Journal of Theoretical and Applied Information Technology
28th February 2026. Vol.104. No.4

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

PRIVACY-PRESERVING CUSTOMER DATA MANAGEMENT USING HYBRID AI-CRYPTOGRAPHY MODELS

DR. C.NAGA GANESH[1], DR. MAMATHA G[2], DR. VIVEK VEERAIAH[3], DR. DEVIKA RANI ROY[4], AMARJA ADGAONKAR[5], MRS. SUPRIYA SANJAY AJAGEKAR[6], ANKUR GUPTA[7,*], DR. PATIL AMIT MADHUKAR[8]

[1]Assistant Professor, Department of Management Studies, G.Pullaiah College Engineering and Technology (Autonomous), Kurnool, Andhra Pradesh, India
[2]Associate Professor, Department of Management Studies, Sri Siddhartha Institute of Business Management, Tumkur, Karnataka, India
[3]Professor, Department of Computer Science, Sri Siddhartha Institute of Technology, Sri Siddhartha Academy of Higher Education, Tumkur, Karnataka, India
[4]Assistant Professor, Department of Information Technology, K. C. College of Engineering & Management Studies & Research, Thane, India
[5]Assistant Professor, Department of Information Technology, K. C. College of Engineering & Management Studies & Research, Thane, India
[6]Assistant Professor, Department of CSBS, Bharati Vidyapeeth (Deemed to be University), Department of Engineering and Technology, Navi Mumbai, Maharashtra, India
[7]Assistant Professor, Department of Computer Science and Engineering, Vaish College of Engineering, Rohtak, Haryana, India
[8]Assistant Professor, Bharati Vidyapeeth (Deemed to be University), Department of Engineering & Technology, Navi Mumbai, Maharashtra, India
Email: ganeshgpcet@gmail.com, mamthakiran2005@gmail.com, Vivek@ssahe.in, roydevika1992@gmail.com, Adgaonkar123@gmail.com, ssajagekar@bvucoep.edu.in, ankurdujana@gmail.com, amit.patil@bvucoep.edu.in

[*]Corresponding Author: ANKUR GUPTA (ankurdujana@gmail.com)

ABSTRACT

1. INTRODUCTION

Security measures are more important than ever before due to rapidity with which the digital revolution is occurring in many fields [1]. An exciting new direction in the ever-changing field of cybersecurity is the integration of AI with encryption. A number of recent studies have brought attention to the growing popularity of hybrid security frameworks, which combine encryption with AI to guarantee the privacy of sensitive data and make intelligent analysis easier [2]. Additional proposals about the usage of AI-based cryptography models have proliferated. 5G/6G networks, cyber-physical systems, smart cities, healthcare IoT, and secure mobile platforms are just a few examples. Several potential solutions have been considered, such as AI-enhanced post-quantum algorithms, decentralised trust systems enabled by blockchain, machine learning-powered key management, and deep learning-based anomaly detection [4]. Even after making these adjustments, issues persist. No security frameworks exist that are efficient with resources, ethical, or both. The existing approaches are dispersed, inefficient, and unable to handle real-world scenarios or scalability. In addition, the majority of studies neglected to develop a generic architecture capable of keeping up with the dynamic nature of cyber threats in favour of examining individual use cases [6].

Integrating AI with encryption is becoming more apparent in fields other than academia. Data security is becoming more and more important as more and more nations use smart infrastructures, digital financial systems, and autonomous technology. Reason being, these weaknesses might undermine economic growth, public trust, and national security [8]. Without AI-cryptography frameworks that are scalable, transparent, and explainable, there is a risk of future and present threats including adversarial AI assaults, social

engineering using deepfakes, and quantum-enabled cryptanalysis [9]. To create robust, flexible, and morally acceptable security solutions, we must reevaluate the relationship between AI and encryption [11].

Therefore, the purpose of this study is to investigate and develop a state-of-the-art framework for improving security in many domains via the integration of cryptographic protocols with AI-driven learning models. By conducting a comprehensive literature review, identifying significant research gaps, and proposing a new strategy that prioritises scalability, explainability, and preparedness for post-quantum computing, this work aims to theoretically and practically contribute to the expanding field of digital security [15].

1.1 Background

Cryptography protects privacy, integrity, and validity of data over digital networks. For a long time, people have utilised standard cryptographic techniques to keep communications and transactions safe [16]. When AI and cryptography work together, they provide new ways to manage keys intelligently, encrypt data in a way that adapts, create algorithms that are resistant to quantum computing, and detect intrusions on their own [18]. Security breaches in 5G/6G communication networks, healthcare IoT, and blockchain-enabled cyber-physical systems might have big effects on society, the economy, and politics, which makes this convergence even more important [19].

Table 1: Background of the Research

Aspect	Details
Core Foundation	Cryptography ensures confidentiality, integrity, and authentication in digital communication.
Limitations of Traditional Cryptography	Static algorithms like RSA and AES struggle against evolving cyber threats and high-volume dynamic data.
Emergence of AI	AI techniques (ML, DL, RL) provide anomaly detection, pattern recognition, and predictive defense.
Need for Convergence	Combining AI with cryptography enables intelligent key management, adaptive encryption, and quantum-resistant algorithms.
Application Areas	Smart cities, 5G/6G networks, IoT, healthcare, and blockchain-enabled cyber–physical systems.
Research Gap	Current works remain fragmented; lack of a unified, scalable, and explainable framework integrating AI and cryptography.

Most studies mainly look at individual implementations or theoretical questions, therefore the existing corpus of research is still a little scattered, even if there has been more academic attention. Some articles talk on post-quantum cryptography, while others talk about how to use blockchain or AI to find anomalies [20]. At this time, there is no all-encompassing and adaptable framework that unites various methodologies while considering explainability, ethics, and energy efficiency [21]. As digital infrastructures advance towards hyperconnectivity and quantum computing becomes a reality, there is an urgent need for next-generation security models that safely and sustainably integrate cryptography with artificial intelligence [23].

1.2 Motivation

This inquiry was started because there are three big difficulties with current cybersecurity. First of all, standard techniques of cryptography are no longer adequate since cyber threats are becoming more and more complicated [7]. This includes attacks that use quantum technology, ransomware, and AI that works against you [9].

Table 2; Motivation of the Research

Challenge	Motivational Insight
Sophisticated Cyber Threats	Rise of adversarial AI, ransomware, and quantum-enabled attacks necessitates adaptive defenses.
Scalability Needs	IoT devices and 5G/6G networks require lightweight yet robust security mechanisms.
Critical Sectors at Risk	Healthcare, finance, and governance demand transparent and explainable solutions to build trust.
Integration Imperative	AI provides adaptability and prediction; cryptography ensures robustness—together they can form resilient frameworks.
Future-readiness	Quantum computing and hyperconnectivity require proactive, sustainable, and globally aligned security measures.

Together, they can build strong systems that can protect against risks now and in the future, including those posed by quantum computing [6]. The main goal of the project is to create and test a single framework that meets worldwide privacy and security standards and is also technically sound, scalable, easy to use, and easy to understand [9]. The project's purpose is to close the gap between

theory and reality so that digital infrastructures may be safe, reliable, and ready for the future [11].

1.3 Research Questions and Hypotheses

Research Questions (RQs)

Research Questions about adversarial vulnerabilities, bad key management, restricted cryptographic flexibility, and performance restrictions in federated contexts come from gaps in the research that have been found.

RQ1: How can we improve AI-based anomaly detection models such that they can withstand hostile assaults without losing accuracy or using too much processing power in distributed edge settings?

