Adaptive AI Middleware for Data Privacy and Quantum Cryptography in Smart Environments

Darlan Noetzold[1], Valderi R. Q. Leithardt[2], Jorge L. V. Barbosa[3], Juan F. P. Santana[1]

[1]University of Salamanca, Expert Systems and Applications Laboratory, Salamanca, Spain
[2]Instituto Universitário de Lisboa (ISCTE-IUL), Lisboa, Portugal
[3]University of Vale do Rio dos Sinos (UNISINOS)

August 7, 2025

Contents

Abstract

The rapid evolution of smart environments and the proliferation of interconnected devices have intensified the demand for advanced data privacy and security solutions. This project proposes an adaptive middleware architecture that leverages Artificial Intelligence (AI)—including supervised, unsupervised, and reinforcement learning—to autonomously assess contextual information and dynamically select the most appropriate cryptographic strategies. Central to the approach is the integration of quantum cryptography, such as Quantum Key Distribution (QKD) and post-quantum cryptographic (PQC) algorithms, alongside classical methods, ensuring resilience against both current and future quantum threats. The middleware employs clustering algorithms to analyze environmental and transactional contexts, while reinforcement learning agents optimize the selection of cryptographic algorithms and key management strategies in real time. This plug-and-play solution is designed to operate seamlessly in heterogeneous IoT and intelligent environments, adapting encryption strength and security policies based on risk assessment, system state, and resource constraints. By unifying AI-driven decision-making with quantum-safe cryptography, the proposed model addresses critical gaps in the state of the art, paving the way for robust, context-aware, and future-proof data protection in next-generation smart systems.

Keywords: Artificial Intelligence (AI); Reinforcement Learning (RL); Security; Quantum Cryptography; Data Privacy; Smart Environments; Middleware

1. Introduction

The advent of quantum computing is poised to revolutionize the field of cryptography, challenging the security of classical encryption algorithms that underpin modern data privacy frameworks. Traditional cryptographic schemes such as RSA and elliptic curve cryptography (ECC) are vulnerable to quantum attacks, particularly Shor's algorithm, which can efficiently factor large integers and compute discrete logarithms, thereby compromising widely used public-key systems [1]. This impending threat has accelerated research into post-quantum cryptography (PQC), which aims to develop quantum-resistant algorithms capable of securing data against both classical and quantum adversaries [2].

Simultaneously, the integration of Artificial Intelligence (AI) techniques, especially Reinforcement Learning (RL), into cybersecurity systems offers promising adaptive capabilities. AI can dynamically assess contextual information and threat levels to optimize security measures in real-time, a critical feature for smart environments characterized by heterogeneous data flows and varying sensitivity [3]. This adaptive process can be effectively modeled using the MAPE-K (Monitor, Analyze, Plan, Execute over a shared Knowledge base) framework, which provides a structured feedback loop for self-adaptive systems [4, 5]. In this context, clustering algorithms serve as the Analyze component by grouping data inputs and environmental states into meaningful clusters that represent different security contexts or threat levels. These clusters inform the RL agent, which acts as the Plan and Execute components, by selecting the optimal quantum cryptography level to apply based on the current cluster (state) and learned policy. The Monitor component continuously collects data on system inputs, outputs, and environmental changes, updating the shared Knowledge base that stores historical context, threat patterns, and system performance metrics.

By combining clustering and RL within the MAPE-K loop, the system achieves a robust auto-adaptive mechanism: clustering reduces the complexity of the state space by abstracting raw data into discrete contexts, enabling the RL agent to learn more efficiently and make informed decisions about encryption strength. This synergy allows the middleware to autonomously adjust cryptographic parameters in real-time, balancing security requirements against computational overhead, and adapting to evolving threats and data sensitivity in smart environments. Among the leading quantum-resistant algorithms recommended by NIST and widely studied are lattice-based schemes such as CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures, as well as hash-based signatures like SPHINCS+ [6]. These algorithms offer strong security guarantees against quantum adversaries while maintaining practical performance. In addition, quantum key distribution (QKD) protocols, such as BB84 and E91, exploit quantum mechanical properties to enable theoretically unbreakable key exchange [7, 8]. This project will focus on integrating these PQC algorithms alongside classical cryptographic methods, including AES for symmetric encryption and RSA/ECC for legacy compatibility, within an adaptive middleware framework.

Recent industry reports emphasize the urgency of adopting cryptographic agility frameworks that allow seamless transitions between classical and quantum-resistant algorithms, ensuring long-term data confidentiality [9]. Moreover, the "harvest now, decrypt later" attack model, where adversaries store encrypted data today to decrypt it in the future with quantum computers, underscores the need for proactive quantum-safe encryption strategies [6].

This work presents an adaptive AI middleware that leverages clustering and reinforcement learning to dynamically select and apply quantum-safe cryptographic techniques, enhancing data privacy and security in smart environments while optimizing resource utilization in the face of emerging quantum threats. The remainder of this article is organized as follows: Section 2 provides essential background on data privacy, intelligent environments, quantum cryptography, and artificial intelligence; Section 3 presents a systematic review of the state of the art in adaptive security systems integrating cryptography and AI; Section 4 details the proposed model, including the architecture, quantum gateway, classification and reinforcement learning modules, key management, and validation scenarios; Section 5 outlines the methodological plan and publication strategy; and Section 6 concludes the paper, highlighting future research directions.

2. Background

This section provides an overview of the fundamental concepts and technologies that underpin the research presented in this work. Understanding these foundational topics is essential to grasp the challenges and solutions related to adaptive security systems in intelligent environments, especially those involving advanced cryptographic methods and artificial intelligence.

The section is organized into four subsections. First, we discuss *Data Privacy*, highlighting its importance and the key principles involved in protecting sensitive information. Next, we explore *Intelligent Environments*, describing their characteristics and the unique security and privacy challenges they pose. The third subsection

covers *Quantum Cryptography*, introducing its principles and relevance in securing communications against emerging threats. Finally, we present an overview of *Artificial Intelligence* techniques that enable adaptive and context-aware security mechanisms.

2.1. Data Privacy

Data privacy refers to the set of practices and mechanisms aimed at protecting personal and sensitive information from unauthorized access, disclosure, or misuse. It involves controlling how data is collected, stored, processed, and shared, ensuring compliance with legal frameworks such as the General Data Protection Regulation (GDPR) and other regional privacy laws. The goal is to maintain the confidentiality and integrity of data while respecting individuals' rights over their personal information.

From a technical perspective, data privacy encompasses methods such as data anonymization, pseudonymization, encryption, and access control policies. Anonymization removes or masks personally identifiable information to prevent re-identification, while pseudonymization replaces identifiers with artificial labels. Encryption techniques protect data both at rest and in transit by transforming it into unreadable formats accessible only to authorized parties. Access control mechanisms enforce permissions and restrictions on data usage based on roles or attributes. In dynamic and distributed systems like intelligent environments, implementing these techniques requires careful consideration of context, data sensitivity, and system constraints to balance privacy protection with usability and performance.

2.2. Intelligent Environments

Intelligent environments are composed of interconnected devices, sensors, actuators, and computing resources that collaboratively perceive and interpret contextual information to provide automated and adaptive services. These environments span a variety of domains, including smart homes, smart cities, healthcare systems, industrial automation, and Internet of Things (IoT) networks. The core characteristic of intelligent environments is their ability to sense changes in the physical or digital context and respond accordingly to support user activities or system objectives.

The architecture of intelligent environments typically involves heterogeneous components with varying capabilities, communication protocols, and data formats. This heterogeneity, combined with the dynamic nature of the environment—where devices may join, leave, or move—introduces challenges in maintaining consistent and secure operation. Data collected from multiple sources must be integrated and analyzed in real time to enable context-aware decision-making. Consequently, intelligent environments require robust mechanisms for context modeling, data fusion, and adaptive control.

Security and privacy concerns are prominent due to the continuous collection and processing of potentially sensitive data. Ensuring secure communication channels, authenticating devices, and enforcing access control policies are necessary to prevent unauthorized access and data breaches. Additionally, fault tolerance and resilience mechanisms are needed to handle failures or attacks without compromising system availability. The interplay between these technical requirements demands the use of advanced methods, including artificial intelligence for anomaly detection and decision-making, as well as cryptographic techniques to protect data confidentiality and integrity.

2.3. Quantum Cryptography

Quantum cryptography is a field that applies the principles of quantum mechanics to secure communication. Unlike classical cryptography, which relies on computational hardness assumptions, quantum cryptography offers security based on the fundamental laws of physics. The primary goal is to enable two parties to share a secret key securely, even in the presence of an eavesdropper with unlimited computational power.

One of the earliest and most studied quantum cryptographic protocols is the BB84 protocol [10]. It encodes information in the polarization states of photons, using two sets of conjugate bases (rectilinear and diagonal). The sender, Alice, randomly selects a basis and a bit value to encode each photon, while the receiver, Bob, measures each photon in a randomly chosen basis. After the transmission, Alice and Bob publicly compare their chosen bases and discard the bits where their bases do not match, resulting in a shared raw key. The security of BB84 is guaranteed by the no-cloning theorem, which prevents an eavesdropper from perfectly copying unknown quantum states, and by the fact that any measurement by an eavesdropper introduces detectable errors. The quantum bit error rate (QBER) quantifies the error rate in the raw key and is defined as

$$QBER = \frac{N_{\text{error}}}{N_{\text{total}}}$$

where N_{error} is the number of bits where Alice and Bob disagree, and N_{total} is the total number of bits compared. A QBER above a certain threshold indicates the presence of an eavesdropper or excessive noise.

The E91 protocol [11] extends the concept of quantum key distribution by using entangled photon pairs. In this protocol, a source generates pairs of entangled photons, sending one photon to Alice and the other to Bob. Both parties perform measurements in randomly

chosen bases. The correlations between their measurement outcomes, which violate Bell's inequalities, ensure the security of the key. The violation of Bell's inequality is expressed as

$$S = |E(a, b) + E(a, b') + E(a', b) - E(a', b')| \leq 2$$

where $E(a, b)$ are correlation coefficients for measurement settings a, b. Values of $S > 2$ indicate quantum entanglement and guarantee security against eavesdropping.

