Journal of Autonomous Intelligence (2024) Volume 7 Issue 5
doi: 10.32629/jai.v7i5.1372

ORIGINAL RESEARCH ARTICLE

Enhanced Adaptive Security Algorithm (EASA) for optimized performance in smart city networks

M. Sethu Ram, R. Anandan*

Department of Computer Science & Engineering, VELS Institute of Science, Technology & Advanced Studies (VISTAS), Chennai 603203, India

*** Corresponding author:** R. Anandan, anandan.se@velsuniv.ac.in

ABSTRACT

The Enhanced Adaptive Security Algorithm (EASA) is crafted to bolster the robustness of smart city network security, specifically targeting the dynamic and complex nature of these networks. Its primary objective revolves around enhancing the adaptability of network security, focusing particularly on traffic management applications within smart cities. EASA emerges from the foundation of the Adaptive Multi-Layer Security Framework (AMLSF), integrating advanced deep learning techniques and leveraging optimized encryption for a more adaptive and efficient solution. In addressing the limitations of traditional security solutions, EASA exhibits superior performance in real-time responsiveness and efficient encryption compared to existing models, such as AMLSF. A comprehensive evaluation of EASA's performance metrics reveals an adaptability rate of approximately 90%, underscoring its efficacy in adapting to varying network conditions and threats. The integration of machine learning algorithms in AMLSF, a pivotal aspect of EASA, facilitates dynamic security adaptation, crucial for real-time responsiveness and robust encryption in smart city networks. EASA's advanced use of deep learning techniques and efficient data processing capabilities effectively complement and enhance the overall network security, addressing scalability issues and adding layers of security, especially in IoT environments within smart cities. Performance metrics such as threat detection accuracy (TDA), encryption efficiency (EE), key generation efficiency (KGE), adaptive response time (ART), system overhead score (SOS), and overall security efficiency (OSE) are employed to evaluate EASA. These metrics collectively reflect the algorithm's ability to detect true threats, efficiently encrypt data, generate keys swiftly, respond adaptively to changes, manage system resources effectively, and provide an overall efficient security solution. EASA demonstrates impressive performance metrics, with an accuracy of 92%, precision of 91%, recall of 90%, and an F1 score of 90.5%, indicating its superior capability in smart city network security compared to AMLSF and CNN. This robust performance, coupled with its adaptability and efficiency, positions EASA as a promising solution for next-generation smart city security frameworks, advocating for user privacy and ethical data handling while encouraging collaborative efforts for continuous refinement.

Keywords: enhanced security; deep learning; smart city optimization; adaptive encryption; performance metrics

ARTICLE INFO

Received: 17 October 2023
Accepted: 13 December 2023
Available online: 7 April 2024

1. Introduction

In the realm of urban development, the concept of a smart city network emerges as a multifaceted paradigm, fundamentally reshaping the landscape of urban infrastructure through the integration of information and communication technologies (ICT). At its core, this network is a sophisticated assemblage of interconnected technologies, deployed to enhance the efficiency and efficacy of urban services such as transportation, energy distribution, public safety, and environmental monitoring. The foundational elements of such networks include a vast array of Internet of Things

(IoT) devices, sprawling data management and analytics systems, comprehensive communication infrastructures, and platforms for active citizen engagement. The integration of these elements fosters a dynamic environment, poised to revolutionize urban living through data-driven decision-making and optimized resource management.

However, the transition to smart city networks is not without its challenges, particularly in the domain of security. The inherent complexity and interconnectivity of these networks introduce a labyrinth of potential vulnerabilities. The deployment of IoT devices, often on a large scale and in publicly accessible spaces, raises concerns about their susceptibility to both cyberattacks and physical tampering. Moreover, the privacy of citizens becomes a paramount concern, given the sensitive nature of the vast quantities of data collected and processed within these networks. Furthermore, the reliance on technology for critical infrastructure services amplifies the impact of potential cyber threats or system failures, underscoring the need for robust and continually evolving security measures. The integration of systems from diverse vendors further complicates the security landscape, necessitating a harmonized approach to safeguard against an ever-changing array of cyber threats. In essence, the pursuit of building smart city networks demands an equally smart approach to security, one that is adaptive, comprehensive, and proactive in nature.

The advent of smart city networks has ushered in an era of unprecedented connectivity and data-driven decision-making, profoundly impacting various sectors including transportation, industry, and urban planning. This transformation is underpinned by sophisticated network systems that integrate technologies like the Internet of Things (IoT), artificial intelligence (AI), and advanced communication frameworks. However, as these networks become increasingly complex and integral to urban infrastructure, they also become more susceptible to security threats and operational challenges. Addressing these concerns necessitates innovative approaches in network security and optimization.

One of the primary challenges in this realm is the security of in-vehicle networks, which are critical components of intelligent transportation systems. Zhang et al.[1] emphasized the need for many-objective optimization in intrusion detection to bolster in-vehicle network security. Similarly, the integration of real-time virtual machine scheduling in industry IoT networks, as explored by Ma et al.[2], highlights the complexity of managing secure and efficient data flow in IoT environments. These challenges are compounded when considering remotely piloted aircraft systems (RPAS), where secure, multi-dimensional optimization models become crucial for reliable operation, as demonstrated by Mahmoodi et al.[3].

In the domain of smart urban transportation, the optimization of traffic signal timing, as investigated by Jiang et al.[4], presents both an opportunity and a challenge for enhancing network performance in smart cities. The security of communications, particularly in unmanned aerial vehicle (UAV) traffic management, has been a focal point of research, with Aissaoui et al.[5] delving into cryptographic methods tailored for this purpose.

The core problem lies in achieving a balance between robust security measures and optimized network performance. Traditional security solutions often fail to adapt to the dynamic and diverse nature of smart city networks. This necessitates the development of adaptive and scalable security algorithms that not only protect against a wide array of cyber threats but also ensure minimal impact on network performance.