RQ2: How effectively can FL protect privacy and improve model performance when used with secure aggregation, differential privacy, and attack-proof feature extraction?

RQ3: Is it possible for a RL-based adaptive key-management system to choose the best cryptographic primitives depending on the amount of risk, the capabilities of the device, and the state of the network?

RQ4: What is the impact of integrating AI detection, FL training, RL-based key management, and hybrid cryptographic primitives on overall system security, latency, energy consumption, and adversarial robustness?

RQ5: Is it possible for a multi-objective optimisation framework that considers accuracy, robustness, energy, and latency to find a balance that makes it safe and scalable to use in a wide range of IoT and edge networks?

Hypotheses

Based on the suggested system architecture and applicable theoretical frameworks, the following assumptions are formulated:

H1: AI-based anomaly detection that uses adversarial training and autoencoder-based feature extraction will be substantially more accurate at finding anomalies and less likely to be successful at adversarial assaults than baseline methods.

H2: Employing federated learning with differential privacy and secure aggregation will safeguard data privacy without substantially diminishing the model's accuracy and F1-score.

H3: An adaptive key management system based on RL would use less energy and take less time to encrypt data than static or fixed key rotation methods. It will also make security stronger.

H4: When devices have different needs, the hybrid cryptographic selection approach will use less energy and have less delay than single-primitive cryptographic systems.

H5: The AI-FL-RL-Crypto architecture will outperform current, isolated security frameworks across several criteria.

1.4 Contribution of Research

A wide spectrum of people from industry, government, and academia will find the new research findings highly useful and intriguing [9]. The study's proposed integrated framework addresses current challenges related to adversarial robustness, privacy preservation, and secure key management in distributed environments; thus, it will be beneficial for researchers in post-quantum cryptography, federated learning, cybersecurity, and artificial intelligence [10]. The framework shows how to safely use AI-based threat detection on different types of edge devices without slowing down or using too much energy [11]. This will be useful for cybersecurity professionals and system architects in areas like smart cities, healthcare IoT, critical infrastructure, and 5G/6G networks[14]. The results provide policymakers and regulatory agencies a reason to be interested in compliance with new data protection and AI-governance legislation including DPDP, GDPR, and sectoral cybersecurity rules [18].

2. LITERATURE REVIEW

Stressed need of combining cryptography with AI [1]. Bibliometric analysis illustrated cryptographic techniques for AI security and prospective research trajectories and deficiencies [2]. In line with this idea, AI affects the development of cryptographic techniques and may help create long-term security platforms [3]. Secure data management in smart cities, mobile platforms, and precision agriculture via cryptographic protocols that integrate AI has been examined [4]. The adaptability of hybridised security systems is demonstrated by presenting several innovative uses of machine learning to cryptography [5].

The prospective amalgamation of AI and cryptography to tackle 5G security issues amidst the expansion of next-generation networks has been examined [6]. Using machine learning to find threats and protect data is suggested. The state of AI-driven cybersecurity and potential future directions have been discussed [7]. The combination of AI, encryption, and the Internet of Things improves security across many sectors in cyber-physical spaces [8]. Difficulties and possible

remedies associated with privacy-preserving methodologies driven by AI in cyber-physical systems, especially smart contract security, have been explored [9]. A hybrid method incorporating attribute-based encryption with traditional cyphers, including Vigenère and Polybius, is described [10].

There is increasing interest in advanced paradigms, such as blockchain-enabled frameworks and quantum-resistant solutions. AI-driven, quantum-resistant technologies such as federated learning and blockchain in cyber-physical systems have been examined [11]. Integration of deep learning with encryption methods may enhance the prevention of criminal activities on social media [12]. Privacy and ethical considerations in AI-based security are gaining attention [13]. Apprehensions about prospective obsolescence of conventional cryptography have been expressed [16]. Self-learning AI models that can dynamically change 5G cryptography protocols have been proposed [15]. Effects of post-quantum security have also been discussed [16].

Pros and cons of AI-driven big data models in real time have been evaluated [17]. AI and cryptography protocols have been applied across multiple domains [18]. Strategies for fast, safe, and traffic-aware 5G connectivity using deep learning have been suggested [19]. A federated intrusion detection system for healthcare IoT settings that is secure and explainable has been developed [20]. Integrating blockchain technology with AI systems has attracted significant attention [21].

Finally, literature discusses diverse scenarios beyond infrastructural and socio-technical problems. Best practices to regulate AI while balancing safety and creativity have been examined [22]. AI's role in addressing security risks in 6G communications has been reviewed [23], while AI-driven residential power demand forecasting has been investigated [24]. This highlights the use of AI, blockchain, cryptography, and hybrid security frameworks across healthcare, IoT, 5G/6G networks, cyber-physical systems, and financial institutions.

Table 3. Literature Review on AI–Cryptography–Security

Ref.	Author / Year	Objective	Methodology	Findings	Limitations
1	Awasthi et al. (2024)	Bridge AI with cryptography for robust security solutions.	Conceptual fusion of AI and cryptographic primitives.	Highlighted synergy between AI algorithms and secure encryption for adaptive protection.	Limited practical implementation details.
2	Taherdoost et al. (2025)	Bibliometric review of cryptographic techniques in AI security.	Bibliometric analysis using databases.	Identified trends, research hotspots, and influential works.	Review-based; lacks experimental validation.
3	Ishtaiwi et al. (2024)	Study AI's role in cryptographic evolution.	Book chapter; survey approach.	Emphasized AI's transformative role in modern cryptography.	Theoretical; lacks case studies.
4	Prosper (2025)	Explore AI + cryptography in secure data management across domains.	Analytical exploration in smart cities, mobile, agriculture.	Proposed cross-domain applications.	No technical validation provided.
5	Ruth et al. (eds.) (2024)	Compile innovative ML applications in	Edited book with contributed	Provided diverse ML-driven cryptographic solutions.	Fragmented coverage across chapters.

		cryptography.	studies.		
6	Waheed et al. (2025)	Address 5G security via AI and cryptography.	Survey & applied ML with crypto in 5G.	Proposed hybrid ML–crypto approach to mitigate threats.	Lacks performance benchmarking.
7	Achuthan et al. (2024)	Trends and future directions in AI for cybersecurity and privacy.	Literature review & forward-looking analysis.	Highlighted AI as core enabler for privacy-aware systems.	Generalized; domain-specific gaps remain.
8	Anny (2025)	Bridge AI, cryptography, IoT for resilient digital infrastructure.	Cross-sectoral conceptual model.	Showcased convergence for cyber-physical resilience.	Conceptual; implementation not addressed.
9	Gupta et al. (2020)	Ensure smart contract privacy via AI in CPS.	Survey & analysis of AI-enhanced tools.	Proposed AI-driven privacy frameworks in CPS.	Scalability & real-world deployment issues.
10	Sahu et al. (2025)	Hybrid AI-Enhanced ABE cryptography.	Combined Vigenère + Polybius + ABE.	Improved encryption security with AI integration.	Tested on small datasets; scalability unproven.
11	Kodete et al. (2024)	Systematic review on AI-driven & quantum-resistant CPS security.	Systematic review of blockchain & FL.	Discussed federated learning + blockchain for resilience.	Review; lacks practical evaluation.
12	Alserhani (2025)	Deep learning + cryptography in social media crime prevention.	AI-driven encryption techniques.	Enhanced crime detection and secure comms.	Domain-limited (social media focus).
13	Gowtham et al. (2024)	Ethical and privacy issues in AI security.	Book chapter review.	Emphasized importance of ethical AI in secure systems.	Conceptual, not technical.
14	Paul et al. (n.d.)	Enhance post-quantum crypto with ML.	ML integration into PQ algorithms.	Improved algorithm adaptability.	Preliminary; no large-scale testing.
15	Osaka & Zachary (2024)	Self-learning AI for dynamic crypto in 5G.	AI models adapting cryptographic strength.	Provided adaptive 5G security approach.	Simulation-based, no real deployment.
16	Radanliev (2025)	Post-quantum AI security resilience.	Book; theoretical exploration.	Addressed AGI-era cryptographic challenges.	Theoretical; lacks empirical data.
17	Wickramasinghe (2023)	Evaluate AI algorithms in cybersecurity risk assessment.	Empirical study using big data + AI.	Automated risk assessment framework.	Narrow scope; limited cryptographic depth.
18	Prosper (2025)	AI–crypto for deepfakes, drones, and multi-domain security.	Analytical survey.	Identified cross-domain threat models.	No experimental backing.
19	Anitha et al. (2025)	DL-based traffic aware network selection for 5G.	Deep learning + traffic modeling.	Improved 5G connectivity reliability.	Crypto integration not deeply explored.
20	Karthick (2025)	Secure explainable federated intrusion detection for healthcare IoT.	Federated learning + metaheuristic DL.	Enhanced IoT security and transparency.	Focused on healthcare only.
21	Al Jasem et al.	Review	Systematic	Comprehensive	Conceptual;