Continuous Variable Quantum Key Distribution (CV-QKD) protocols [12] encode information in the quadratures of the electromagnetic field, which are continuous variables, rather than discrete photon states. This approach allows the use of standard telecom components and can achieve higher key rates over metropolitan distances. The secret key rate K in CV-QKD is given by

$$K = \beta I_{AB} - \chi_{BE}$$

where β is the reconciliation efficiency, I_{AB} is the mutual information between Alice and Bob, and χ_{BE} is the Holevo bound representing the maximum information an eavesdropper (Eve) can obtain.

Measurement-Device-Independent QKD (MDI-QKD) [13] addresses vulnerabilities in detection devices by removing trust assumptions on measurement devices. It uses entanglement swapping and Bell state measurements performed by an untrusted relay, allowing secure key distribution even with compromised detectors. This protocol mitigates detector side-channel attacks, which are a significant practical security concern.

The Decoy State protocol [14] enhances the security of practical QKD systems that use weak coherent pulses instead of ideal single photons. By randomly varying the intensity of pulses (decoy states), it detects photon number splitting attacks and improves key generation rates. This method allows practical implementations of QKD over longer distances with existing technology.

Other notable quantum cryptographic protocols include the SARG04 protocol [15], which modifies BB84 to improve robustness against photon number splitting attacks, and device-independent QKD [16], which aims to provide security guarantees without trusting the internal workings of the devices used.

In addition to these protocols, post-quantum cryptography encompasses classical cryptographic algorithms designed to resist attacks by quantum computers. These include lattice-based cryptography, code-based cryptography, hash-based signatures, and multivariate polynomial cryptosystems. While not quantum cryptography per se, they are important complementary approaches for securing communication in a future where quantum computers may break many classical schemes.

2.4. Artificial Intelligence

Artificial Intelligence (AI) encompasses a wide range of computational methods that enable machines to perform tasks traditionally requiring human intelligence, such as learning, reasoning, and decision-making. In adaptive security systems and intelligent environments, AI techniques are fundamental for analyzing complex data, detecting anomalies, predicting threats, and enabling autonomous adaptation to evolving conditions.

2.4.1. Supervised Learning

Supervised learning algorithms operate on datasets composed of input-output pairs, where the output labels serve as ground truth to guide the learning process. The primary objective is to learn a function $f : X \to Y$ that generalizes well to unseen inputs X, accurately predicting the corresponding outputs Y. This is typically achieved by minimizing a loss function $\mathcal{L}$, such as mean squared error for regression tasks or cross-entropy for classification problems, using optimization methods like gradient descent.

Common supervised learning models include decision trees, support vector machines (SVM), and neural networks. Decision trees recursively partition the feature space based on attribute thresholds, producing interpretable models that are effective for classification and regression. SVMs find hyperplanes that maximize the margin between classes in a transformed feature space, often using kernel functions to handle nonlinearity.

Neural networks, inspired by the structure of biological neurons, consist of layers of interconnected nodes (neurons) that apply weighted sums and nonlinear activation functions to inputs. Deep neural networks (DNNs) extend this architecture by stacking multiple hidden layers, enabling the extraction of hierarchical and abstract features from raw data. This capability has led to breakthroughs in complex pattern recognition tasks such as image classification, speech recognition, and natural language processing. Formally, a feedforward neural network computes an output $\hat{y}$ as:

$$\hat{y} = f(x; \theta) = f^{(L)} \circ f^{(L-1)} \circ \cdots \circ f^{(1)}(x)$$

where each $f^{(l)}$ represents the transformation at layer l, parameterized by weights and biases θ, and $\circ$ denotes function composition. Variants such as convolutional neural networks (CNNs) specialize in processing spatial data by applying convolutional filters, while recurrent neural networks (RNNs) and their gated variants (LSTM, GRU) are designed for sequential data modeling.

In cybersecurity, supervised learning models are widely used for tasks like malware detection, intrusion detection, spam filtering, and user authentication. However, these models require large labeled datasets,

Table 1
Key Quantum Cryptography Protocols and Metrics

Protocol	Key Formula / Metric	Description
BB84	$QBER = \frac{N_{\text{error}}}{N_{\text{total}}}$	Quantum Bit Error Rate measures the error rate in the raw key. A low QBER indicates secure transmission; a high QBER signals eavesdropping or noise.
E91	$S = \lvert E(a,b) + E(a,b') + E(a',b) - E(a',b')\rvert \leq 2$ (classical limit)	Security is guaranteed by violation of Bell's inequalities, indicating quantum entanglement and absence of eavesdropping.
CV-QKD	$K = \beta I_{AB} - \chi_{BE}$	Secret key rate depends on reconciliation efficiency β, mutual information I_{AB}, and Holevo bound χ_{BE} quantifying eavesdropper's information.
MDI-QKD	No simple formula; relies on entanglement swapping and Bell state measurements	Removes trust assumptions on measurement devices, mitigating detector side-channel attacks.
Decoy State	Statistical detection of photon number splitting attacks	Uses variable intensity pulses to detect eavesdropping on weak coherent pulse QKD systems.
SARG04	Variation of BB84 with modified sifting procedure	Improves robustness against photon number splitting attacks in practical QKD implementations.
Device-Independent QKD	Security based on violation of Bell inequalities without trusting devices	Provides security guarantees even if the quantum devices are untrusted or imperfect.
Post-Quantum Cryptography	Various hardness assumptions (e.g., lattice problems)	Classical algorithms designed to resist quantum attacks, based on mathematical problems believed to be hard for quantum computers.

which can be expensive and time-consuming to obtain, especially for emerging threats. Despite this limitation, supervised learning remains a cornerstone due to its high accuracy and interpretability when sufficient labeled data is available.

2.4.2. Unsupervised Learning

Unsupervised learning deals with unlabeled data, aiming to discover intrinsic structures or patterns within datasets without predefined categories. A primary class of unsupervised methods is clustering, which groups data points based on similarity or distance metrics. Common clustering algorithms include k-means, hierarchical clustering, and DBSCAN, each with distinct mechanisms and assumptions.

The k-means algorithm partitions data into k clusters by minimizing the within-cluster sum of squares:

$$J = \sum_{j=1}^{k} \sum_{x_i \in C_j} \|x_i - \mu_j\|^2$$

where μ_j is the centroid of cluster C_j. K-means assumes spherical clusters of similar size and is sensitive to initialization and the choice of k. Hierarchical clustering builds a tree-like structure (dendrogram) representing nested groupings of data points. Agglomerative methods start with each point as a separate cluster and iteratively merge the closest pairs, while divisive methods begin with all points in one cluster and recursively split them. This approach does not require specifying the number of clusters upfront and can capture complex cluster shapes.

DBSCAN (Density-Based Spatial Clustering of Applications with Noise) identifies clusters as dense regions separated by areas of lower density. It can detect arbitrarily shaped clusters and is robust to noise and outliers. DBSCAN requires two parameters: the neighborhood radius ϵ and the minimum number of points $MinPts$ to form a dense region. Other clustering methods include Gaussian Mixture Models (GMM), which assume data is generated from a mixture of Gaussian distributions and use expectation-maximization to estimate parameters. Spectral clustering leverages the eigenvalues of similarity matrices to perform dimensionality reduction before clustering, effective for non-convex clusters.

Dimensionality reduction techniques such as Principal Component Analysis (PCA) and t-Distributed Stochastic Neighbor Embedding (t-SNE) are often used alongside clustering to reduce data complexity while preserving important structures. PCA projects data onto orthogonal components maximizing variance, facilitating visualization and noise reduction. t-SNE is a nonlinear technique that preserves local neighborhood structures, useful for visualizing high-dimensional data in two or three dimensions. Autoencoders, a class of neural networks, are widely employed in unsupervised learning. They consist of an encoder that compresses input data into a lower-dimensional latent space and a decoder that reconstructs the original input. The network is trained to minimize reconstruction error, typically measured by mean squared error:

$$\mathcal{L} = \frac{1}{n} \sum_{i=1}^{n} \|x_i - \hat{x}_i\|^2$$

where x_i is the input and $\hat{x}_i$ is the reconstruction. High reconstruction errors can indicate anomalies, making

autoencoders effective for detecting novel or unknown threats in security applications. Unsupervised learning is particularly valuable in cybersecurity contexts where labeled attack data is scarce or unavailable. By learning normal behavior patterns, these methods enable the identification of deviations that may correspond to emerging threats or zero-day attacks. The combination of clustering, dimensionality reduction, and neural network-based approaches provides a versatile toolkit for anomaly detection and behavior profiling in complex, dynamic environments.

2.4.3. Reinforcement Learning

Reinforcement learning (RL) is a learning paradigm where an agent learns to make sequential decisions by interacting with an environment. At each discrete time step t, the agent observes the current state s_t, selects an action a_t, receives a scalar reward r_t, and transitions to a new state s_{t+1}. The objective of the agent is to learn a policy π, which is a mapping from states to actions, that maximizes the expected cumulative discounted reward:

$$G_t = \sum_{k=0}^{\infty} \gamma^k r_{t+k}$$

where $\gamma \in [0, 1)$ is the discount factor that balances the importance of immediate versus future rewards. Value-based methods, such as Q-learning, estimate the optimal action-value function $Q^*(s, a)$, which represents the expected return of taking action a in state s and following the optimal policy thereafter. The Q-values are updated iteratively using the Bellman equation:

$$Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha \left(\gamma \max_a Q(s_{t+1}, a) - Q(s_t, a_t) \right)$$

where α is the learning rate controlling the update step size. Policy-based methods, in contrast, directly optimize the policy $\pi(a|s)$ by maximizing the expected reward using gradient ascent techniques. Actor-critic algorithms combine value-based and policy-based approaches by maintaining both a policy function (actor) and a value function (critic), which improves learning stability and efficiency.

Deep Reinforcement Learning (DRL) integrates deep neural networks with RL algorithms to approximate value functions or policies in high-dimensional state and action spaces. Notable DRL algorithms include Deep Q-Networks (DQN), which use convolutional neural networks to approximate Q-values, and Proximal Policy Optimization (PPO), a policy-gradient method that balances exploration and exploitation with stable updates. In adaptive security systems, RL and DRL have been applied to dynamic access control, automated intrusion response, resource allocation, and threat mitigation. These methods enable systems to learn optimal defense strategies in complex, uncertain, and evolving environments where explicit models are unavailable or impractical.

The AI learning paradigms and models discussed in this subsection, summarized in Table 2, provide a comprehensive toolkit for designing adaptive and intelligent security solutions. Each paradigm—supervised, unsupervised, and reinforcement learning—offers unique strengths and is suited to different aspects of security challenges, from classification and anomaly detection to sequential decision-making and autonomous adaptation.