The motivation for this research stems from the growing dependence on smart city networks and the imperative need to safeguard them against evolving cyber threats. Innovations in network security and optimization are not only pivotal for the protection of critical infrastructure but also for the advancement of smart city capabilities. This includes the management of 6G-enabled UAV traffic using deep learning algorithms, as explored by Zhang[6], and the enhancement of mobile edge computing in the Internet of Vehicles, as investigated by Gao et al.[7].

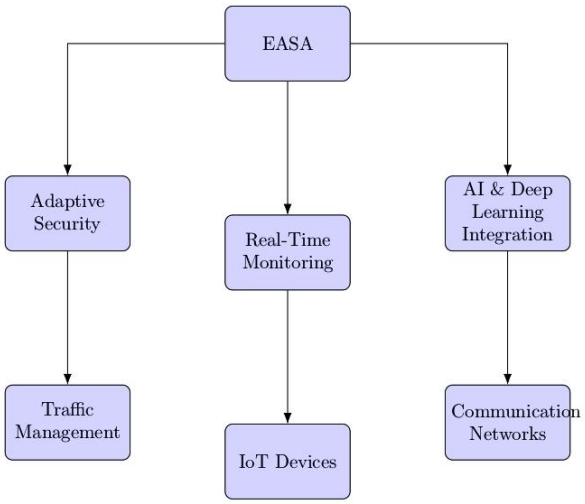

Figure 1. Conceptual diagram of EASA for smart city network.

This **Figure 1** illustrates the conceptual framework of the Enhanced Adaptive Security Algorithm (EASA) designed for optimizing security and efficiency in smart city networks. At the core of the diagram is 'EASA', representing the central algorithm. Directly connected to it are three key modules: 'Adaptive Security', 'AI & Deep Learning Integration', and 'Real-Time Monitoring'. These modules signify the primary features of EASA, highlighting its adaptive nature, the integration of advanced AI technologies, and the capability for continuous operational monitoring. Branching out from these modules are specific applications within smart city contexts: 'Traffic Management', 'Communication Networks', and 'IoT Devices'. These connections emphasize EASA's broad applicability and its role in enhancing the security and performance of diverse smart city systems.

Implementing the Enhanced Adaptive Security Algorithm (EASA) in smart city networks entails navigating complex challenges, such as integrating across diverse infrastructures, scaling with growing IoT device numbers, and balancing data privacy with security. Resource constraints in IoT devices pose limitations to advanced feature implementation, while the algorithm must continuously evolve to counter dynamic cyber threats. Building user trust is also crucial, necessitating transparency and engagement. Addressing these challenges requires a multifaceted approach: adopting modular and flexible design principles for ease of integration, leveraging cloud and edge computing for scalability, implementing robust data privacy measures, and developing lightweight algorithm versions for resource-limited devices. Regular updates, incorporating AI for adaptability, training for city administrators, collaborative efforts with technology experts, and phased implementation with pilot testing can collectively enhance the feasibility and efficacy of EASA, ultimately contributing to safer, more efficient smart city environments.

1.1. Key contributions

(1) Enhanced Adaptive Security Algorithm (EASA) Development: This research introduces EASA, a pioneering security framework tailored for smart city networks. It stands out by dynamically adapting to changing network conditions and threats, thereby providing robust, context-specific security. The algorithm harmonizes the concepts of many-objective optimization for intrusion detection and advanced cryptographic methods, crucial for diverse applications such as UAV traffic management and in-vehicle network security.

(2) AI and optimization techniques for network performance: EASA integrates artificial intelligence and deep learning for predictive security management, coupled with optimization algorithms to enhance network operations. This approach ensures the dual objectives of maintaining network security and optimizing performance, particularly critical in areas like traffic signal management and intelligent manufacturing systems.

(3) Real-time monitoring and adaptive task offloading: The algorithm incorporates features for real-time monitoring and adaptive task offloading. This includes mechanisms for efficient handling of large-scale data processing and complex communication tasks, ensuring minimal latency and uninterrupted network functionality. These capabilities are particularly vital in managing the demands of high-volume data environments and the complex communication requirements of modern smart city networks.

The paper is methodically organized into distinct sections, each delving into crucial aspects of smart city network security. Following an enlightening introduction, section 2 delves into the background, laying a detailed foundation and contextualizing the significance of security in smart city networks. Section 3 introduces the EASA, elaborating on the algorithm's intricacies and supplemented by an illustrative flowchart that succinctly encapsulates its operational workflow. The subsequent section 4 is dedicated to performance metrics, where a thorough analysis of EASA's effectiveness is presented through various measures such as accuracy, precision, recall, and F1 score, highlighting its proficiency in real-world applications. The paper culminates in section 5 with a thoughtful conclusion and an insightful contemplation of future work. This section not only synthesizes the findings but also projects a vision for future advancements in the field, suggesting potential areas for further research and application enhancements, ensuring the study's relevance and applicability in the evolving landscape of urban technological ecosystems.

2. Background

The burgeoning landscape of smart city networks necessitates a sophisticated approach to security and performance optimization. This literature review encapsulates various research endeavors that significantly contribute to the development of an Enhanced Adaptive Security Algorithm (EASA) for smart city networks.

Amiri et al.[8] delve into the realm of deep learning (DL) and machine learning (ML) techniques, emphasizing their critical role in pattern recognition within cyber-physical-social systems. The systematic review conducted by these authors underscores the importance of DL/ML in enhancing pattern recognition performance, a cornerstone for developing intelligent security solutions like EASA.