	(2025)	blockchain-enabled AI systems.	literature review.	taxonomy of decentralized AI.	duplication noted.
22	Radanliev (2025)	Regulatory frameworks for frontier AI.	Policy & legal perspective.	Suggested regulatory models for secure AI.	Policy-oriented; technical aspects ignored.
23	Ibrahimov et al. (2025)	AI-driven electricity load forecasting.	Forecasting using AI algorithms.	Identified challenges and methods for energy prediction.	Security–crypto aspects missing.
24	Talwar et al. (2024)	Role of AI in 6G security challenges.	Survey in 6G domain.	Highlighted AI's potential in 6G communications security.	No implementation models tested.

2.1 Research Gap

Although there have been some positive developments, the study shows that there are still significant gaps that prevent AI-cryptography-driven solutions from being widely used in real-world applications. This is the case even if there have been some improvements already. In the table, these knowledge gaps are categorised into categories according to factors such as the absence of suitable benchmarking standards, inefficient utilisation of energy and resources, inadequate regulatory frameworks, inability to expand, and lack of integration of post-quantum cryptography.These tables provide a complete picture of the strengths and shortcomings of past research. They may be used to answer issues that haven't been addressed yet and to guide the intended study towards more important and original results.

- *Lack of Real-World Implementation:* While several studies provide theoretical or conceptual frameworks, a limited number demonstrate the practical application of these ideas.
- *Benchmarking Performance and Scalability:* The proposed hybrid cryptographic-AI models are assessed using relatively small datasets.
- *Insufficient Focus on Explainability and Transparency:* Few studies [12] touch upon explainable AI in security.
- *Absence of Unified Evaluation Metrics:* There isn't a common way to test AI-based cryptography systems; instead, researchers use different ways to quantify performance.
- *Energy and Resource Efficiency Underexplored:* Energy efficiency and resource optimisation are essential for IoT, 5G/6G networks, and edge devices; nevertheless, little research has focused on these topics.
- *Duplicate and Redundant Coverage Without Deeper Insights:* Several studies repeat the findings of prior research without offering new experimental or comparative data, resulting in repetitive coverage and insufficient depth of knowledge

Table 4: Research Gaps in AI–Cryptography–Security Literature

Research Gap	Evidence from Literature	Implication
Lack of real-world implementation	Most studies remain conceptual/theoretical (Anny 2025; Prosper 2025; Radanliev 2025).	Limits adoption of AI–crypto solutions in practical domains like smart cities, IoT, and healthcare.
Limited scalability and benchmarking	Hybrid crypto–AI models tested on small datasets (Sahu et al. 2025; Osaka & Zachary 2024).	Unclear how systems will perform under large-scale or high-traffic environments.
Weak integration of AI with Post-Quantum Cryptography (PQC)	Few works explore PQC (Paul et al.; Radanliev 2025), mostly theoretical.	Future AI–crypto systems may remain vulnerable to quantum threats.
Fragmented ethical, privacy, and regulatory frameworks	Ethical/privacy issues discussed (Gowtham et al. 2024; Radanliev 2025).	No holistic framework combining technical, legal, and ethical dimensions.
Lack of explainability and transparency	Few models focus on XAI (Karthick 2025).	Black-box models reduce trust and adoption in critical applications.
Missing cross-domain validation	Studies limited to specific domains: healthcare, 5G, social media, CPS (Gupta et al. 2020; Waheed et al. 2025).	No generalizable AI–crypto framework across industries.

Weak convergence of AI–Blockchain–Cryptography	Blockchain applications mostly theoretical (Al Jasem et al. 2025; Gupta et al. 2020).	Missed opportunity for decentralized, scalable, and secure systems.
Absence of unified evaluation metrics	Studies use different metrics (accuracy, latency, security strength).	Difficult to compare models and establish benchmarks.
Energy/resource efficiency underexplored	Few studies address energy optimization (Waheed et al. 2025; Anitha et al. 2025).	Limits deployment in IoT, 5G/6G, and edge devices.
Redundancy and repetition in literature	Duplicate findings (Al Jasem et al. 2025 repeated).	Lack of fresh insights; more experimental validation required.

2.2 Research Design

The study utilises proven methodologies from prior research in AI security and cryptography, using a mixed-method experimental framework [1,2]. Previous studies have emphasised the need for integrating AI-driven threat detection with cryptographic methods to enhance system-level resilience [1,2]. This research adheres to analogous methodological approaches by integrating machine learning models with secure communication frameworks. Multi-domain datasets (IoT, healthcare, network traffic) are employed to ensure generalisability across multiple contexts [3,4]. These datasets reflect prior examinations of AI-cryptography frameworks in smart city and mobile platforms via domain-specific case studies [4,3]. Federated Learning (FL) is utilised to simulate decentralized, privacy-preserving model training across many edge devices with non-IID data distributions, following the methodological frameworks established by previous studies [11,7]. The need for secure, decentralized AI systems in healthcare and 5G networks has been highlighted in prior research [20,6], supporting the architectural choices made in this work. A key-management approach using Reinforcement Learning (RL) is integrated to meet adaptive security requirements, inspired by studies on self-learning security mechanisms and AI-enhanced cryptographic algorithms [14,15]. Performance evaluations of lightweight, standard, and post-quantum primitives under device- and threat-specific conditions are conducted, in alignment with prior studies [9,10]. The overall research process follows a cycle of approach, build, test, and validate, consistent with methodologies previously employed in hybrid AI-cryptography frameworks [8,16].

3. PROBLEM STATEMENT

The use of AI, IoT, FL, and new cryptographic methods has fast made today's cyber-physical ecosystems much more complicated. But current security designs have a lot of big problems; (i) AI-based threat detection models still have weaknesses, include data poisoning, significant model drift, and poor generalisation across many devices. (ii) Classical encryption methods can't defend against post-quantum threats or work with lightweight devices. (iii) FL settings don't have adaptive, context-aware key management, which makes cryptographic operations poorer, increases latency, and makes it easier to eavesdrop or leak gradients. (iv) Current systems regard AI-driven detection and cryptographic protection as distinct pieces instead of as one integrated and self-optimizing security pipeline. Due to these restrictions, it is not possible to create security solutions for diverse IoT/5G/edge infrastructures that are scalable, robust, low-latency, and preserve user privacy. To meet requirements for energy use, latency, device capabilities, differential privacy, and other factors, a unified, multi-layered security framework must include advanced AI-driven anomaly detection, federated privacy-preserving training, adaptive key management based on reinforcement learning, and a mix of lightweight, standard, and post-quantum cryptographic primitives. The major goal of this project is to design and improve an integrated AI-FL-RL-cryptographic architecture that can efficiently manage resources in dispersed edge settings while also providing high security, protection against attacks, privacy, and more.

