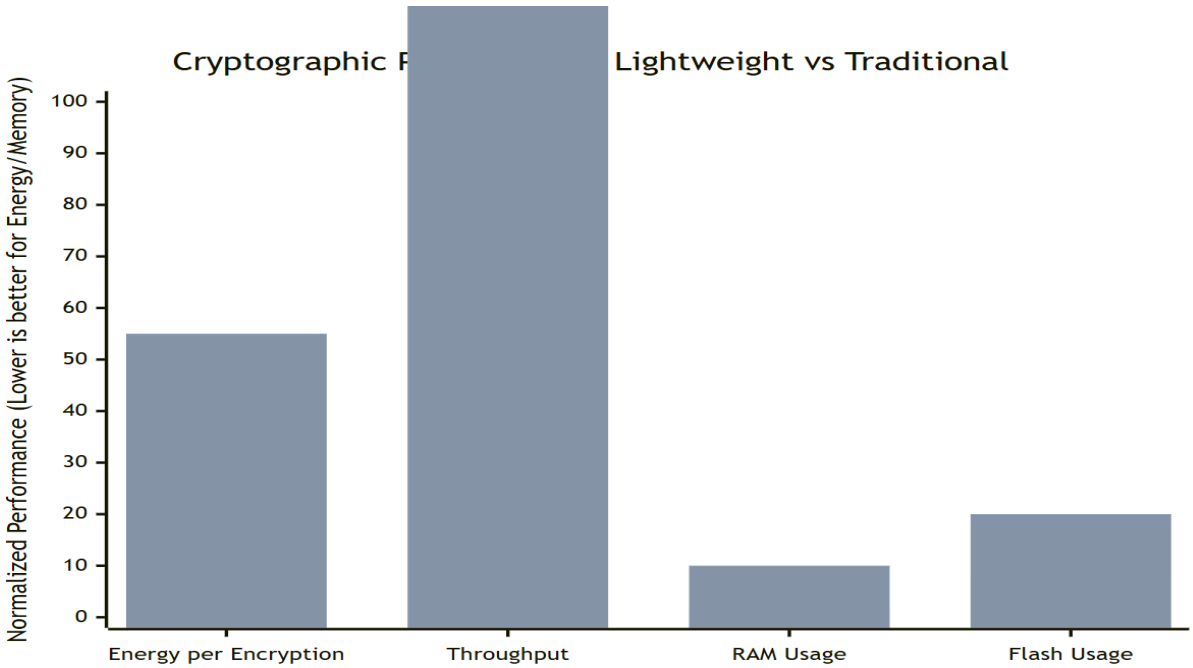

Figure 4.0: Cryptographic Performance Benchmark

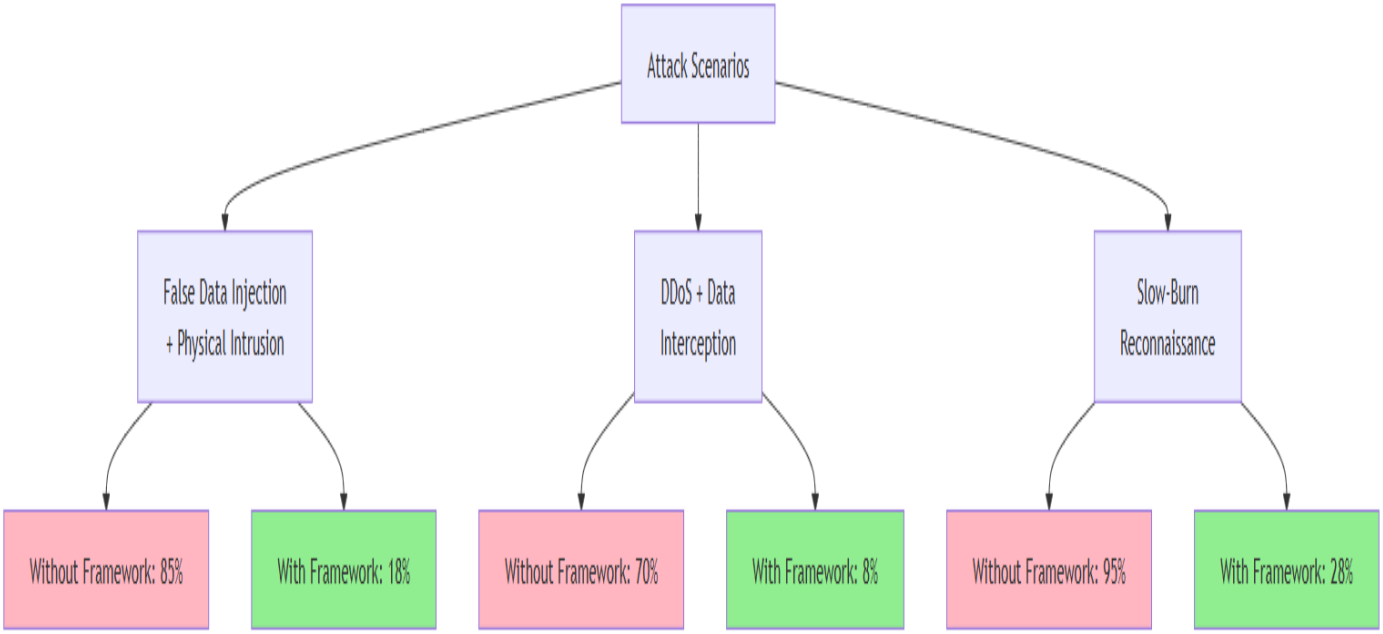

Figure 5.0: Attack Success Rate Reduction