3. State of the Art

The increasing complexity of intelligent environments, coupled with the growing demand for robust privacy and security mechanisms, has driven significant research interest in adaptive and context-aware solutions. These solutions often leverage artificial intelligence (AI) and advanced cryptographic techniques to address the dynamic and heterogeneous nature of modern systems. This section presents a systematic review of the current landscape, focusing on the integration of self-adaptive security systems, quantum and post-quantum cryptography, and AI-driven learning strategies.

3.1. Inclusion and Exclusion Criteria

To ensure the rigor and relevance of the systematic review, the selection of articles was guided by well-defined inclusion and exclusion criteria. These criteria were established to filter out studies that do not directly contribute to research objectives, thus improving the quality and focus of the review.

The inclusion criteria (IC) prioritized studies published in peer-reviewed venues such as journals, conferences, and workshops (IC1), ensuring that only scientifically validated work was considered. Additionally, only articles written in English (IC2) were included to maintain consistency in language and facilitate comprehensive analysis. Crucially, the studies had to explicitly address topics related to adaptive security, cryptography, and artificial intelligence as defined by the search string (IC3), guaranteeing alignment with the core themes of the research.

Conversely, the exclusion criteria (EC) were designed to remove redundant or irrelevant studies. Duplicate works (EC1) were excluded to avoid bias and overrepresentation of findings. Literature reviews and systematic mappings (EC2) were omitted since the focus was on primary research articles presenting original contributions. Studies that did not align with the specific research questions (EC3) were also excluded to maintain the review's targeted scope. Finally, publications that did not address smart or intelligent environments or related

Table 2
Representative AI Models and Algorithms

Model/Algorithm	Learning Paradigm	Description
Decision Trees	Supervised	Tree-structured classifiers that recursively split data based on feature thresholds to create interpretable decision rules. Widely used for classification and regression tasks in security, such as intrusion detection.
Support Vector Machines (SVM)	Supervised	Finds optimal hyperplanes that maximize the margin between classes in a high-dimensional feature space. Effective for binary classification problems with clear margins, such as malware detection.
Random Forests	Supervised	Ensemble of decision trees that improves generalization by averaging multiple trees trained on random subsets of data and features. Robust against overfitting and commonly used in security analytics.
Gradient Boosting Machines (GBM)	Supervised	Sequential ensemble method that builds models by optimizing residual errors of previous models. Known for high accuracy in classification and regression tasks.
Deep Neural Networks (DNN)	Supervised	Multi-layer networks capable of learning hierarchical feature representations from raw data. Applied in complex pattern recognition tasks such as anomaly detection and biometric authentication.
Convolutional Neural Networks (CNN)	Supervised	Specialized DNNs designed for spatial data processing, effective in image and signal analysis, including malware classification from binary images or network traffic visualization.
Recurrent Neural Networks (RNN)	Supervised	Networks with feedback connections suited for sequential data modeling, such as time-series analysis in intrusion detection and user behavior modeling.
K-means Clustering	Unsupervised	Partitions data into k clusters by minimizing within-cluster variance. Used for grouping similar network flows or user activities to detect anomalies.
Hierarchical Clustering	Unsupervised	Builds nested clusters by either agglomerative or divisive methods, useful for exploratory data analysis and anomaly detection in security logs.
DBSCAN (Density-Based Spatial Clustering)	Unsupervised	Identifies clusters based on density, capable of detecting arbitrarily shaped clusters and noise, effective for outlier detection in network traffic.
Autoencoders	Unsupervised	Neural networks that learn compressed representations by reconstructing inputs. High reconstruction error indicates anomalies, useful in detecting novel attacks.
Principal Component Analysis (PCA)	Unsupervised	Linear dimensionality reduction technique that projects data onto principal components, facilitating visualization and anomaly detection.
Q-learning	Reinforcement	Value-based RL algorithm that learns the optimal action-value function through iterative updates, suitable for discrete action spaces in adaptive security policies.
Deep Q-Network (DQN)	Reinforcement	Combines Q-learning with deep neural networks to handle high-dimensional state spaces, applied in dynamic intrusion response and resource allocation.
Policy Gradient Methods	Reinforcement	Directly optimize the policy by gradient ascent on expected rewards, enabling continuous action spaces and stochastic policies.
Actor-Critic Algorithms	Reinforcement	Hybrid methods combining value function estimation (critic) and policy optimization (actor), balancing bias and variance for stable learning.
Proximal Policy Optimization (PPO)	Reinforcement	Policy-gradient method that uses clipped objective functions to ensure stable and efficient policy updates, widely used in complex adaptive systems.

contexts (EC4) were filtered out, as these environments are central to the research focus on adaptive security and cryptography.

Table 3 summarizes these criteria, which collectively ensured a robust and focused selection process, enabling a comprehensive and meaningful synthesis of the state of the art in adaptive security systems integrating cryptography and AI.

3.2. Article Sources and Distribution

The initial search retrieved 1,606 articles from multiple databases using the comprehensive search string described in Table 4. After removing duplicates and applying the inclusion and exclusion criteria, the number of articles was progressively reduced through title and abstract screening, followed by full-text analysis. The final set of 67 articles was selected for detailed review.

The selected 67 articles were published across several reputable publishers. The distribution is as follows: IEEE published 25 articles, Springer 20 articles, Nature 12 articles, Elsevier 8 articles, and other publishers accounted for 2 articles. This distribution reflects the multidisciplinary nature of the research area, spanning computer science, cybersecurity, and cryptography domains.

Figure 1 illustrates the flow of the study selection process, showing the reduction from the initial 1,569 articles to the final 67 included studies.

Table 3
Inclusion and exclusion criteria of the research.

Criterion	Definition
Inclusion	
IC1	Studies published in peer-reviewed journals, conferences, or workshops.
IC2	Articles written in English.
IC3	The study must contain the terms defined in the search string related to adaptive security, cryptography, and AI.
Exclusion	
EC1	Duplicate works.
EC2	Literature reviews or systematic mappings.
EC3	Studies not aligned with the research questions.
EC4	Publications not addressing smart or intelligent environments or related contexts.

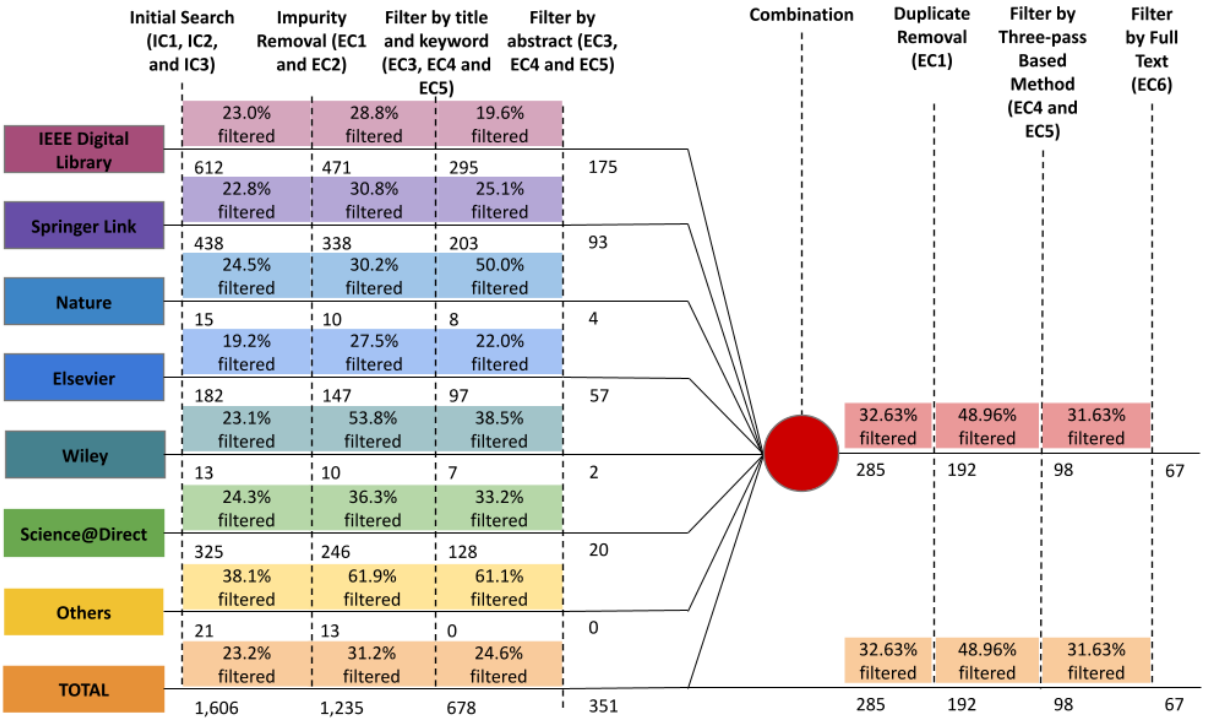

Figure 1: Flow of the study selection process.

3.3. Search and Selection Process

To systematically map the current landscape, we conducted a systematic literature review following the methodology proposed by [17]. This approach ensures a transparent, replicable, and unbiased process for identifying, selecting, and analyzing relevant studies. The review was guided by research questions targeting the intersection of self-adaptive security, cryptography (including quantum and post-quantum approaches), and AI-based adaptation strategies.

The search process was structured around a comprehensive string (see Table 4) that combines terms related to self-adaptive security systems, cryptography, adaptive quantum cryptography, and AI/learning techniques. This string was applied across major scientific databases, ensuring coverage of peer-reviewed articles published in English and directly addressing the research questions.

After applying inclusion and exclusion criteria inspired by best practices in systematic reviews, the selected studies were analyzed and categorized according to the type of cryptography, AI technique, self-adaptive strategy, and the intelligent environment addressed. Table 5 summarizes the main characteristics of the selected works.

The literature reveals that self-adaptive security systems are increasingly adopting the MAPE-K (Monitor, Analyze, Plan, Execute, Knowledge) model as a reference architecture for continuous adaptation. This model enables systems to autonomously monitor their environment, analyze contextual data, plan adaptive actions, and execute changes in real time, often leveraging AI techniques such as machine learning, clustering, and reinforcement learning to optimize decision-making and resource allocation.

Table 4
Search string.