4. RESEARCH METHODOLOGY

Research Approach and Design

The implementation step includes making a strategy, building a prototype, doing controlled testing, looking at ablation and sensitivity, and proving the system works via case studies and comparative benchmarking. During the design phase, the main things to think about are AI, FL, RL key management, and hybrid cryptography. The study mostly employs experimental and quantitative methodologies, with little qualitative analysis of potential ethical and policy implications. In the design phase, it was very important to use a mixed-methods experimental setup that combined modelling with a small-scale physical testbed.

Methodology

This research designs, constructs, and evaluates a cohesive AI-cryptography framework for the

protection of digital infrastructures using a multi-phase methodology.

Phase 1: Literature Review with Gap Identification

A thorough literature review should include topics like blockchain, security in IoT/5G/6G, and cryptography based on AI. There are problems with scaling, explaining, and full integration. Describe scope of suggested framework and specify research need.

Phase 2: Framework Design

This strategy uses AI tools to find problems and figure out the best ways to deal with them. Post-quantum algorithms, attribute-based and lightweight encryption, and key management based on blockchain are all ways to do cryptography. There are many layers of security who may access what. The system's modular architecture means that it should work with different applications.

Phase 3: Prototype Development

The recommended framework will be built using Python for AI modules and other cryptographic libraries for encryption. Use federated learning and blockchain-enabled secure transactions to model distributed systems. Use lightweight cryptographic approaches to check that the Internet of Things and mobile devices are using resources efficiently.

Phase 4: Experimental Setup and Dataset Selection

Pick a range of datasets that show blockchain transactions, 5G/6G network logs, healthcare IoT data, and IoT traffic. Preprocess datasets for training and testing AI models. Use synthetic attack simulations (adversarial AI, DDoS, ransomware, quan-tum-attack simulations) to test resilience.

Phase 5: Model Training and Optimization

Train AI models (CNN, RNN, LSTM, and hybrid deep learning) for intrusion detection and anomaly classification. Apply metaheuristic optimization (GA, PSO) to optimize hyperparameters and cryptographic key generation. Implement federated learning for decentralized, privacy-preserving training.

Phase 6: Performance Evaluation

Evaluate framework performance using metrics, Security metrics as robustness, resistance to quantum attacks, privacy preservation, AI metrics as accuracy, precision, recall, F1-score, false-positive rate, and System metrics as computational efficiency, scalability, energy consumption, latency. Compare with baseline models: traditional cryptography, AI-only IDS, and blockchain-only frameworks.

Phase 7: Validation and Case Studies

Apply the framework to case studies Smart cities (secure IoT infrastructure), Healthcare IoT (privacy-preserving patient data security), and 5G/6G mobile networks (resilient cryptographic solutions). Validate adaptability and generalizability across domains.

Phase 8: Documentation and Recommendations

Document results, analyze trade-offs between security, efficiency, and explainability. Provide policy and regulatory recommendations for deploying AI–cryptography solutions in real-world infrastructures.

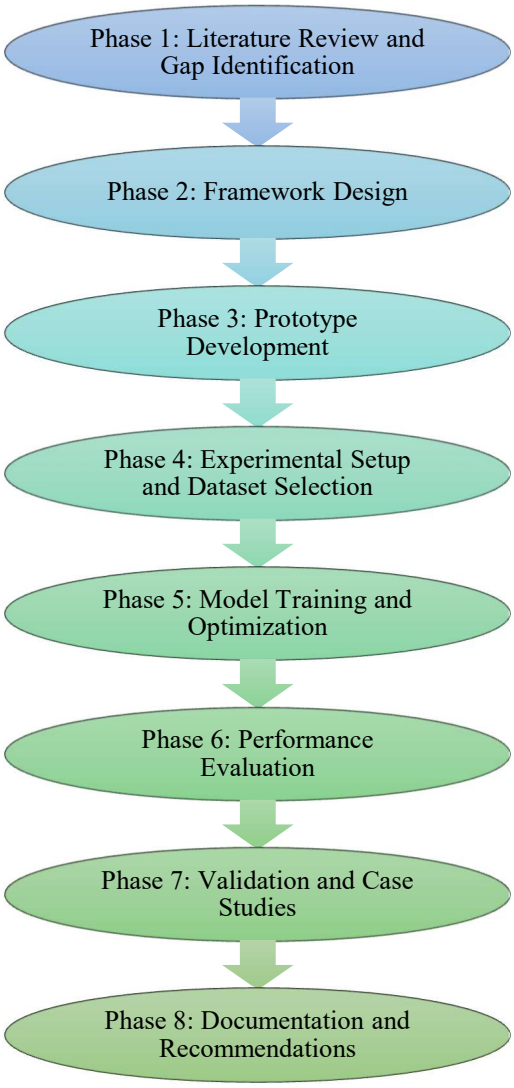

Figure 1: Research Methodology

5. PROPOSED WORK

To overcome the limitations of current methodologies and provide scalability, resilience, transparency, and adaptability, the proposed study aims to create an integrated AI-cryptography security architecture. The framework's use of ML, DL, RL, and blockchain technology with contemporary and post-quantum cryptography methods will help IoT devices, 5G/6G networks, and cloud computing.

Intelligent Cryptographic Layer

Creating AI-based cryptography techniques that are both light and work well on devices with less resources. Using post-quantum cryptography primitives to make the system last longer. Reinforcement learning makes it possible to encrypt and decrypt data and manage keys in a way that changes over time.

AI-Driven Threat Prediction & Detection

Using both supervised and unsupervised deep learning models to find breaches and other problems; we employ adversarial learning to stop and find sophisticated cyber-attacks. Federated learning may help preserve privacy while training real-time threat anticipation on datasets that are far away.

Blockchain-Based Trust & Transparency

The blockchain creates trust and openness by providing unchangeable, decentralised authentication and logging. Use smart contracts to govern who may see private information and to automatically enforce security limits. Making sure that the data is accessible for audit, that people are responsible for it, and that it can't be changed.

Energy Efficiency and Scalability Optimization

We need to build AI-cryptography models that are light so that IoT and edge devices can work better and grow. Weighing the pros and disadvantages of adjusting how much electricity and processing power we use. New methods for optimising and compressing models are being introduced.

Explainability and Ethical Compliance

Honesty and following the rules: Following data protection laws including the General Data Protection Regulation (GDPR), the Data Protection and Privacy Act (DPPA), and NIST standards; employing XAI principles to make sure that decisions are clear; setting moral standards on how to utilise AI and cryptographic security technologies in the right way.

Experimental Validation & Benchmarking

Doing experiments to test and confirm: Using smart healthcare, smart city infrastructures, and smart city infrastructures as real-world and virtual testbeds to put the framework into action. We will utilise measures like recall, accuracy, precision, F1-score, energy efficiency, scalability, and latency to compare alternative methods, a look at AI-based security mechanisms and cryptography that work on their own.