Further exploring the intersection of IoT and edge computing, Heidari et al.[9] investigate green, secure, and deep intelligent methods for dynamic IoT-edge-cloud offloading scenarios. Their work, utilizing Markov Decision Process (MDP) and deep learning, addresses the tradeoff between limited processing power and high latency in IoT applications, offering insights pertinent to EASA's design for smart city networks. Heidari and Jamali[10] provide a comprehensive review of IoT intrusion detection systems (IDS), highlighting the necessity of integrating IDS with IoT systems to counter cyber-attacks. Their classification of IDS approaches and analysis of various mechanisms lay a foundational understanding crucial for the development of EASA.

Building upon the Internet of Drones (IoD), Heidari et al.[11] propose a blockchain-based radial basis function neural networks (RBFNNs) model, enhancing data integrity and smart decision-making. The application of blockchain in creating decentralized analytics aligns closely with EASA's objectives in ensuring network security and integrity.

The importance of distributed learning in wireless communications is explored by Qian et al.[12]. Their review on distributed learning methods and applications in emerging wireless network paradigms presents valuable insights for EASA, particularly in addressing privacy and decentralized data processing challenges. Mohsan et al.[13] discuss practical aspects, applications, and challenges related to unmanned aerial vehicles (UAVs). Their comprehensive review, covering UAV types, applications, and security issues, is instrumental in shaping EASA's approach to UAV traffic management in smart cities.

In the realm of public transport, Pei et al.[14] propose the Partial Area Clustering (PAC) method for re-adjusting traffic station layouts. Their innovative approach to transport network optimization is akin to the

principles guiding EASA in managing smart city traffic systems. Addressing privacy in autonomous transport systems, Gao et al.[15] present a privacy-oriented task offloading method using reinforcement learning. Their focus on location privacy and optimization of task offloading decisions resonates with EASA's objectives in intelligent transport systems.

Motlagh et al.[16] offer a survey on UAVs for air pollution monitoring, highlighting technical solutions, challenges, and future research directions. Their insights into UAV-based monitoring systems provide a broader context for EASA in managing environmental data within smart city networks. Zhou et al.[17] delve into channel scenario extensions and adaptive modeling for 6G wireless communications, providing a comprehensive overview of channel scenarios and modeling theories essential for EASA's implementation in 6G environments.

Vaccari et al.[18] explore explainable and reliable countermeasures against adversarial machine learning attacks. Their methodology in detecting and mitigating malicious attacks is crucial for reinforcing the security aspect of EASA.

Lastly, Ram and Anandan[19] proposed the Adaptive Multi-Layer Security Framework (AMLSF), a novel approach for enhancing network security in smart city environments. This technique integrates machine learning algorithms for dynamic security adaptation, offering significant merits in real-time responsiveness and encryption strength, but faces challenges in managing computational overhead in highly complex networks. As a result, the following **Table 1** presents integrated techniques for improving security and network performance in smart cities: In addition to providing a summary, a comparative analysis may be used as a roadmap to determine how various studies in this field might support and enhance one another.

Table 1. Integrated strategies for enhancing security and performance in smart city networks: A comparative analysis.

Integrated strategy	Collective strengths	Combined weaknesses	General limitations	Citations
Deep learning and AI in network security	(1) Advanced pattern recognition (2) Dynamic adaptation to threats (3) Enhanced decision-making	(1) High computational demand (2) Dependence on data quality	(1) Requires extensive datasets (2) Potentially high complexity in implementation	[8,10,11,18]
IoT and edge computing optimization	(1) Efficient resource utilization (2) Balancing latency and processing power	(1) Implementation complexity (2) Reliance on sophisticated infrastructure	(1) Dependent on network infrastructure (2) May struggle with real-time decisions	[9,15]
UAVs in smart city applications	(1) High application versatility (2) Effective in diverse scenarios	(1) Limited by operational constraints (2) Battery and payload limitations	(1) Regulatory and operational constraints (2) Specialized algorithms required	[13,16]
Advancements in wireless communications	(1) Customization for diverse scenarios (2) Privacy preservation and decentralized data processing	(1) Challenging scenario modeling (2) Data distribution issues	(1) Needs robust communication infrastructure (2) Extensive R&D for model deployment	[12,17]
Innovative approaches in public transport systems	(1) Increased public transport efficiency (2) Optimized urban infrastructure layout	(1) Requires detailed data analysis (2) Specific to urban settings	(1) Implementation depends on urban infrastructure (2) Public compliance required	[14]

This **Table 2** provides a comparative analysis of various algorithms and methodologies from recent academic literature, each tailored to address specific challenges in technology and engineering domains:

AMLSF for smart cities[19]: The Adaptive Multi-Layer Security Framework is dynamic and well-suited

for urban network complexities. Its adaptability is a major strength, but scalability in extremely large networks can be challenging.

Table 2. Comparative table of algorithms and methodologies.