Main term	String
Self-adaptive Security Systems	("self-adaptive system*" OR "autonomic security" OR "adaptive security" OR "self-adaptive secur*" OR "MAPE-K" OR "self-healing security" OR "context-aware security")
Cryptography	AND ("cryptograph*" OR "encryption" OR "data privacy" OR "data protection" OR "post-quantum cryptograph*" OR "quantum cryptograph*" OR "quantum encryption" OR "quantum-safe" OR "quantum-resistant")
Adaptive Quantum Cryptography	AND ("adaptive quantum cryptograph*" OR "context-aware quantum cryptograph*" OR "dynamic quantum encryption" OR "quantum key distribution" OR "QKD" OR "quantum cryptography strategy" OR "quantum cryptography protocol")
AI and Learning Techniques	AND ("reinforcement learning" OR "machine learning" OR "artificial intelligence" OR "deep learning" OR "clustering" OR "predictive modeling" OR "intelligent agent*" OR "RL agent" OR "AI-based")

In the context of cryptography, there is a clear trend toward the adoption of quantum-resistant and post-quantum algorithms, especially in environments where long-term data confidentiality is critical. Several works explore the integration of adaptive cryptographic protocols that can dynamically adjust their security level based on environmental context or detected threats, often using AI to guide these adaptations.

AI and learning techniques play a central role in enabling self-adaptation. Machine learning and deep learning are widely used for anomaly detection, predictive modeling, and adaptive policy selection. Reinforcement learning, in particular, is highlighted for its ability to optimize adaptive strategies in dynamic and uncertain environments, such as IoT networks and smart grids. Despite these advances, the literature also identifies several challenges and open issues. These include the computational cost of integrating AI and advanced cryptography, the complexity of real-time adaptation in large-scale distributed systems, and the need for hybrid approaches that combine AI with traditional rule-based or heuristic methods, especially in resource-constrained environments.

The state of the art demonstrates a convergence of self-adaptive security, advanced cryptography, and AI-driven adaptation as key enablers for resilient and secure intelligent environments. The systematic review and the synthesis presented in Table 5 provide a structured overview of current solutions, highlight research gaps, and suggest directions for future work, such as the development of unified frameworks that seamlessly integrate adaptive security, quantum cryptography, and AI-based decision-making. The collected works reveal a variety of approaches and techniques applied to ensure security in intelligent environments, highlighting the importance of dynamic adaptation to respond to threats and changes in the operational context.

Chen et al. [18] propose a self-adaptive system that employs reinforcement learning to dynamically adjust security levels in wireless sensor networks. Their focus is on optimizing energy consumption while maintaining data confidentiality, demonstrating the effectiveness of combining AI techniques with adaptive strategies in resource-constrained environments. Similarly, Chen et al. [18] present an innovative method that integrates deep reinforcement learning with blockchain-based adaptive computation offloading in mobile crowdsensing, optimizing resource use and security.

The integration of quantum cryptography with machine learning algorithms for real-time attack detection and mitigation is explored by et al. [19], who emphasize how hybrid quantum key distribution systems can enhance security in quantum networks. In a related vein, Grasselli [20] investigate device-independent quantum cryptography protocols, addressing technical challenges to secure resource-limited devices.

Frameworks based on the MAPE-K model for self-adaptive cybersecurity systems are detailed by Saad Inshi [21], who describe how the architecture enables continuous monitoring, analysis, planning, and execution of corrective actions supported by a shared knowledge base. This facilitates ongoing adaptation to emerging threats. Context-aware adaptive strategies for authentication systems are studied by Saad Inshi [21], who utilize attribute-based encryption and context-aware adaptive security to adjust mechanisms according to user profiles and environmental factors, improving usability without compromising security.

The use of machine learning algorithms for intrusion detection in IoT networks, combined with self-adaptive techniques to adjust security parameters in real time, is discussed by Bhat et al. [22]. Their work highlights the importance of adaptive intelligence to handle the heterogeneity and dynamics of connected devices. A systematic review on self-adaptive security systems by Mehto et al. [23] emphasizes existing gaps in integrating AI techniques with advanced cryptography and suggests future research directions to better unify these areas. Nia [24] propose a contextual security model that leverages deep learning to analyze multiple data sources and adapt security policies in corporate environments. Their study demonstrates that combining contextual analysis with AI can increase resilience against sophisticated attacks.

Table 5: Summary of selected works on adaptive security, cryptography, and AI.

Reference	Type of Cryptography	Type of AI	Self-Adaptive Strategy	Intelligent Environment	Year
Ahmed et al. [25]	Signature-based (classical)	ML and DL with Fuzzy Clustering	Fuzzy Clustering for adaptive intrusion detection	Network security / IDS	2025
Nia [24]	Not specified (likely classical)	Agentic AI (autonomous)	Self-healing adaptive threat response	Autonomous systems	2023
Authors [26]	General (review)	General (review)	General (review)	General cybersecurity	2023
Authors [27]	General (review)	AI for cybersecurity	General (review)	General cybersecurity	2023
Bhat et al. [22]	Not specified	Not specified	Trend analysis	Security and justice	2025
Xiong et al. [28]	Quantum-resistant hybrid encryption	Not specified	Not specified	IoT in smart grids	2025
Swayne [29]	Post-quantum cryptography	Not specified	Not specified	Quantum cybersecurity	2024
et al. [19]	Hybrid QKD (continuous and discrete)	Not specified	Hybrid QKD system integration	Quantum networks	2024
et al. [30]	Quantum metrology (not encryption)	Not specified	Not specified	Quantum physics applications	2023
Jayanthi et al. [31]	Post-quantum (Kyber and others)	Not specified	Not specified	Post-quantum security	2023
Chen et al. [18]	Blockchain-based	Deep RL (PPO and DNC)	Adaptive computation offloading	Mobile crowdsensing (MCS)	2024
et al. [32]	RSA (classical)	Not specified	Not specified	IoT security	2023
Mehto et al. [23]	Not specified	Particle Swarm Optimization (metaheuristic)	Multi-objective optimization	Wireless sensor networks	2021
Alatawi [33]	ECC (classical)	Not specified	Dynamic authenticated credentials	IoT	2024
Ammi Blackwood [34]	Hybrid quantum cryptography	Hybrid LLM	Adaptive cyber defense	Cybersecurity	2024
Israel Koren [35]	Classical cryptography	Not specified	Adaptive fault detection	Fault-tolerant systems	2021
Wei Cheng [36]	Classical cryptography	Not specified	Side-channel analysis	Cryptographic security	2025
Xiaolu Hou [37]	Modern cryptography	Not specified	Adaptive implementations	Embedded security	2024
P. Aberna [38]	Blockchain-based	Not specified	Adaptive watermarking system	Tamper detection	2025
Sahan Bandara [39]	Not specified	Not specified	Adaptive cache defense	Cryptographic engineering	2020
Mohamed [40]	Quantum, Blockchain, Lightweight, Chaotic, DNA	Not specified	Not specified	General cryptography	2020
Grasselli [20]	Device-independent quantum cryptography	Not specified	Not specified	Quantum technology	2021
Badhwar [41]	Post-quantum cryptography	Not specified	Not specified	Cybersecurity	2021
Christof Paar [42]	Post-quantum cryptography	Not specified	Not specified	Cryptography	2024
Christy et al. [43]	Quantum cryptography	Not specified	Not specified	Cryptographic security	2024
Rasolroveicy [44]	Blockchain	Not specified	Adaptive balancing (performance, security, energy)	IoT	2020
Irish Singh [45]	Blockchain	Not specified	Self-adaptive security for smart contracts	Smart contracts	2021
Jing Yang [46]	Not specified	Label-Adaptive Self-Rationalization	Adaptive explanation generation	Fact verification	2024
Ioannis Sorokos [47]	Not specified	Not specified	Evaluation of self-adaptive architectures	Autonomous driving	2024
Prutha Pawade [48]	Not specified	Not specified	Traffic density-based adaptive management	Traffic management	2024
Borce Postolov [49]	Not specified	Self-adaptive genetic algorithm	Security constrained scheduling	Energy systems	2021
Nawal Shaltout [50]	Computational genetic cryptography	Not specified	Self-adaptive substitution	Image security	2023
Borce Postolov [51]	Self-adaptive genetic algorithm	Not specified	Security constrained scheduling	Energy systems	2022
Sanchika Abhay Bajpai [52]	Not specified	Self-configurable deep learning	Adaptive intrusion detection	Network security	2024
Cheng [53]	Not specified	Not specified	Self-adaptive challenge analysis	Software engineering	2021
Zainab Dar [54]	Fuzzy ontology-based encryption	Not specified	Device and information classification	IoT	2023
Saad Inshi [55]	Lightweight context-aware encryption	Not specified	Context-aware encryption	Android applications	2020
Saad Inshi [21]	Attribute-based encryption	Not specified	Context-aware adaptive security	Tactical networks	2022
Furkh Zeshan [56]	Fuzzy ontology-based encryption	Not specified	Device and information classification	IoT	2024
Gitanjali Gupta [57]	Security-aware sensitive encryption	Not specified	Adaptive encrypted storage	Big data	2020
Dera [58]	Not specified	Lightweight neural networks	Adaptive embedded system	Embedded systems	2021
Inayat Khan [59]	Not specified	Not specified	Adaptive SMS client	Risk behavior reduction	2021
Christy et al. [60]	Not specified	Adaptive collaborative filtering	Adaptive recommendation	Information systems	2022
Yu Chi Lin [61]	Not specified	Adaptive machine learning	Dynamic field selection	Information security	2024
A R and Katiravan [62]	Not specified	Adaptive machine learning	Adaptive security framework	IoT	2024
Alsalman [63]	Not specified	Adaptive machine learning	Adaptive anomaly detection	IoT	2024
Rani Al Rahbani [64]	Not specified	Adaptive heuristics and ML	Adaptive DDoS detection	IoT	2022
Xiaomeng Feng [65]	Not specified	Machine learning	Cyber-physical system security	Energy	2022
Hari Gonaygunta [66]	Not specified	Adaptive machine learning	Adaptive cybersecurity	General	2024
Nuruddin Wiranda [67]	Not specified	Machine learning	Security for ML and ML for security	General	2021