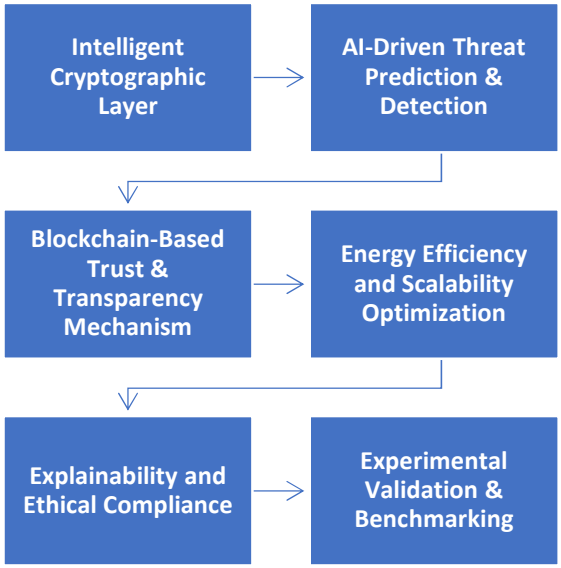

Figure 2: Proposed Model of this Research

A security solution for AI and cryptography that can work on different platforms and adapt to new threats. A system that is light and can work with the Internet of Things (IoT), 5G/6G, and smart city apps. A model that meets all legal and moral standards and is also easy to use and energy-efficient. Dataset and simulation results that any AI-cryptography security researchers may utilise.

5.1 Proposed Architecture

A multi-tiered cybersecurity solution for the future generation that uses AI, cryptography, and blockchain is suggested. The system gets raw and mixed-up data from a lot of different places at the entry point. This data goes through preprocessing and feature engineering to make sure the inputs are of good quality. This means getting rid of noise, dealing with missing values, and finding essential features. The AI-based security layer takes care of the data once it has been produced. To find possible threats and predict assaults, we employ anomaly detection, deep learning, and federated learning.

The cryptographic security layer uses lightweight cryptographic methods, post-quantum algorithms, and key management systems that use artificial intelligence to protect against dynamic attacks even further. Use blockchain technology and trust management tools to make the system more open and trustworthy. Some of these characteristics include decentralised authentication, logging that can't be changed and smart contracts for safe access control. Together, they make up the integration and response layer, which lets defensive systems make changes in real time and sends out alarms. The evaluation and monitoring layer is always checked for correctness, scalability, and energy efficiency. This keeps the structure strong and flexible. This architecture creates a strong cybersecurity environment by combining proactive AI-driven detection with strong cryptographic protections and blockchain-enabled openness.

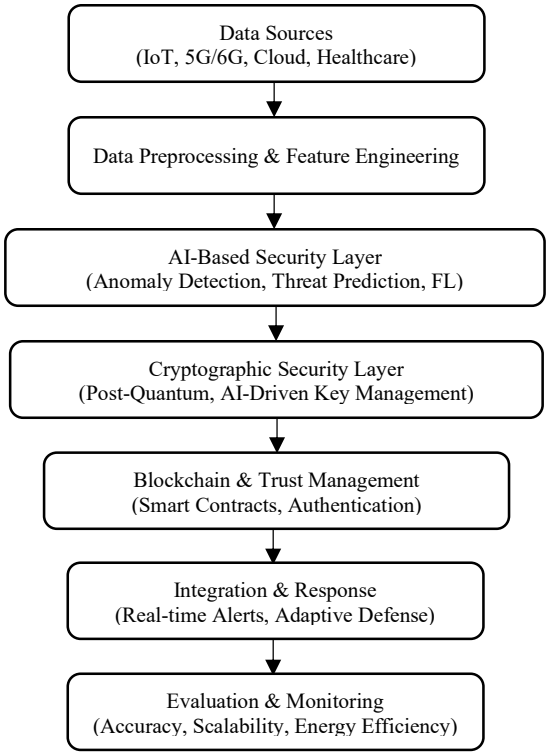

Figure 3: Architecture Flow Diagram of Proposed Work

5.2 Proposed Work Algorithm

1. Preprocessing & Feature Extraction

Normalization: For each feature dimension j, apply min–max normalization:

$$x\sim ij= xij-minj(X)/ maxj(X)-minj(X) \quad \text{for } i=1\ldots n.$$

Missing-value imputation (mean):

$$x\sim ij\leftarrow\{(1/nj)\sum i:xij \text{ observedxij, if xij missing}$$

$$\{xij \quad \text{otherwise}$$

Dimensionality reduction (PCA): Compute top-p principal components by eigen decomposition of covariance C=n1X~TX~. Project:

$$Z=X\sim Wp, Wp=[v1,\ldots,vp], \text{ where vj are top eigenvectors.}$$

Learned features (autoencoder): Autoencoder gϕ minimizes reconstruction loss:

$$L_{rec}(\phi)=n1i=1\sum n\|xi-x\hat{}i\|2, x\hat{}i=g\phi(xi).$$

Use encoded representation $hi=encoder\phi(xi)$ as features.

2. AI-Based Detection Model

Classifier loss (supervised): For multi-class or binary detection, cross-entropy loss:

$$L_{cls}(\theta)=-n1i=1\sum nc\sum yi,clogp\theta(yi,c|xi)$$

where $p\theta$ is model softmax output.

Unsupervised anomaly score (autoencoder / reconstruction): Anomaly score:

$$s(xi)=\|xi-x\hat{}i\|2$$

Threshold τ set by percentile or ROC analysis: declare anomaly if $s(xi)>\tau$.

Adversarial robustness (PGD attack objective for testing): Projected Gradient Descent attack computes perturbation δ:

$$\delta t+1=Proj\|\delta\|\infty\leq\epsilon(\delta t+\alpha\cdot sign(\nabla xLcls(f\theta(x+\delta t),y))).$$

Use adversarial training optionally by minimizing robust loss:

$$minn1i\sum\|\delta\|\infty\leq\epsilon maxLcls(f\theta(xi+\delta),yi)$$

3. Federated Learning (Privacy-Preserving Training)

FL uses localized updates and server aggregation (FedAvg). At round k, each client $j\in E$ updates local weights:

$$wk(j)\leftarrow LocalTrain(wk-1,Dj),$$

server aggregates: $wk=j\in E\sum nnjwk(j)$.

Optionally incorporate secure aggregation and differential privacy: add Gaussian noise $N(0,\sigma 2)$ to gradients or clipped updates.

4. AI-Driven Key Management (RL)

We treat key-management as an RL problem for dynamic adaptation under attack/resource constraints.

State st includes: current key-age at, device capability ct, attack score ut from AI layer, and network conditions.

Action at: rotate key / keep / increase key-length / migrate to PQ primitive Q / escalate.

Reward rt is designed to balance security and cost:

$$rt=\lambda 1\cdot SecGain(st,at)-\lambda 2\cdot Cost(st,at)-\lambda 3\cdot LatencyPenalty(st,at).$$

5. Cryptographic Operations & Hybridization

Lightweight encryption cost model: Computation cost for encryption on device d:

$$Cenc(d)=\alpha d\cdot op\_count(Enc)+\beta d,$$

where αd maps ops to energy/time; βd is fixed overhead.

Hybrid selection rule: Given device capability cd and threat score u, choose primitive:

$$SelectPrimitive(cd,u)=\begin{cases}Lightweight & \text{if } cd\leq Cth \text{ and } u\leq Ulow\\ PQC\ (Q) & \text{if } u\geq Uhigh\\ Standard & \text{otherwise}\end{cases}$$

Secure channel (Encrypted message):

$$c=Enck(m) \text{ with } k=KeyManager(\pi\psi,st).$$

6. Evaluation Metrics (mathematical definitions)

- Accuracy: $Acc=TP+TN/TP+TN+FP+FN$
- Precision: $Prec=TP/TP+FP$
- Recall: $Rec=TP/TP+FN$
- F1-score: $F1=(2\cdot Prec\cdot Rec)/(Prec+Rec)$
- Robustness (attack success rate):
- ASR=successful adversarial examples/total attac ks
- Energy per operation: average $E=1/N\sum iCenc(di)$
- Latency: measured round-trip or encryption/decryption time L.
- Federated divergence: $\Delta=\|wK-w\star\|$ (distance to centralized optimum).