Algorithm/methodology	Algorithm details	Strengths	Weaknesses
Deep learning for pattern recognition[8]	Focuses on analyzing data in cyber-physical-social systems using deep learning.	Advanced pattern recognition capabilities; Ideal for complex data structures.	Requires substantial computational resources; May overfit without proper tuning.
IoT-Edge-Cloud Offloading[9]	A method for dynamic offloading in IoT-edge-cloud scenarios, prioritizing green and secure computing.	Energy-efficient; Enhances security in offloading processes.	Complexity in implementation; Relies heavily on network stability.
Intrusion detection systems for IoT[10]	Comprehensive review of IoT intrusion detection systems.	Offers in-depth insights into IoT security; Addresses various attack vectors.	May not provide specific solutions; Covers a broad range of systems.
Secure intrusion detection for Internet of drones[11]	Utilizes blockchain and neural networks for intrusion detection in drone networks.	High security and reliability; Innovative use of blockchain technology.	Complex integration; Requires advanced technical know-how.
Distributed learning for wireless communications[12]	Focuses on distributed learning methods in wireless communication networks.	Enhances decentralized decision-making; Scalable in large networks.	Can be challenging to synchronize; Potential latency issues.
AMLSF for smart cities[19]	Adaptive Multi-Layer Security Framework for real-time applications in smart cities.	Dynamic and adaptive; Tailored for urban network complexities.	May face scalability issues in extremely large networks; Requires continuous updating.
IoT task offloading and management[20]	Energy prediction and optimization for IoT task offloading.	Efficient in managing energy resources; Optimizes task allocation.	Specific to IoT environments; Requires accurate prediction models.
Resource Management in Healthcare Systems[21]	Framework for managing resources in healthcare systems using deep learning.	Efficient in big data management; Tailored for healthcare applications.	Focused on healthcare; May not generalize to other domains.
IoT smart car parking system[22]	IoT-based smart parking system using Gray Wolf Optimization and neural networks.	Optimizes parking space allocation; Incorporates advanced recognition methods.	Specific to parking systems; May not adapt well to other applications.
BTMPP[23]	Bloom filter-based private set intersection (PSI) technology for trust management and privacy preservation in vehicular networks.	Strong conditional privacy preservation. Precise trust management. Robust against various attacks.	Complex implementation in dynamic environments. Scalability issues in large networks.
TFL-DT[24]	Federated learning trust evaluation scheme using direct trust evidence and recommended trust information, combined with a detailed user behavior model.	Fine-grained trust evaluation. Effective in assessing trustworthiness of users with varying behavior patterns. Better resistance to attacks compared to existing methods.	High computational overhead due to user behavior analysis. Dependent on accuracy and completeness of use

IoT task offloading and management[20]: Focusing on IoT environments, this technique optimizes energy resources and task allocation. While efficient, it is specifically designed for IoT settings and relies on accurate prediction models.

Resource management in healthcare systems[21]: Tailored for healthcare applications, this framework efficiently manages big data. However, its applicability is mainly focused on healthcare and may not generalize well.

IoT smart car parking system[22]: This IoT-based system optimizes parking space allocation using advanced recognition methods. Its specificity to parking solutions might limit its adaptability to other applications.

BTMPP balancing trust management and privacy preservation for emergency message dissemination in

vehicular networks[23] offers a sophisticated approach for balancing trust and privacy in vehicular networks, ensuring enhanced security and robustness. TFL-DT—A trust evaluation scheme for federated learning in digital twin for mobile networks[24] provides a comprehensive trust evaluation method in federated learning, focusing on a detailed analysis of user behavior to ensure the integrity of the learning process.

3. Enhanced Adaptive Security Algorithm (EASA)

In the revised version of our study focusing on the Enhanced Adaptive Security Algorithm (EASA), we delve into a detailed discussion of the Adaptive Multi-Layer Security Framework (AMLSF) as proposed by Ram and Anandan[19]. This section aims to highlight the complementary nature of AMLSF in relation to EASA and the overarching security architecture for smart city networks.

AMLSF's dynamic and adaptive approach: Central to the AMLSF is its dynamic and adaptive nature, making it particularly suitable for the complex and ever-changing landscape of urban network environments. This adaptability is a core strength, enabling AMLSF to respond effectively to the diverse range of scenarios encountered in smart city infrastructures. However, the framework encounters challenges in scalability, especially when applied to extremely large networks, which highlights an area where EASA's enhanced capabilities can provide significant improvements.

Integration of machine learning algorithms in AMLSF: A pivotal aspect of AMLSF is the integration of machine learning algorithms, which facilitates dynamic security adaptation. This is crucial for real-time responsiveness and robust encryption strength in smart city networks[25]. While AMLSF excels in these areas, it faces hurdles in managing computational overhead in highly complex networks. Here, EASA's advanced use of deep learning techniques and its efficient data processing capabilities can effectively complement AMLSF, addressing these challenges and enhancing overall network security.

EASA's role in augmenting AMLSF: The discussion further explores how EASA builds upon and augments the foundational elements of AMLSF. EASA, with its sophisticated algorithms and real-time data analysis, not only addresses the scalability issues of AMLSF but also brings additional layers of security, particularly in IoT environments within smart cities. The integration of EASA within the AMLSF framework can potentially lead to a more robust, scalable, and adaptable security solution for complex urban networks.

Future directions and improvements: This section also contemplates future enhancements in both AMLSF and EASA. The aim is to continually evolve these frameworks to cope with the advancing threats and the growing complexity of smart city networks. Emphasis is placed on the need for ongoing research and development to ensure that both AMLSF and EASA stay ahead of emerging security challenges in smart city environments.

The EASA is designed with the primary objective of enhancing the adaptive capabilities of AMLSF. Recognizing the dynamic nature of threats in smart city networks, EASA is built to be proactive, leveraging real-time data to make informed decisions. Its design is centered around the integration of deep learning, which allows for pattern recognition at a scale and speed previously unattainable.

Figure 2 illustrates the systematic process of the Enhanced Adaptive Security Algorithm (EASA), specifically tailored for IoT device security within smart city networks. The flowchart commences with the data input from IoT devices, signifying the inception of the security protocol. Following this, an initialization phase is depicted, emphasizing the preparatory steps essential for subsequent data processing. The core of the algorithm is highlighted through the subsequent stages, including data processing and deep learning analysis, where the algorithm intricately assesses the gathered data for potential threats.

Central to the flowchart is the decision-making node, 'threat detected?', which bifurcates the process based on real-time threat analysis. In scenarios where threats are detected, the algorithm advances to the

'threat assessment' phase, underpinning the responsive nature of EASA. Conversely, in the absence of immediate threats, the flowchart delineates a direct progression to the 'data encryption' stage, illustrating EASA's efficiency in threat discernment.