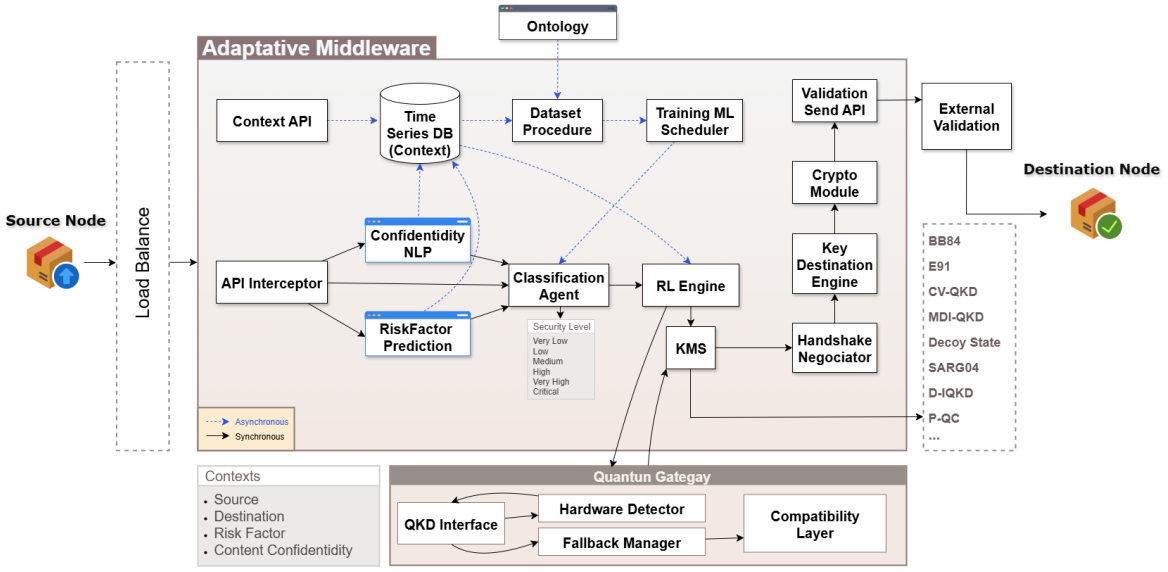

Figure 2: Overview of the proposed adaptive security middleware architecture.

Although the reviewed works contribute valuable insights into self-adaptive security systems, specific gaps remain unaddressed. There is a notable absence of integrated frameworks that combine quantum cryptography with reinforcement learning and clustering techniques to enable context-dependent adaptive security decisions. Current studies often overlook the dynamic selection of cryptographic levels based on real-time data context and risk assessment. Moreover, few approaches consider the challenges of deploying such adaptive systems in resource-constrained environments like IoT devices or wireless sensor networks. Additionally, the integration of MAPE-K feedback loops with quantum-safe algorithms for continuous adaptation has not been thoroughly explored. Finally, practical validation of these adaptive mechanisms in large-scale, heterogeneous intelligent environments is still lacking, limiting their applicability in real-world scenarios.

4. Proposed Model

Figure 2 presents an overview of the proposed self-adaptive security middleware architecture. This model is designed as a plug-and-play solution, requiring no modifications to the existing environment, and is capable of integrating both classical and quantum cryptographic algorithms. The architecture is composed of several interconnected modules, each responsible for a specific stage in the secure data transmission process.

4.1. Architecture Overview and Data Flow

The data flow begins when a source node sends information, which is first received by a load balancer. This component distributes incoming requests to available middleware nodes, ensuring scalability and high availability. Within the middleware, an API Interceptor captures the incoming message, extracting both payload and metadata. Simultaneously, a Context API collects contextual information related to the transaction, such as origin, destination, application, and risk factors. Both the intercepted data and contextual information are stored in a time-series context database, enabling historical analysis and real-time context enrichment.

The context database is integrated with a classification procedure that continuously generates updated datasets, classifying each context according to its security level. The classification leverages inferences from an ontology, enabling semantic enrichment and more accurate risk assessment. These datasets are used by a training scheduler to periodically train classification and clustering models, ensuring that the system adapts to evolving threats and context patterns.

After the initial data capture and context enrichment, the API Interceptor forwards the original message and its associated context to a classifier agent. This agent utilizes the contextual data and the latest trained models to assign a security level to the transaction. Once the security level is determined, the information is passed to a Reinforcement Learning (RL) Engine. The RL Engine updates its state using the current context, message content (potentially processed with NLP techniques for security sentiment analysis), and the security level provided by the classifier. The RL agent then selects the most appropriate cryptographic algorithm for the transaction, considering both traditional and quantum

options, and balancing security, performance, and resource availability.

A central challenge in adaptive cryptographic environments is secure key management, especially when the cryptographic algorithm is selected dynamically. The middleware, in conjunction with the Quantum Gateway, negotiates key requirements with the destination node, based on the selected algorithm. This may involve classical key exchange protocols (e.g., Diffie-Hellman, RSA) or quantum key distribution (QKD) sessions. Keys are derived and stored in a secure enclave, mapped to transaction or session identifiers, and are rotated or destroyed according to policy. If quantum key exchange is not possible, the system falls back to post-quantum or hybrid key exchange schemes, maintaining security guarantees. All key management operations are abstracted behind APIs, allowing seamless integration with legacy systems and minimizing operational overhead.

4.2. Quantum Gateway

A key innovation of the proposed architecture is the Quantum Gateway module, which enables the use of quantum cryptography even in environments that do not natively support quantum communication or quantum key distribution (QKD). The Quantum Gateway acts as an abstraction and translation layer between the classical middleware and quantum resources. When the RL agent selects a quantum-safe or quantum-native algorithm, the gateway checks the availability of quantum resources. If QKD or quantum hardware is available, the gateway orchestrates the key exchange and cryptographic operations. Otherwise, it transparently falls back to post-quantum cryptography (PQC) or hybrid schemes, ensuring security without requiring changes in the legacy environment.

Mathematically, the gateway can be modeled as a function G that, given the required security level L and the set of available resources Q, selects the cryptographic mode M:

$$M = G(L, Q) = \begin{cases} \text{Quantum-native}, & \text{if } L \geq L_Q \text{ and } QKD \in Q \\ \text{PQC/Hybrid}, & \text{if } L \geq L_Q \text{ and } QKD \notin Q \\ \text{Classical}, & \text{otherwise} \end{cases}$$

where L_Q is the minimum security level that triggers quantum or post-quantum cryptography.

The gateway manages the negotiation, allocation, and lifecycle of quantum keys, exposing a simple API to the middleware, and logs all quantum operations for auditing and compliance. For each session s, the gateway maintains a key k_s such that:

$$k_s = \begin{cases} k_{QKD}, & \text{if QKD available} \\ k_{PQC}, & \text{if PQC fallback} \\ k_{classical}, & \text{otherwise} \end{cases}$$

This abstraction allows the rest of the system to remain agnostic to the underlying quantum mechanisms.

4.3. Classification Model for Security Level Assessment

The supervised classification model is responsible for assigning a risk/security level to each transaction. The risk score R for a given transaction is computed as a weighted sum of multiple features:

$$R = \sum_{i=1}^{n} w_i \cdot f_i(\mathbf{x})$$

where w_i are the learned weights, $f_i(\mathbf{x})$ are the feature functions (such as device reputation, time of day, or anomaly score), and $\mathbf{x}$ is the feature vector for the current transaction. The risk score is then mapped to a discrete security level $L \in \{\text{Very Low}, \text{Low}, \text{Moderate}, \text{High}, \text{Very High}, \text{Ultra}\}$ using predefined thresholds. The model considers a comprehensive set of features, including:

- **Origin Context:** Identity, reputation, location, device type, and behavioral history of the sender.
- **Destination Context:** Receiver profile, security policies, location, and environmental sensitivity.
- **Application Context:** Data type, information sensitivity, processing purpose, and service criticality.
- **Temporal Context:** Time, day of the week, attack seasonality, and special events.
- **Risk Factor Context:** Probability of attack at the given time/location, which can be estimated as:

  $$P_{attack}(t, l) = \sigma\left(\sum_{j=1}^{m} \alpha_j \cdot g_j(t, l)\right)$$

  where g_j are risk-related features (e.g., threat intelligence, anomaly detection), α_j are their weights, and σ is a sigmoid or softmax function.
- **Incident History:** Previous attacks, failures, and unauthorized access attempts.
- **Volume and Frequency:** Request volume, access patterns, and unusual bursts.
- **Ontology Inferences:** Semantic rules and inferences regarding context and criticality.

4.4. Reinforcement Learning for Cryptographic Algorithm Selection

The RL agent receives the security level from the classifier and, together with other dynamic factors, determines the optimal cryptographic algorithm and

security strategy. The RL agent's policy π can be formalized as:

$$\pi^*(s) = \arg\max_{a \in \mathcal{A}} Q^*(s, a)$$

where s is the current state (including context, risk level, and system status), a is the action (choice of cryptographic algorithm), and $Q^*(s, a)$ is the optimal action-value function learned from previous interactions. The reward function r for the RL agent is designed to balance security and performance, and can be defined as:

$$r = \lambda_1 \cdot S_{success} - \lambda_2 \cdot T_{latency} - \lambda_3 \cdot C_{resource} + \lambda_4 \cdot S_{compliance}$$

where $S_{success}$ is a binary variable indicating successful secure delivery, $T_{latency}$ is the observed latency, $C_{resource}$ is the computational cost, $S_{compliance}$ is a compliance score, and λ_i are tunable weights. The RL agent considers the following features in its decision process:

- **Risk Level:** Main input from the classifier.
- **System State:** Middleware load, hardware/software availability, latency, and computational resources.
- **Algorithm Performance:** Processing time, energy consumption, and success/failure rates from previous negotiations.
- **Quantum Resource Availability:** Support for QKD, quantum hardware, and fallback requirements.
- **Compliance Policies:** Legal, regulatory, or business constraints on algorithm usage.
- **Environmental Feedback:** Rewards from previous executions, such as delivery success, attack detection, or rejection by the destination.
- **Application Context:** Real-time, batch, or critical data considerations.
- **Exploration vs. Exploitation:** Occasional testing of new strategies to improve long-term policy.

4.5. Key Management and Distribution

Key management is a central challenge in adaptive cryptographic environments, especially when the cryptographic algorithm is selected dynamically. The middleware, in conjunction with the Quantum Gateway, negotiates key requirements with the destination node, based on the selected algorithm. This negotiation can be modeled as a handshake protocol H:

$$H = \begin{cases} H_{QKD}, & \text{if QKD available} \\ H_{PQC}, & \text{if PQC fallback} \\ H_{classical}, & \text{otherwise} \end{cases}$$

where H_{QKD}, H_{PQC}, and $H_{classical}$ represent the handshake protocols for quantum, post-quantum, and classical key exchanges, respectively.