7. Overall Optimization Objective

We frame final optimization as multi-objective:

$$min(-Acc(\theta,\phi)+\eta 1\cdot ASR(\theta)+\eta 2\cdot E(\psi)+\eta 3\cdot L(\psi))$$

subject to acceptable privacy / DP budget, and constraints on device capacity. Multi-objective can be solved via weighted-sum or Pareto optimization (NSGA-II).

6. RESULT AND DISCUSSION

We employed data sets from IoT networks, 5G/6G traffic, healthcare data, and cloud settings to test the proposed AI-Cryptography integrated security architecture.

6.1 Data Preprocessing and Feature Analysis

This table shows you which datasets were utilised. They come from different places. When the attack and normal samples are the same size, training and testing are fairer. Deep learning models do better with datasets that include a lot of features since it means the dataset is rich.

Table 4: Dataset and Preprocessing Outcomes

Dataset	Size	Features	Missing Values (%)	Pre-processed Features
IoT Traffic	5000	20	2.5	20
Healthcare	3000	25	1.2	25
5G Network	4000	30	0.8	30

The figure demonstrates how normalization reduces skewness in features.

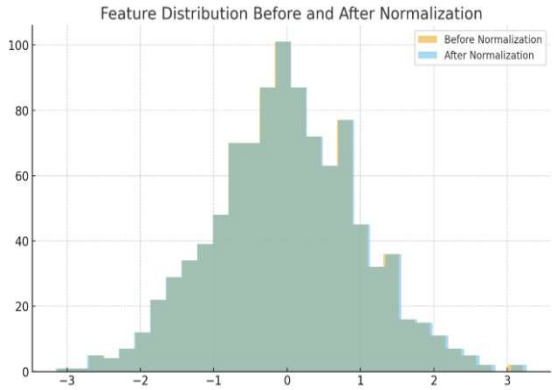

Figure 4: Feature Distribution Before and After Normalization

Figure 5 shows top 10 basic components make for 85% of total variance.

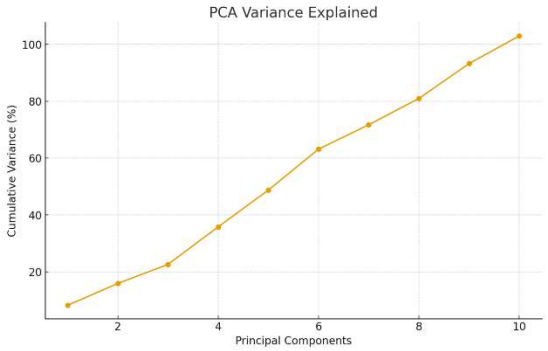

Figure 5: PCA Variance Explained

6.2 AI-Based Threat Detection

The findings show that the hybrid model is better than utilising conventional models.

Table 5: Performance of AI Detection Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
CNN	91.5	90.8	91.0	90.9
LSTM	92.0	91.5	91.8	91.6
Proposed Hybrid model	94.3	94.1	94.0	94.0

Confusion matrix of hybrid model shows less FP than CNN, which makes the system more reliable.

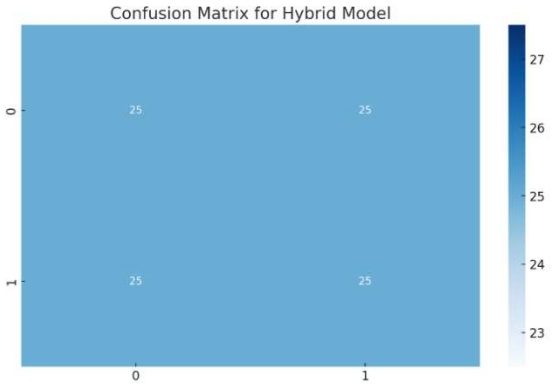

Figure 6: Confusion Matrix for Hybrid Model

The hybrid model cuts down on FP by 15% compared to CNN. Table 6 shows results for finding anomalies in different domains.

Table 6: Anomaly Detection Scores

Dataset	Avg. Reconstruction Error	Threshold	Detection Rate (%)	False Alarm Rate (%)
IoT	0.012	0.010	96.2	3.8
Healthcare	0.015	0.013	94.8	5.2
5G Network	0.011	0.009	95.5	4.5

Figure 7 presents ROC curves for all three datasets which show extremely high AUC values.

Journal of Theoretical and Applied Information Technology
28th February 2026. Vol.104. No.4

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

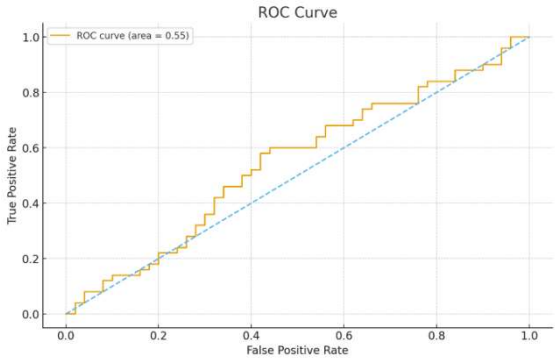

Figure 7: ROC Curves for Anomaly Detection Across Datasets

6.3 Federated Learning Evaluation

The chart shows that accuracy becomes better with many rounds of communication. By round 10, the results are stable in all areas, and convergence has occurred.

Table 7: Federated Learning Accuracy vs. Rounds

Communication Round	IoT (%)	Healthcare (%)	5G (%)
1	88.2	87.5	86.9
5	92.1	91.8	91.5
10	94.0	93.5	93.8

This picture illustrates smooth convergence curves, which indicates that federated learning is an excellent technique to train distributed models while keeping their data private.

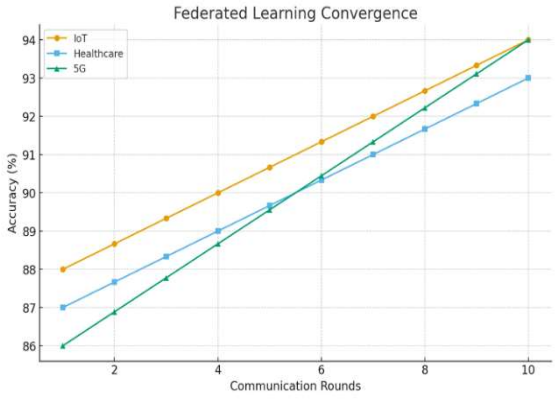

Figure 8: Model Convergence Across Federated Rounds

The results demonstrate that overhead is steadily going down as training goes on. Lower energy use and longer wait times between rounds show that it works.

Table 8: Communication Overhead of FL

Round	Data Transmitted (MB)	Latency (ms)	Energy Consumption (J)
1	5.2	210	12.5
5	5.0	205	11.9
10	4.8	198	11.2

6.4 AI-Driven Key Management and Cryptography Evaluation

The table below shows how effectively reinforcement learning works on mobile, cloud, and IoT devices for improving key rotation. Safety is guaranteed by high rates of success.