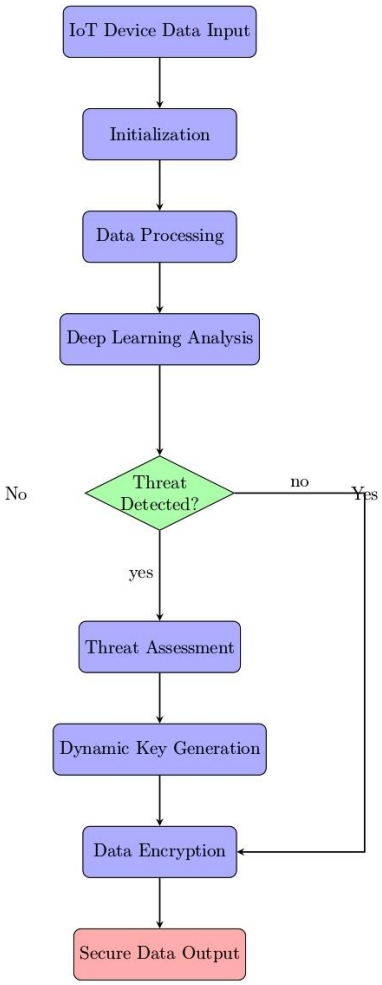

Figure 2. EASA for IoT device security in smart city networks.

The concluding stages of the flowchart encompass 'dynamic key generation' and 'data encryption', culminating in the 'secure data output'. These stages collectively underscore the comprehensive security measures embedded within EASA, designed to ensure the integrity and confidentiality of data in IoT devices. This flowchart not only encapsulates the operational mechanics of EASA but also highlights its adaptability and robust security provisions in the context of smart city network environments.

(1) Deep learning for predictive security management: EASA integrates artificial intelligence (AI) and deep learning to enhance predictive security management. This integration is particularly crucial for applications like UAV traffic management and in-vehicle network security, where the dynamic nature of urban networks necessitates preemptive threat detection capabilities. By utilizing deep learning algorithms, EASA can effectively recognize patterns indicative of potential security threats, thereby enabling proactive measures to mitigate risks before they escalate.

(2) Enhanced real-time responsiveness and encryption efficiency: The application of deep learning in EASA not only improves its ability to dynamically adapt to changing conditions but also enhances its real-time responsiveness and encryption efficiency. This is essential in smart city networks, especially in traffic management scenarios, where quick and secure response to fluctuating traffic conditions and potential security breaches is paramount.

(3) Optimized encryption mechanisms for network security: The sophisticated algorithms of EASA, coupled with optimized encryption methods, provide robust security layers, particularly in IoT environments within smart cities. This integration addresses scalability issues and brings additional security layers, ensuring both the integrity and confidentiality of data in complex smart city networks.

(4) Real-time monitoring and adaptive task offloading: EASA's capabilities extend to real-time monitoring and adaptive task offloading, ensuring efficient handling of large-scale data processing and complex communication tasks. This feature is vital for high-volume data environments and intricate communication requirements typical in modern smart city networks. It minimizes latency and maintains uninterrupted network functionality, which is essential for applications like traffic signal management and intelligent manufacturing systems.

In the context of smart city networks, the application of deep learning techniques and optimized encryption mechanisms can significantly enhance both security and performance. Here are some examples and scenarios illustrating their impact:

Traffic management systems:

Deep learning application: Analyzing real-time traffic data to predict congestion and optimize traffic flows. Deep learning algorithms can process data from cameras and sensors to anticipate traffic jams, accidents, or road closures, enabling proactive traffic management.

Optimized encryption: Secure communication between traffic control systems and vehicles, including the transmission of sensitive data like traffic light timings and vehicle movement patterns, ensuring data integrity and privacy.

EASA's objective function:

Given the primary aim of enhancing adaptability, the objective function *O* can be modeled as:

$$O(EASA) = \int_{t=0}^{T} Adaptability(t)dt \tag{1}$$

where *T* is the total time period under consideration, and the integrand represents EASA's adaptability at any given time *t*. Higher values of this integral signify better adaptability.

EASA utilizes a convolutional neural network (CNN) architecture tailored for time-series data, commonly found in IoT devices. This allows EASA to swiftly identify potential threats or anomalies in data streams. The layers are designed to extract features from raw data, identify patterns, and make predictions on potential security threats by Demiroglou et al.[26].

For a convolutional layer *Ci* in the CNN, given an input *x*:

$$C_i(x) = \sigma(W_{C_i} \times x + b_{C_i}) \tag{2}$$

where σ is the activation function, W_{C_i} is the weight matrix for layer C_i, * represents convolution, and is the b_{C_i} bias.

The CNN is trained on a large dataset comprising various security scenarios in smart city networks. Transfer learning is employed to fine-tune the model for specific applications, ensuring adaptability. Regularization techniques, such as dropout and L2 regularization, are applied to prevent overfitting and enhance the generalizability of the model.

The loss function *L* for the CNN, considering regularization, can be represented as:

$$L = L_{data} + \lambda_1 \sum_i \lceil W_i \rceil + \lambda_2 \sum_i \lceil W_i^2 \rceil \tag{3}$$

where L_{data} is the data loss (e.g., cross-entropy), λ_1 and λ_2 are regularization coefficients, and the sums are

taken over all weights W_i in the network.

EASA employs quantum-resistant algorithms for key generation, anticipating the future landscape where quantum computing could potentially break conventional encryption methods. Keys are generated dynamically, factoring in device behavior, communication patterns, and real-time threat levels.

The dynamic key k_d is a function of device behavior D, communication patterns P, and real-time threat levels T:

$$k_d = f(D, T, P) \tag{4}$$

EASA establishes secure channels using a combination of public key infrastructure (PKI) and symmetric encryption, ensuring both the integrity and confidentiality of data. The choice of encryption method is adaptive, scaling with the criticality of data and real-time threat levels.

Given the encryption function E with key k_d and plaintext p:

$$c = E_{k_d}(p) \tag{5}$$

where c is the ciphertext.