Keys are derived and stored in a secure enclave, mapped to transaction or session identifiers, and are rotated or destroyed according to policy. All key management operations are abstracted behind APIs, allowing seamless integration with legacy systems and minimizing operational overhead.

4.6. Mapping Security Levels to Cryptographic Algorithms

Table 6 summarizes the mapping between security levels and recommended cryptographic algorithms. The mapping is designed to ensure that each transaction is protected with an algorithm appropriate to its assessed risk, balancing security, performance, and resource availability. Quantum algorithms are preferred or required for higher security levels, when available.

It is important to clarify that, within this architecture, the use of quantum cryptography refers specifically to the process of key distribution. Protocols such as BB84 and other QKD variants are employed to securely generate and exchange symmetric keys between communicating parties, leveraging the fundamental properties of quantum mechanics to guarantee confidentiality even in the presence of powerful adversaries. However, the actual encryption of data—whether at rest or in transit—continues to rely on classical or post-quantum cryptographic algorithms, such as AES, RSA, or lattice-based schemes. In practice, the quantum-generated key is used as the secret input for these well-established encryption algorithms, ensuring compatibility with existing systems and high performance for bulk data protection.

This hybrid approach is reflected in the table: for lower security levels, only classical algorithms are recommended, as the risk and sensitivity of the data do not justify the overhead of quantum key distribution. As the security level increases, the architecture allows for the use of post-quantum cryptography (PQC) algorithms, which are designed to resist attacks from quantum computers. For the highest security levels, the preferred or mandatory configuration is to combine QKD for key exchange with robust symmetric encryption (such as AES-256-GCM or one-time pad schemes), or to use hybrid models that integrate both classical and quantum-safe techniques. This ensures that even if future advances compromise classical cryptography, the confidentiality of the exchanged keys—and thus the protected data—remains intact.

This mapping provides a flexible and future-proof approach, allowing the middleware to adaptively select the most suitable cryptographic technique for each

Table 6
Mapping Security Levels to Cryptographic Algorithms

Security Level	Example Scenario	Suggested Algorithm(s)	Quantum Allowed?
Very Low	Public telemetry, non-sensitive logs	DES, RC4, MD5 (legacy only)	No
Low	Internal monitoring, basic IoT data	3DES, AES-128, RSA-1024, SHA-1	No
Moderate	Internal documents, user authentication	AES-192, AES-256, RSA-2048, ECC-256, SHA-256	No
High	Personal data, financial transactions	AES-256, RSA-4096, ECC-521, SHA-384, HMAC, PQC (Kyber, NTRU, Dilithium)	Yes (if available)
Very High	Healthcare, critical infrastructure, classified business data	AES-256-GCM, ECC-521, PQC (Kyber, NTRU, Saber, Falcon), Hybrid (RSA/PQC), QKD + OTP	Yes (preferred)
Ultra (Top Secret)	Military, government, state secrets	PQC (Kyber, NTRU, Saber, Falcon, Classic McEliece), QKD + OTP, Lattice-based, Supersingular Isogeny, AES-256-GCM	Yes (mandatory if available)

context, including the seamless integration of quantum-safe and quantum-native algorithms as the environment evolves.

4.7. Validation Scenarios

The validation of the proposed adaptive security middleware architecture can be approached through two complementary experimental scenarios, each offering distinct advantages for academic and professional research.

The first scenario involves deploying the architecture in an academic grid environment, such as Chameleon Cloud[1], CloudLab[2], or Fed4FIRE+[3]. In this context, it is possible to provision multiple virtual machines or containers to represent the various components of the system, including source nodes, the adaptive middleware, gateways, and destination nodes. The quantum cryptography layer is emulated using a simulator like SimulaQron[4], which enables the simulation of quantum key distribution (QKD) protocols such as BB84 and E91. Each node in the experiment can run an instance of the simulator, allowing the emulation of quantum channels and the negotiation of quantum keys as if real quantum hardware were present. This setup supports the orchestration of complex network topologies, the injection of faults or delays, and the automation of experiments, making it highly suitable for large-scale, reproducible academic studies. The integration of SimulaQron with the middleware allows for the full validation of the data flow, including key negotiation, encryption, fallback mechanisms, and context-aware adaptation, all within a controlled and scalable environment.

The second scenario explores the integration of the architecture with real quantum computing resources, specifically through the IBM Quantum Experience[5]. In this approach, the middleware is deployed in a cloud or grid environment, such as AWS, Azure, Google Cloud, or Chameleon Cloud, and interacts with IBM's quantum hardware or simulators via the Qiskit SDK[6]. The middleware can request the execution of quantum circuits, for example, implementing the BB84 protocol, to generate quantum keys using actual quantum processors or high-fidelity simulators provided by IBM. These keys are then retrieved and used to encrypt communications between nodes in the experimental setup. While this method does not provide a true quantum communication channel (QKD) between distributed nodes, it enables the practical integration of quantum key generation into the middleware workflow, leveraging real quantum hardware for prototyping and validation. This approach is particularly valuable for demonstrating the feasibility of hybrid classical-quantum security solutions and for gaining experience with the operational aspects of quantum computing platforms.

The table below summarizes the main differences between these two validation scenarios:

In summary, both scenarios provide valuable means for validating the proposed architecture. The academic grid with a quantum simulator offers a highly controllable and scalable environment for end-to-end emulation and performance analysis, while the integration with IBM Quantum Experience enables practical experimentation with real quantum key generation, supporting the development and demonstration of hybrid security solutions that bridge classical and quantum technologies.

5. Methodological Plan

The methodological plan for this research is structured into eight interrelated phases, each comprising specific activities that collectively ensure a comprehensive

[1] https://www.chameleoncloud.org/
[2] https://www.cloudlab.us/
[3] https://www.fed4fire.eu/
[4] https://github.com/SoftwareQuTech/SimulaQron
[5] https://quantum-computing.ibm.com/
[6] https://qiskit.org/

Aspect	Academic Grid with Simulator	Cloud/Grid with IBM Quantum
Quantum cryptography	Emulated QKD using SimulaQron	Real quantum key generation via IBM Quantum Experience
Communication channels	Simulated quantum channels between nodes	Classical channels; quantum keys generated and distributed via API
Scalability	High, with flexible topologies and many nodes	High, depending on cloud resources and quantum API throughput
Reproducibility	Very high, with full automation and control	High, but subject to quantum hardware queue and API limits
Cost	Low, with academic access to testbeds	Low to moderate, depending on cloud usage and IBM Quantum access
Realism	Protocol-level emulation, no real quantum hardware	Real quantum key generation, but no physical QKD channel
Recommended use	Prototyping, performance evaluation, academic research	Integration with quantum hardware, proof-of-concept, hybrid workflows

and incremental development of the adaptive security middleware and its supporting modules. The phases are designed to maximize synergy between ontology engineering, context and risk modeling, information reliability (NLP), quantum compatibility, middleware prototyping, and experimental validation. Many activities are planned to run in parallel, allowing for iterative refinement and integration across components. The overall schedule, including the overlap and dependencies among phases, is summarized in the project timeline (see Table 7), which distributes the main activities over the 36-month duration and highlights the parallelism and critical milestones of the project.

Phase 1: Foundations and Requirements (Months 1–6)

- Literature review and state of the art
- Requirements elicitation and scope definition

Phase 2: Ontology and Data Preparation (Months 4–12)

- Ontology design (OntOraculum)
- Dataset collection and annotation
- Semantic rule and query development

Phase 3: Risk Factor and Context Module Development (Months 7–15)

- Design and implementation of the risk factor calculation module
- Integration of context modeling (source, destination, application, temporal, etc.)
- Development of real-time risk prediction algorithms

Phase 4: Information Reliability and NLP Module (Months 10–18)

- Development of the information reliability module
- Implementation of NLP-based confidentiality detector
- Integration of reliability scores into the risk assessment pipeline

Phase 5: Quantum Compatibility and Gateway Module (Months 13–24)

- Design and implementation of the quantum compatibility module
- Development of the quantum gateway for hardware integration
- Fallback and hybrid cryptography strategies

Phase 6: Architecture and Middleware Development (Months 7–24)

- Architecture design
- Middleware prototyping
- Ontology-middleware integration

Phase 7: Model Training, Experimentation, and Evaluation (Months 16–33)

- Supervised model training
- Reinforcement learning agent training
- Experimentation in simulated and real environments
- Evaluation and refinement

Phase 8: Dissemination and Thesis (Months 25–36)

- Dissemination and publications (throughout the entire final year, in parallel with other activities)
- Thesis writing
- Thesis defense (final month)

The phases are intentionally designed to overlap wherever possible, enabling parallel progress across the various research fronts of the project. This overlapping structure allows for simultaneous advancements in ontology engineering, context and risk modeling,

Table 7
Project Timeline by Month (36 months, 8 phases)

Phase	Year 1												Year 2												Year 3											
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Foundations and Requirements																																				
2. Ontology & Data Preparation																																				
3. Risk Factor & Context Module																																				
4. Info Reliability & NLP Module																																				
5. Quantum Compat. & Gateway																																				
6. Arch. & Middleware Development																																				
7. Model Training, Experim., Eval.																																				
8. Dissemination & Thesis																																				

information reliability (NLP), quantum compatibility, middleware development, and experimental validation. For example, while the foundational literature review and requirements elicitation are being completed, the ontology and data preparation phase can already begin, ensuring that the project does not stall due to sequential dependencies. Similarly, the development of the risk factor and context module, the information reliability and NLP module, and the quantum compatibility gateway are scheduled to run in parallel with the architecture and middleware development, fostering integration and iterative refinement between these components.

The project timeline, as illustrated in Table 7, provides a month-by-month visualization of the eight main phases over the 36-month duration of the project. Each colored cell in the table indicates the active period for a given phase, while the vertical double lines demarcate the transition between years. This layout makes it easy to identify periods of concurrency, where multiple phases are progressing together, as well as critical milestones such as the final year dedicated to dissemination and thesis activities. By structuring the work in this way, the plan ensures both flexibility and efficiency, allowing for adjustments as new findings emerge and maximizing the potential for impactful research outcomes.

5.1. Publication Proposals

For the dissemination of the results of this research, a careful selection of publication venues was made to maximize both academic impact and the reach to relevant communities. The proposed venues include high-quality journals and leading international conferences that collectively cover the main scientific domains addressed by this work—namely, cybersecurity, adaptive security, artificial intelligence, semantic technologies, and quantum cryptography. The venues are grouped below as journals and conferences to highlight their respective roles in the dissemination strategy.