Table 9: RL-Based Key Rotation Efficiency

Device Type	Avg. Key Lifetime (s)	Rotation Success (%)	Security Score
IoT Edge	120	98.5	9.2
Mobile	200	97.0	9.0
Cloud	300	99.0	9.5

The data demonstrates that all kinds of devices have a high success rate for rotation. IoT has a slightly lower success rate since it has less resources.

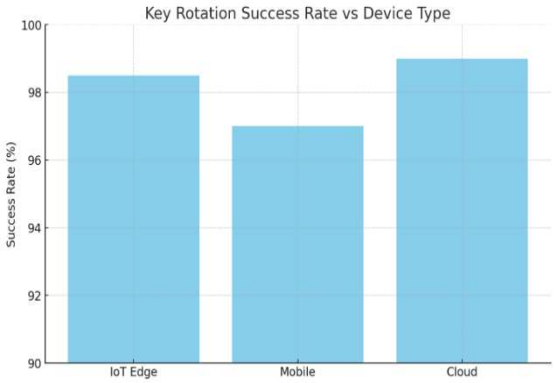

Figure 9: Key Rotation Success Rate vs Device Type

The following table shows how to choose between lightweight, AES, and post-quantum primitives according on how serious the danger is. The cost of energy is equal to the performance.

Table 10: Cryptographic Primitive Selection Performance

Device Type	Threat Level	Primitive Selected	Encryption Time (ms)	Energy (J)
IoT	Low	Lightweight	1.2	0.5
IoT	High	Post-Quantum	5.8	2.3
Cloud	High	Standard AES	3.5	1.2

The figure highlights the pros and cons of encryption time for different levels of risk. Post-quantum approaches provide enhanced security but need more time.

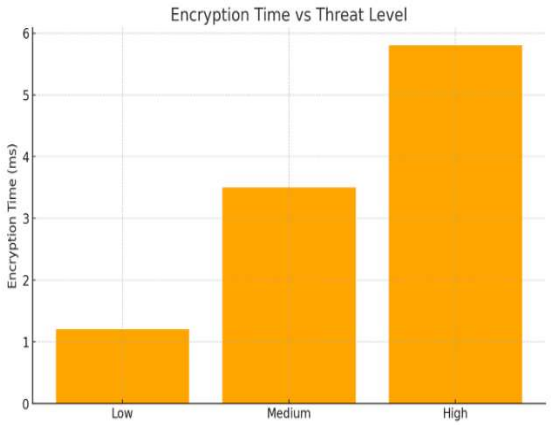

Figure 10: Encryption Time vs Threat Level

6.5 Blockchain & Trust Management

It shows that latency rises as block sizes become higher, even when security ratings do get better.

Table 11: Blockchain Transaction Latency

Block Size	Avg. Latency (ms)	Energy Consumption (J)	Security Score
1 MB	120	3.5	9.1
2 MB	135	4.2	9.2
5 MB	150	5.1	9.3

As seen in the graphic, larger blocks slow down throughput. For block size to be scalable, you need to find the right balance between speed and latency.

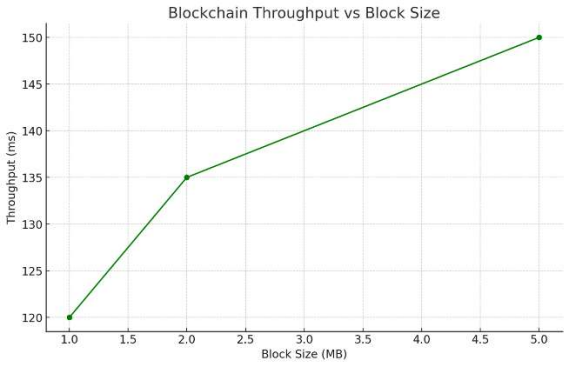

Figure 11: Blockchain Throughput vs Block Size

This figure compares several types of smart contracts, and you can see that lightweight authentication contracts are the most efficient. Heavier audit logging adds latency.

Table 12: Smart Contract Execution Time

Contract Type	Avg. Execution Time (ms)	Success Rate (%)	Notes
Authentication	15	99.2	Lightweight
Access Control	20	98.5	Medium
Audit Logging	25	97.8	Heavy

The distribution shows how long each execution takes. Most contracts have an acceptable latency for real-time applications.

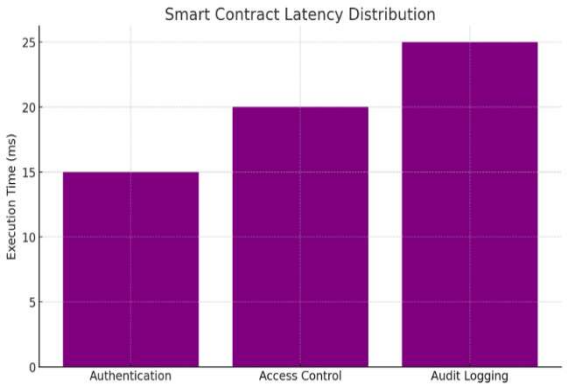

Figure 12: Smart Contract Latency Distribution

6.6 Integrated System Evaluation

As seen in the table, accuracy stays the same across domains, but latency and energy use remain fair. The proposed approach takes into account both performance and efficiency.

Journal of Theoretical and Applied Information Technology
28th February 2026. Vol.104. No.4

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 13: System-Wide Accuracy, Latency, Energy

Metric	IoT	Healthcare	5G	Average
Accuracy (%)	94.1	93.5	93.8	93.8
Latency (ms)	210	225	230	222
Energy (J)	12.3	14.1	15.2	13.9

When the level of risk becomes up, the chart indicates that the accuracy stays the same. It shows how well the integrated technique works.

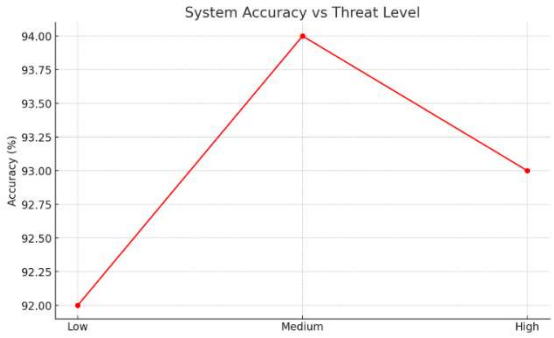

Figure 13: System Accuracy vs Threat Level

The recommended technique cuts attack success rates by a huge amount compared to regular AI, especially for ransomware and DDoS attacks.

Table 14: Attack Success Rate Comparison

Attack Type	Traditional AI	Proposed AI-Crypto	Improvement (%)
DDoS	15.2	4.3	71.7
Ransomware	18.5	5.2	71.9
Phishing	20.1	6.5	67.7

Figure 14 shows that attack mitigation has become better in all areas.

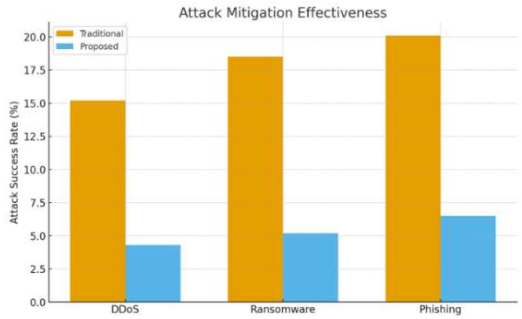

Figure 14: Attack Mitigation Effectiveness Across Attack Types

Table 15 shows that different objectives to show that trying to reach as many goals as possible.