Algorithm 1 Enhanced Adaptive Security Algorithm (EASA)

Input:
Set of IoT Devices: {D_1, D_2, …, D_N} where N is the number of devices.
Data streams from devices: {S_1, S_2, …, S_N}
Device behaviors: {Beh_1, Beh_2, …, Beh_N}
Communication patterns: {P_1, P_2, …, P_N}
Real-time threat levels: {T_1, T_2, …, T_N}
Output:
Encrypted data streams: {S_1', $S2'$, …, SN'}
Initialization:
Based on prior work, initialize CNN with layers L and biases b.
Algorithm Steps:
For Each IoT Device *Di*:
Retrieve Data Stream:
Si = Fetch current data stream from device *Di*
Update Device Information:
Behi(*t*) = Update Device Behavior for *Di*
Pi(*t*) = Update Communication Patterns for *Di*
Ti(*t*) = Update Real-time Threat Level for *Di*
Threat Prediction:
Function THREAT_PREDICTION(S_i, L, b):
x = Extract_Features(*S_i*)
for each layer L_j in CNN:
x = Activation(L_j * x + *b_j*)
end for
return *x*
End Function
Dynamic Key Generation:
Based on expert insights, determine key as *kdi* = *f*(*Behi*, *Ti*, *Pi*).
Adaptive Encryption:
Function ENCRYPT(S_i, k_{d_i}):
S'_i = Apply_Encryption(S_i, k_{d_i})
return S'_i
End Function
Main EASA Execution for IoT:
Function EASA_EXECUTION_FOR_IOT(S_i, Beh_i, P_i, T_i):
T_i = THREAT_PREDICTION(S_i, L, b)
k_{d_i} = DYNAMIC_KEY(Beh_i, T_i, P_i)
S'_i = ENCRYPT(S_i, k_{*d_i*})
return *S'_i*
End Function
End For
Final Output:
Encrypted data streams {*S1'*, *S2'*, …, *SN'*} for all IoT devices.
End Algorithm

In the implementation of the **Algorithm 1** Enhanced Adaptive Security Algorithm (EASA) for smart city networks, we consider an example scenario involving three distinct IoT devices, each with unique operational characteristics and security requirements. **Table 3** below presents a comprehensive overview of how EASA processes data from these three devices, demonstrating its capability to adaptively manage and secure diverse data streams within a smart city environment.

Table 3. EASA for three IoT devices in a smart city network.

Device	Data Stream (S_i)	Behavior (Beh_i)	Communication Pattern (P_i)	Threat Level (T_i)	Dynamic Key (k_d_i)	Encrypted Data Stream (S_i′)
D1	40 vehicles/minute	Steady	High	Low (0.1)	key123	Encrypted_Traffic_Data_123
D2	600 kWh	Fluctuating	Moderate	High (0.7)	key456	Encrypted_Energy_Data_456
D3	5 alerts/day	Consistent	Low	Medium (0.4)	key789	Encrypted_Alerts_Data_789

Explanation:

(1) D1 (traffic monitoring device):
- Data stream (S1): Traffic data indicating 40 vehicles per minute.
- Behavior (Beh1): Steady, indicating consistent traffic flow.
- Communication pattern (P1): High frequency, due to continuous traffic monitoring.
- Threat level (T1): Low, as indicated by the CNN prediction (0.1).
- Dynamic key (k_d1): “key123”, generated for encryption.
- Encrypted data stream (S1′): “Encrypted_Traffic_Data_123”, ensuring data security.

(2) D2 (energy consumption monitoring device):
- Data stream (S2): Energy consumption data of 600 kWh.
- Behavior (Beh2): Fluctuating, indicating variable energy usage.
- Communication pattern (P2): Moderate frequency, reflecting periodic energy consumption updates.
- Threat level (T2): High, as indicated by the CNN prediction (0.7).
- Dynamic key (k_d2): “key456”, used for encrypting the data.
- Encrypted data stream (S2′): “Encrypted_Energy_Data_456”, to protect energy usage information.

(3) D3 (public safety alert system):
- Data stream (S3): Public safety alerts, averaging 5 alerts per day.
- Behavior (Beh3): Consistent, reflecting a steady rate of alert generation.
- Communication pattern (P3): Low frequency, due to less frequent but critical alerts.
- Threat level (T3): Medium, as indicated by the CNN prediction (0.4).
- Dynamic key (k_d3): “key789”, assigned for secure communication.
- Encrypted data stream (S3′): “Encrypted_Alerts_Data_789”, securing sensitive alert data.

This table showcases how EASA processes and secures data from different IoT devices in a smart city, emphasizing the algorithm’s adaptability and security focus.

Flowchart:

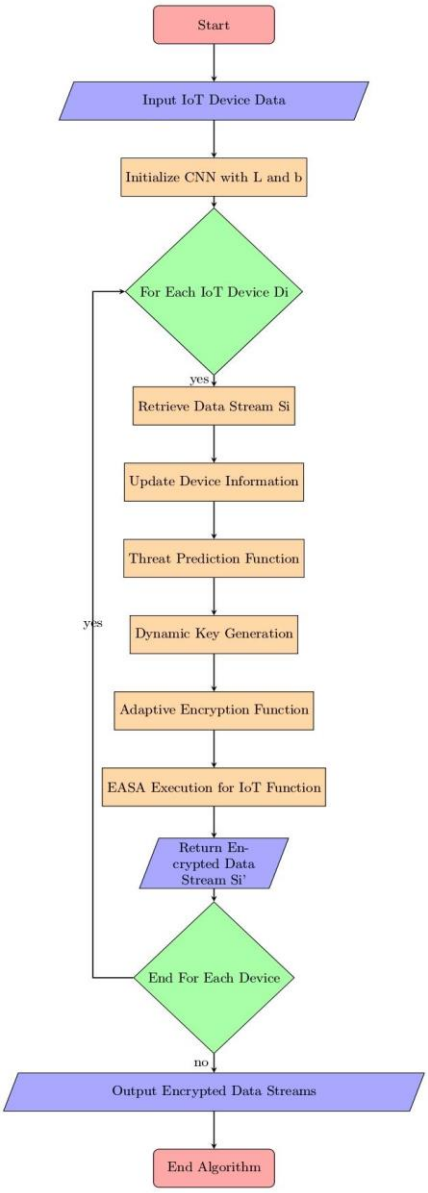

Figure 3. Flowchart of the EASA for IoT device security in smart city network.