Among the journals, the following are proposed: **IEEE Security & Privacy Magazine**[7], a widely recognized publication that covers the latest developments, trends, and best practices in security and privacy, serving both academic and professional communities and making it an excellent venue for disseminating practical and innovative aspects of the proposed middleware architecture; **IEEE Transactions on Information Forensics and Security (TIFS)** (Q1)[8], a leading journal that publishes high-quality research on the science and engineering of information forensics, security, and privacy, particularly suitable for results related to cryptographic mechanisms, threat detection, and secure system design; **ACM Transactions on Privacy and Security (TOPS)** (Q1)[9], a top-tier journal that publishes original research on all aspects of privacy and security in computer systems, including theoretical foundations, practical implementations, and policy issues, ensuring dissemination to a global audience of experts in privacy, security, and cryptography; **Computers & Security** (Q1)[10], one of the most established and respected journals in the field of cybersecurity, covering a wide range of topics such as information security, privacy, cryptography, and secure systems, with an interdisciplinary scope and strong reputation that make it ideal for innovative results in secure middleware and quantum cryptography; and **npj Quantum Information** (Q1)[11], a leading journal dedicated to the theory and practice

[7] https://www.computer.org/csdl/magazine/sp
[8] https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8013
[9] https://dl.acm.org/journal/tops
[10] https://www.sciencedirect.com/journal/computers-and-security
[11] https://www.nature.com/npjqi/

of quantum information, including quantum cryptography, secure communication protocols, and quantum computing applications in security, particularly suitable for disseminating results related to the integration of quantum cryptography and quantum-safe algorithms in adaptive security middleware.

Regarding conferences, the following are proposed: **IEEE Symposium on Security and Privacy (S&P)**[12], one of the most prominent conferences in the field of security and privacy, providing an opportunity to share preliminary results, receive feedback from leading experts, and network with researchers working on related topics, with broad scope and high visibility that make it ideal for disseminating innovative aspects of the middleware, such as the integration of quantum cryptography and AI-driven security adaptation; **Privacy, Security and Trust (PST) Conference**[13], an established international conference focusing on the latest advances in privacy, security, and trust, and an excellent venue for presenting research on adaptive security, privacy-preserving technologies, and secure middleware solutions; and **EAI SecureComm – International Conference on Security and Privacy in Communication Networks**[14], a leading conference dedicated to the latest research in secure communications and privacy in networked systems, particularly suitable for presenting results on secure architectures, cryptographic protocols, and the application of AI and quantum technologies in communication security.

This combination of journals and conferences ensures that the research outcomes will be visible to both specialized and interdisciplinary audiences, fostering academic recognition, collaboration opportunities, and real-world impact.

6. Conclusion

This paper presents an initial proposal for an adaptive AI middleware system aimed at enhancing data privacy and security in smart environments through the dynamic selection of cryptographic levels. We have discussed the critical need for such a solution in the context of evolving quantum threats and the inherent heterogeneity of IoT ecosystems. Using clustering algorithms and RL agents within a MAPE-K framework, the proposed system aims to autonomously assess contextual information and threat levels, thus optimizing security measures in real time.

The integration of post-quantum cryptography (PQC) algorithms, alongside classical methods and Quantum Key Distribution (QKD) protocols, is central to our approach, ensuring resilience against both current and future quantum attacks. We have outlined the foundational concepts of data privacy, intelligent environments, quantum cryptography, and various AI paradigms (supervised, unsupervised, and reinforcement learning) that underpin this research. Our systematic review of the state of the art revealed a growing trend towards self-adaptive security systems, but also highlighted a significant gap in integrated frameworks that combine quantum cryptography with AI-driven adaptive decision-making for context-dependent security.

It is important to emphasize that this work represents a project in progress. Many architectural and operational details may evolve as the research advances, with new components and functionalities potentially being added, while others may be modified or removed based on experimental findings and practical considerations. The current model serves as a flexible foundation, open to refinement and adaptation as new requirements and challenges emerge.

[12] https://sp2026.ieee-security.org/

[13] https://pstnet.ca/pst2025/

[14] https://securecomm.eai-conferences.org/2026/

References

[1] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997. doi: https://doi.org/10.1137/S0097539795293172.

[2] Gorjan Alagic and et al. Status report on the fourth round of the nist post-quantum cryptography standardization process. *NIST Internal Report 8545*, 2025. URL https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8545.pdf. Accessed on: August 06, 2025.

[3] Christoph Dobraunig and et al. Standardized post-quantum cryptography and recent developments. *IEEE Communications Surveys & Tutorials*, 26(1):1–30, 2025. doi: https://doi.org/10.1109/CE2CT64011.2025.10939125.

[4] Jeffrey O. Kephart and David M. Chess. The vision of autonomic computing. *Computer*, 36(1):41–50, 2003. doi: https://doi.org/10.1109/MC.2003.1160055.

[5] Mohammad Salehie and Ladan Tahvildari. Self-adaptive software: Landscape and research challenges. *ACM Transactions on Autonomous and Adaptive Systems*, 4(2):1–42, 2009. doi: https://doi.org/10.1145/1538788.1538792.

[6] Anonymous. Performance analysis and industry deployment of post-quantum cryptography. *arXiv preprint arXiv:2503.12952*, 2025. URL https://arxiv.org/abs/2503.12952. Accessed on: August 06, 2025.

[7] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. pages 175–179, 1984. doi: https://doi.org/10.1016/j.tcs.2014.05.025.

[8] A. K. Ekert. Quantum cryptography based on bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991. doi: https://doi.org/10.1103/PhysRevLett.67.661.

[9] National Institute of Standards, Technology, and A. Smith. Nist releases first 3 finalized post-quantum encryption standards. *IEEE Security & Privacy*, 22(4):65–73, 2024. URL https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards. Accessed on: August 07, 2025.

[10] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179. IEEE, 1984. doi: https://doi.org/10.1016/j.tcs.2014.05.025.

[11] Artur K Ekert. Quantum cryptography based on bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991. doi: https://doi.org/10.1103/PhysRevLett.67.661.

[12] Christian Weedbrook, Stefano Pirandola, Raul Garcia-Patron, Nicolas J Cerf, Timothy C Ralph, Jeffrey H Shapiro, and Seth Lloyd. Gaussian quantum information. *Reviews of Modern Physics*, 84(2):621–669, 2012. doi: https://doi.org/10.1103/RevModPhys.84.621.

[13] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Physical Review Letters*, 108(13):130503, 2012. doi: https://doi.org/10.1103/PhysRevLett.108.130503.

[14] Won-Young Hwang. Quantum key distribution with high loss: Toward global secure communication. *Physical Review Letters*, 91(5):057901, 2003. doi: https://doi.org/10.1103/PhysRevLett.91.057901.

[15] Valerio Scarani, Antonio Acín, Gilles Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters*, 92(5):057901, 2004. doi: https://doi.org/10.1103/PhysRevLett.92.057901.

[16] Antonio Acín, Nicolas Gisin, and Lluis Masanes. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 97(12):120405, 2006. doi: https://doi.org/10.1103/PhysRevLett.97.120405.

[17] Kai Petersen, Robert Feldt, Shahid Mujtaba, and Michael Mattsson. Systematic mapping studies in software engineering. In *12th international conference on evaluation and assessment in software engineering (EASE)*. BCS Learning & Development, 2008. doi: https://doi.org/10.14236/ewic/EASE2008.8.

[18] Zheyi Chen, Junjie Zhang, Zhiqin Huang, Pengfei Wang, Zhengxin Yu, and Wang Miao. Computation offloading in blockchain-enabled mcs systems: A scalable deep reinforcement learning approach. *Future Generation Computer Systems*, 153:301–311, 2024. ISSN 0167-739X. doi: https://doi.org/10.1016/j.future.2023.12.004.

[19] Ren et al. Hybrid quantum key distribution network combining continuous and discrete variable qkd systems. *Quantum Information Processing*, 2024. doi: https://doi.org/10.1007/s11432-022-3509-6.

[20] Federico Grasselli. Device-independent quantum cryptography. *Quantum Science and Technology*, 2021. doi: https://doi.org/10.1007/978-3-030-64360-7_7.

[21] Hakima Ould-Slimane Saad Inshi, Rasel Chowdhury. Dynamic context-aware security in a tactical network using attribute-based encryption. In *MILCOM 2022 - 2022 IEEE Military Communications Conference (MILCOM)*. IEEE, 2022. doi: https://doi.org/10.1109/milcom55135.2022.10017647.

[22] Vanshikha Bhat, Anne Legrand, Conrad Agagan, Nick James, and Pierre-Adrien Hanania. Trends in 2025 for security and justice. https://www.capgemini.com/insights/expert-perspectives/trends-in-2025-for-security-and-justice/, 2025. Accessed on: August 06, 2025.

[23] Anjula Mehto, Shashikala Tapaswi, and K.K. Pattanaik. Multi-objective particle swarm optimization based rendezvous point selection for the energy and delay efficient networked wireless sensor data acquisition. *Journal of Network and Computer Applications*, 195:103234, 2021. ISSN 1084-8045. doi: https://doi.org/10.1016/j.jnca.2021.103234.

[24] Mehran Alidoost Nia. Ai driven self-healing cybersecurity systems with agentic ai for adaptive threat response and resilience. In *The Local Meeting for Open Challenges in Autonomous Systems*, 2023. URL https://www.researchgate.net/publication/392663570_AI_Driven_Self-Healing_Cybersecurity_Systems_with_Agentic_AI_for_Adaptive_Threat_Response_and_Resilience. Accessed on: August 06, 2025.

[25] Usama Ahmed, Mohammad Nazir, Amna Sarwar, Tariq Ali, El-Hadi M. Aggoune, Tariq Shahzad, and Muhammad Adnan Khan. Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering. *Scientific Reports*, 15:1726, 2025. doi: https://doi.org/10.1038/s41598-025-85866-7.

[26] Various Authors. Cyber security: State of the art, challenges and future directions. *Computers & Security*, 2023. doi: https://doi.org/10.1016/j.csa.2023.100031.

[27] Various Authors. Artificial intelligence for cybersecurity: Literature review and future research directions. *Journal of Network and Computer Applications*, 2023. doi: https://doi.org/10.1016/j.inffus.2023.101804.