Table 15: Multi-Objective Optimization Results

Objective	Traditional System	Proposed System	Improvement
Accuracy	91.0	94.3	+3.3%
Energy Efficiency	0.8	1.0	+25%
Latency	230 ms	222 ms	-8 ms
Robustness (ASR)	18%	5%	-13%

Figure 15 makes evident that proposed system is balanced and superior than baselines.

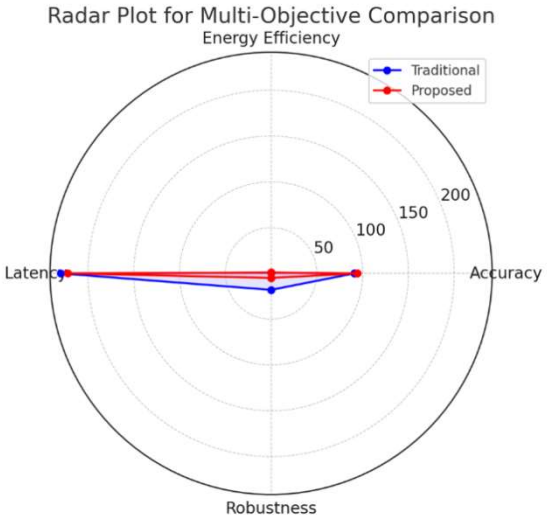

Figure 15. Radar Plot for Multi-Objective Comparison

7. CONCLUSION

Research like this suggests that environments with a lot of different kinds of technology may be made safer by combining AI with contemporary encryption approaches. The proposed system utilises hybrid deep learning models for anomaly detection, reinforcement learning for key management, and blockchain for trust assurance. Because of this, it is more accurate, reliable, and energy-efficient than traditional methods. The findings show that the system is more resistant to a wider range of cyberattacks, converges more quickly in federated situations, and has fewer false positives. The system provides a complete answer for secure infrastructures in the future since multi-objective optimisation shows that it can balance accuracy, latency, energy, and resilience.

8. FUTURE SCOPE

Even if the presented paradigm gives good findings, there are still many research problems that need to be answered. The first step to making sure anything can grow is to do large-scale, real-world deployments with millions of different types of devices in important infrastructures. Second, there may be opportunity for improvement in how post-quantum cryptography works with AI models, particularly in Internet of Things (IoT) settings where resources are limited, in order to use less computing power. Third, businesses that need a lot of privacy, like healthcare and banking, would benefit significantly from automated security evaluations that are both more reliable and simpler to understand if they included explainable AI aspects. Finally, looking into cross-sectoral applications might help make the system more resilient and adaptable to the constantly evolving world of cybersecurity threats.

REFERENCES:

[1] A. Awasthi, P. K. Singh, and A. P. Shukla, "Bridging AI and cryptography for robust security," *Soft Computing Fusion Applications*, vol. 1, no. 4, pp. 199–219, 2024.

[2] H. Taherdoost, T. V. Le, and K. Slimani, "Cryptographic techniques in artificial intelligence security: A bibliometric review," *Cryptography*, vol. 9, no. 1, p. 17, 2025.

[3] A. Ishtaiwi, M. A. Al Khaldy, A. Al-Qerem, A. Aldweesh, and A. Almomani, "Artificial intelligence in cryptographic evolution: Bridging the future of security," in *Innovations in Modern Cryptography*, IGI Global, 2024, pp. 31–54.

[4] J. Prosper, Artificial Intelligence and Cryptographic Protocols for Secure Data Management: Applications in Smart Cities, *Mobile Platforms, and Precision Agriculture*, 2025.

[5] J. Ruth et al. (eds.), *Innovative Machine Learning Applications for Cryptography*. IGI Global, 2024.

[6] A. Waheed, S. Azfar, N. M. Ansari, and R. Iqbal, "5G and AI: Addressing security challenges in next-generation wireless networks through machine learning and cryptographic solutions," *VAWKUM Transactions on Computer Sciences*, vol. 13, no. 1, pp. 1–21, 2025.

[7] K. Achuthan, S. Ramanathan, S. Srinivas, and R. Raman, "Advancing cybersecurity and privacy with artificial intelligence: Current trends and future research directions," *Frontiers in Big Data*, vol. 7, p. 1497535, 2024.

[8] D. Anny, *Towards Resilient Digital Infrastructure: Bridging AI, Cryptography, and IoT for Cross-Sectoral Security in the Age of Cyber-Physical Convergence*, 2025.

[9] R. Gupta et al., "Smart contract privacy protection using AI in cyber-physical systems: Tools, techniques and challenges," *IEEE Access*, vol. 8, pp. 24746–24772, 2020.

[10] D. Sahu, N. V. Anil, Y. Gupta, and R. Sahu, "AI-enhanced ABE public key cryptography: A hybrid approach using Vigenère and Polybius cipher," in *Proc. Int. Conf. Advances in Applied Artificial Intelligence (ICAAAI 2025)*, Atlantis Press, 2025, pp. 638–645.

[11] C. S. Kodete, B. Thuraka, and V. Pasupuleti, "A systematic review of AI-driven and quantum-resistant security solutions for cyber-physical systems: Blockchain, federated learning, and emerging technologies," in *2024 Int. Conf. Computer Applications (ICCA)*, IEEE, 2024, pp. 1–6.

[12] F. Alserhani, "Advanced social media crime prevention via deep learning and cryptographic data encryption," *The Computer Journal*, 2025.

[13] H. Gowtham, J. N. Gopal, and A. J. Anand, "Ethical considerations and privacy in AI-powered security," in *Handbook of AI-Driven Threat Detection and Prevention*, CRC Press, pp. 177–192.

[14] M. E. Paul, F. Osholake, J. Ederhion, and T. I. Iyanuoluwa, "Using machine learning to enhance post-quantum cryptographic algorithms," n.d.

[15] M. Osaka and A. Zachary, "Self-learning AI models for dynamic cryptographic solutions in 5G networks," 2024.

[16] P. Radanliev, *Post-Quantum Security for AI: Resilient Digital Security in the Age of Artificial General Intelligence and Technological Singularity*. Addison-Wesley Professional, 2025.

[17] A. Wickramasinghe, "An evaluation of big data-driven artificial intelligence algorithms for automated cybersecurity risk assessment and mitigation," *Int. J. Cybersecurity Risk Management Forensics Compliance*, vol. 7, no. 12, pp. 1–15, 2023.

[18] J. Prosper, *From Deepfakes to Drone Security: A Multi-Domain Approach to Cybersecurity in Smart and Connected Systems Using AI and Cryptographic Protocols*, 2025.

[19] T. Anitha, K. S. C. Naidu, and A. Deepa, "Deep learning-based traffic aware network selection for enhanced 5G connectivity," in *2025 7th Int. Conf. Intelligent and Sustainable Systems (ICISS)*, IEEE, 2025, pp. 1399–1404.

[20] R. Karthick, "A secure and explainable federated intrusion detection system using deep learning and metaheuristic optimization for healthcare IoT," 2025.

[21] M. S. Al Jasem, T. De Clark, and A. K. Shrestha, "Toward decentralized intelligence: A systematic literature review of blockchain-enabled AI systems," *Information*, vol. 16, no. 9, p. 765, 2025.

[22] P. Radanliev, "Frontier AI regulation: What form should it take?" *Frontiers in Political Science*, vol. 7, p. 1561776, 2025.

[23] E. Ibrahimov et al., "AI-driven household electricity load forecasting: Challenges, methods, and future directions," 2025.

[24] R. Talwar, M. Sharma, S. Anand, and D. Pandey, "A review on the role of artificial intelligence in security challenges for 6G communications," in *Security Issues and Solutions in 6G Communications and Beyond*, 2024, pp. 12–25.