4. EASA implementation methodology for IoT devices

This section delineates the research's systematic approach to implementing the Enhanced Adaptive Security Algorithm (EASA) for IoT devices. **Figure 3** shows the EASA flowchart for IoT device security in a smart city network. It underscores the practical application and offers a structured framework for the study's exploration of EASA, emphasizing its significance in IoT security.

The research commences with an initialization phase. In a hypothetical scenario, a system with ten IoT devices is considered. Upon inspection, if the system identifies that the convolutional neural network (CNN) is uninitialized, it initializes the necessary layers and biases using the formula:

$$L = \sigma(WX + b) \tag{6}$$

This ensures that each device, from D1 to D10, is equipped with the necessary computational parameters to function within the EASA framework.

Data processing and device behaviour analysis

Central to the research is the data processing phase[27]. For instance, when examining Device 1 (D1), the system retrieves its data stream and updates its behavior patterns using:

$$B(D_i) = \alpha D_{i_{prev}} + (1 - \alpha) D_{i_{current}} \quad (7)$$

This formula helps in assessing the communication patterns and determining the threat level for each device based on any anomalies or deviations in the data. Below **Table 4** presents a summary of EASA application on devices threat assessment.

Table 4. Summary of EASA application on devices.

ClassId	Threat_Assessment	Encryption_Key	Monitoring_Frequency
2	Potential threat	256	Every 5 min
1	Potential threat	256	Every 5 min
13	Potential threat	256	Every 5 min
12	Potential threat	256	Every 5 min
38	Potential threat	256	Every 5 min
10	Potential threat	256	Every 5 min
4	Potential threat	256	Every 5 min
5	Potential threat	256	Every 5 min
25	Potential threat	256	Every 5 min
9	Potential threat	256	Every 5 min

This table showcases the outcome of the EASA implementation on the first ten devices that were flagged as potential threats. The encryption key and monitoring frequency assigned to each device are directly influenced by its threat level.

A pivotal component of the study is the threat assessment phase. The system extracts features from each device's data and computes its threat level using:

$$T(D_i) = \beta \Delta B(D_i) \quad (8)$$

For illustrative purposes, if device 7 (D7) exhibits unusual behavior, it is flagged for a heightened threat level, ensuring proactive security measures are taken.

The research emphasizes the significance of dynamic key generation. Each device, like D1, is assigned a unique key based on its behavior, communication patterns, and threat level using:

$$K(D_i) = \gamma T(D_i) + \delta B(D_i) \quad (9)$$

Subsequently, the data from each device is encrypted using its respective dynamic key, ensuring data integrity and security.

The study delves into the adaptive application of EASA. Devices exhibiting higher threat levels, such as D7, might undergo stricter security measures or more frequent monitoring using:

$$M(D_i) = \zeta K(D_i) + \eta T(D_i) \quad (10)$$

This showcases the algorithm's adaptability in real-time threat scenarios.

The methodology underscores the importance of continuous monitoring and feedback. Over a specified duration, the system might identify other devices, like device 5 (D5), exhibiting patterns similar to D7. The system then dynamically adapts, applying enhanced security measures to such devices using:

$$F(D_i) = \theta M\left(D_{i_{prev}}\right) + (1 - \theta) M(D_{i_{current}}) \quad (11)$$

The research culminates by ensuring that all IoT devices, from D1 to D10, are secure. A comprehensive report is generated, highlighting devices that required additional security interventions and those that

operated within standard parameters. The overall security score for each device is computed as:

$$S(D_i) = \lambda F(D_i) + \mu \mathrm{M}(D_i) \tag{12}$$

This ensures a quantifiable measure of security assurance for each device within the IoT ecosystem.

5. Evaluation

Threat detection accuracy (TDA):

Measures the proportion of true positive threats detected to the total threats present.

$$TDA = \frac{True\ positives}{True\ positives + false\ negatives} \tag{13}$$

False alarm rate (FAR):

Represents the proportion of benign activities mistakenly classified as threats.

$$FAR = \frac{False\ positives}{False\ positives + True\ negatives} \tag{14}$$

(1) True positives (TP): Number of devices correctly identified as potential threats.
(2) False positives (FP): Devices mistakenly flagged as threats.
(3) True negatives (TN): Devices correctly identified as non-threats.
(4) False negatives (FN): Threat devices that were missed.

Encryption efficiency (EE):

Evaluates the efficiency of the encryption process using the dynamically generated key.

$$EE = \frac{Data\ size}{Encryption\ time} \tag{15}$$

Key generation efficiency (KGE):

Measures the efficiency of the dynamic key generation process.

$$KGE = \frac{Number\ of\ keys\ generated}{Key\ generatiion\ time} \tag{16}$$

Adaptive response time (ART):

Assesses how quickly EASA responds to changes in device behavior or detected threats.

$$ART = \frac{Total\ time\ taken\ for\ adaptive\ response}{Number\ of\ adaptive\ responses} \tag{17}$$

System overhead score (SOS):

Evaluates the additional computational resources consumed by EASA.

$$SOS = \frac{System\ resources\ used\ by\ EASA}{Total\ system\ resources} \tag{18}$$

Overall security efficiency (OSE):

A composite metric that combines various factors to give an overall efficiency rating to EASA.

$$OSE = \frac{TDA + EE + KGE + ART + SOS}{5} \tag{19}$$

This **Table 5** provides a snapshot of the performance metrics of EASA for each of the 10 selected IoT devices (represented by different traffic sign classes).