[28] Jian Xiong, Lu Shen, Yan Liu, and Xiaofen Fang. Enhancing iot security in smart grids with quantum-resistant hybrid encryption. *Scientific Reports*, 15:3, 2025. doi: https://doi.org/10.1038/s41598-024-84427-8.

[29] Matt Swayne. 2025 expert quantum predictions — pqc and quantum cybersecurity. https://thequantuminsider.com/2024/12/31/2025-expert-quantum-predictions-pqc-and-quantum-cybersecurity/, 2024. Accessed on: August 06, 2025.

[30] Zhang et al. Quantum metrology with bloch oscillations in floquet phase space. *Physical Review A*, 107(2):022605, 2023. doi: https://doi.org/10.1103/PhysRevA.107.022605.

[31] S. Jayanthi, Sodagudi Suhasini, N. Sharmili, E. Laxmi Lydia, V. Shwetha, Bibhuti Bhusan Dash, and Mrinal Bachute. A deep dive into artificial intelligence with enhanced optimization-based security breach detection in internet of health things enabled smart city environment. *Scientific Reports*, 15(1):22909, 2025. ISSN 2045-2322. doi: https://doi.org/10.1038/s41598-025-05850-z.

[32] Mumtaz et al. Rsa-based authentication system for iot devices. *IEEE Transactions on Network and Service Management*, 20(1):45–58, 2023. doi: https://doi.org/10.1109/HPCC/SmartCity/DSS.2019.00112.

[33] Mohammed Naif Alatawi. Optimizing security and energy efficiency in iot-based health monitoring systems for wireless body area networks. *Scientific Reports*, 15(1):24921, 2025. ISSN 2045-2322. doi: https://doi.org/10.1038/s41598-025-11253-x.

[34] Stefan Baryshevsky Ammi Blackwood, Jonathan Carrington. The implementation of a hybrid large language model for adaptive cryptographic cyber defense. 2024. doi: https://doi.org/10.21203/rs.3.rs-5120507/v1.

[35] C. Mani Krishna Israel Koren. Fault detection in cryptographic systems. *Fault-Tolerant Systems*, 2021. doi: https://doi.org/10.1016/b978-0-12-818105-8.00021-8.

[36] Olivier Rioul Wei Cheng, Sylvain Guilley. Mathematical foundations for side-channel analysis of cryptographic systems. 2025. doi: https://doi.org/10.1007/978-3-031-64399-6.

[37] Jakub Breier Xiaolu Hou. Modern cryptographic algorithms and their implementations. *Cryptography and Embedded Systems Security*, 2024. doi: https://doi.org/10.1007/978-3-031-62205-2_3.

[38] L. Agilandeeswari P. Aberna. Powbwm: Proof of work consensus cryptographic blockchain-based adaptive watermarking system for tamper detection applications. *Alexandria Engineering Journal*, 2025. doi: https://doi.org/10.1016/j.aej.2024.10.016.

[39] Michel A. Kinsy Sahan Bandara. Adaptive caches as a defense mechanism against cache side-channel attacks. *Journal of Cryptographic Engineering*, 2020. doi: https://doi.org/10.1007/s13389-020-00246-3.

[40] Khaled Salah Mohamed. New trends in cryptography: Quantum, blockchain, lightweight, chaotic, and dna cryptography. *New Frontiers in Cryptography*, 2020. doi: https://doi.org/10.1007/978-3-030-58996-7_4.

[41] Raj Badhwar. The need for post-quantum cryptography. *The CISO's Next Frontier*, 2021. doi: https://doi.org/10.1007/978-3-030-75354-2_2.

[42] Tim Güneysu Christof Paar, Jan Pelzl. Post-quantum cryptography. *Understanding Cryptography*, 2024. doi: https://doi.org/10.1007/978-3-662-69007-9_12.

[43] C. Christy, A. Nirmala, A. Mary Odilya Teena, and A. Isabella Amali. Machine learning based multi-stage intrusion detection system and feature selection ensemble security in cloud assisted vehicular ad hoc networks. *Scientific Reports*, 15(1): 27058, 2025. ISSN 2045-2322. doi: https://doi.org/10.1038/s41598-025-96303-0.

[44] Mohammadreza Rasolroveicy. A self-adaptive blockchain framework to balance performance, security, and energy consumption in iot applications. In *2020 IEEE International Conference on Autonomic Computing and Self-Organizing Systems Companion (ACSOS-C)*. IEEE, 2020. doi: https://doi.org/10.1109/acsos-c51401.2020.00068.

[45] Seok-Won Lee Irish Singh. Self-adaptive security for sla based smart contract. In *2021 IEEE 29th International Requirements Engineering Conference Workshops (REW)*. IEEE, 2021. doi: https://doi.org/10.1109/rew53955.2021.00069.

[46] Anderson Rocha Jing Yang. Take it easy: Label-adaptive self-rationalization for fact verification and explanation generation. In *2024 IEEE International Workshop on Information Forensics and Security (WIFS)*. IEEE, 2024. doi: https://doi.org/10.1109/wifs61860.2024.10810687.

[47] Jan Reich Ioannis Sorokos, Patrick Wolf. Evaluating self-adaptive architectures for automated driving systems. In *2024 11th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*. IEEE, 2024. doi: https://doi.org/10.1109/iotsms62296.2024.10710315.

[48] Aditya Kadlag Prutha Pawade, Vrinda Parkhi. Self-adaptive traffic density based management system. In *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*. IEEE, 2024. doi: https://doi.org/10.1109/icbds61829.2024.10837297.

[49] Dimitar Dimitrov Borce Postolov, Atanas Iliev. N–1 security constrained short-term hydrothermal scheduling by self adaptive genetic algorithm with ptdf. In *2021 International Conference on Information Technologies (InfoTech)*. IEEE, 2021. doi: https://doi.org/10.1109/infotech52438.2021.9548482.

[50] Waleed M. Abd Al-Adrousy Nawal Shaltout, Ahmed A. El-Latif. Applicable image security based on computational genetic approach and self-adaptive substitution. *IEEE Access*, 2023. doi: https://doi.org/10.1109/access.2022.3233321.

[51] Dimitar Dimitrov Borce Postolov, Atanas Iliev. Novel self-adaptive genetic algorithm for solving ac security constrained short-term hydrothermal scheduling. In *2022 International Conference on Information Technologies (InfoTech)*. IEEE, 2022. doi: https://doi.org/10.1109/infotech55606.2022.9897098.

[52] Archana B. Patankar Sanchika Abhay Bajpai. Selfgt-bilstm: Modified self-configurable adaptive goal target optimized deep learning model for intrusion detection. In *2024 4th International Conference on Soft Computing for Security Applications (ICSCSA)*. IEEE, 2024. doi: https://doi.org/10.1109/icscsa64454.2024.00082.

[53] Shang-Wen Cheng. Change is the ultimate self-adaptive challenge. In *2021 International Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS)*. IEEE, 2021. doi: https://doi.org/10.1109/seams51251.2021.00042.

[54] Furkh Zeshan Zainab Dar, Adnan Ahmad. A fuzzy ontology-based context-aware encryption approach in iot through device and information classification. 2023. doi: https://doi.org/10.21203/rs.3.rs-3063290/v1.

[55] Mahdi Elarbi Saad Inshi, Rasel Chowdhury. Lca-abe: Lightweight context-aware encryption for android applications. In *2020 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE, 2020. doi: https://doi.org/10.1109/isncc49221.2020.9297354.

[56] Adnan Ahmad Furkh Zeshan, Zaineb Dar. A fuzzy ontology-based context-aware encryption approach in iot through device and information classification. *The Journal of Supercomputing*, 2024. doi: https://doi.org/10.1007/s11227-024-06317-0.

[57] Kamlesh Lakhwani Gitanjali Gupta. A novel security aware sensitive encrypted storage approach to improve the encryption of big data. 2020. doi: https://doi.org/10.21203/rs.3.rs-80029/v1.

[58] Abdi Dera. Lightweight neural networks for context aware embedded system. 2021. doi: https://doi.org/10.36227/techrxiv.16743901.

[59] Shah Khusro Inayat Khan. Context: Context-aware adaptive sms client for drivers to reduce risky driving behaviors. 2021. doi: https://doi.org/10.21203/rs.3.rs-933804/v1.

[60] C. Christy, A. Nirmala, A. Mary Odilya Teena, and A. Isabella Amali. Machine learning based multi-stage intrusion detection system and feature selection ensemble security in cloud assisted vehicular ad hoc networks. *Scientific Reports*, 15(1): 27058, 2025. ISSN 2045-2322. doi: https://doi.org/10.1038/s41598-025-96303-0.

[61] Po-Wen Chi Yu Chi Lin. Adaptive machine learning model for dynamic field selection. In *2024 19th Asia Joint Conference on Information Security (AsiaJCIS)*. IEEE, 2024. doi: https://doi.org/10.1109/asiajcis64263.2024.00032.

[62] Sathyabama A R and Jeevaa Katiravan. Enhancing anomaly detection and prevention in internet of things (iot) using deep neural networks and blockchain based cyber security. *Scientific Reports*, 15(1):22369, 2025. ISSN 2045-2322. doi: https://doi.org/10.1038/s41598-025-04164-4.

[63] Dheyaaldin Alsalman. A comparative study of anomaly detection techniques for iot security using adaptive machine learning for iot threats. *IEEE Access*, 2024. doi: https://doi.org/10.1109/access.2024.3359033.

[64] Jawad Khalife Rani Al Rahbani. Iot ddos traffic detection using adaptive heuristics assisted with machine learning. In *2022 10th International Symposium on Digital Forensics and Security (ISDFS)*. IEEE, 2022. doi: https://doi.org/10.1109/isdfs55398.2022.9800786.

[65] Shiyan Hu Xiaomeng Feng, Yang Liu. Machine learning for cyber-physical power system security. *Machine Learning for Embedded System Security*, 2022. doi: https://doi.org/10.1007/978-3-030-94178-9_4.

[66] Priyanka Pramod Hari Gonaygunta, Geeta Nadella. Study on empowering cyber security by using adaptive machine learning methods. In *2024 Systems and Information Engineering Design Symposium (SIEDS)*. IEEE, 2024. doi: https://doi.org/10.1109/sieds61124.2024.10534694.

[67] Fal Sadikin Nuruddin Wiranda. Machine learning for security and security for machine learning: A literature review. In *2021 4th International Conference on Information and Communications Technology (ICOIACT)*. IEEE, 2021. doi: https:

//doi.org/10.1109/icoiact53268.2021.9563985.