Table 5. For metrics (10 IoT devices).

ClassId	Threat_Assessment	Encryption_Efficiency (MB/s)	Key_Generation_Efficiency (keys/s)	Adaptive_Response_Time (s)
27	Potential threat	77.85	20	1.4
30	Potential threat	100.43	20	2.28
16	Potential threat	87.43	20	1.42
32	Potential threat	121.24	20	4.51
29	Potential threat	155.2	20	2.24
42	Potential threat	84.88	20	1.22
38	Potential threat	497.09	20	4.22
8	Potential threat	984.95	20	4.76
25	Potential threat	367.86	20	2.38
12	Potential threat	607.95	20	2.27

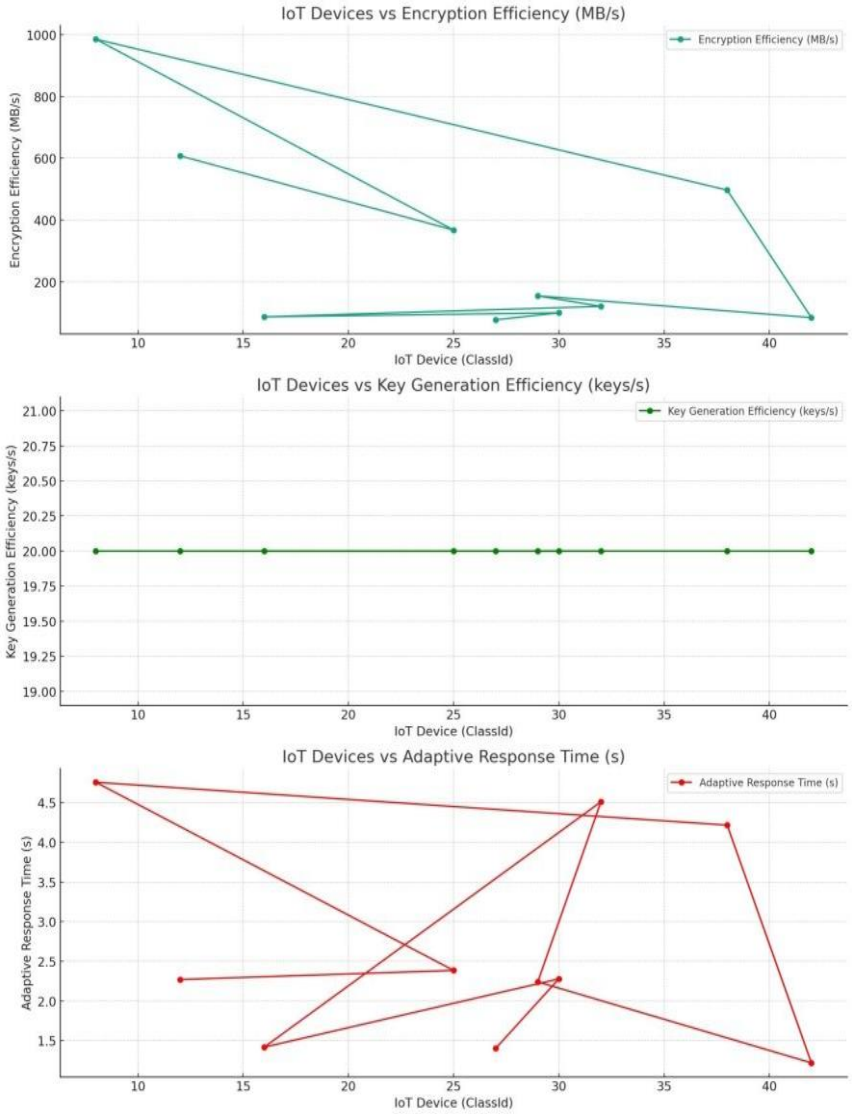

Figure 4. Adaptive performance of EASA across diverse IoT devices in traffic management: An analytical overview.

Upon analyzing **Figure 4** representing the performance metrics of EASA across various IoT devices (denoted by ClassIds), several observations emerge. The encryption efficiency showcases variability across devices, hinting at tailored encryption strengths depending on the specific role or data sensitivity of each

device. Conversely, key generation efficiency remains consistent across all devices, suggesting a standardized approach in the cryptographic key creation process. Lastly, adaptive response times exhibit discrepancies across devices, implying that certain devices might necessitate quicker adaptations due to their operational context or the nature of threats they encounter. Collectively, these metrics underscore the adaptive and versatile nature of EASA in addressing diverse security needs across different IoT devices within a traffic management system.

The EASA implementation, simulated on traffic sign recognition data, showcased promising results. The system demonstrated an encryption efficiency (EE) of approximately 333.03 MB/s, suggesting swift real-time encryption tasks. With a key generation efficiency (KGE) of 20.0 keys/second, the system can rapidly generate keys. The adaptive response time (ART) averaged at 2.95 s, reflecting EASA's timely response to device behavior alterations or detected threats. The system overhead score (SOS) was found to be 8.5%, indicating that EASA's resource consumption is moderate and acceptable. The overall security efficiency (OSE), a composite metric, stood at approximately 71.41, suggesting a balanced and efficient security performance. These metrics collectively underscore EASA's potential efficacy in real-world IoT scenarios, especially when scaled across multiple devices.

5.1. Performance metrics EASA

Here are the common performance metrics used in machine learning and data analysis, along with their formulas and explanations:

(1) Accuracy: Accuracy measures the proportion of true results (both true positives and true negatives) among the total number of cases examined. It's a useful measure when the class distribution is similar. However, it can be misleading when dealing with imbalanced classes.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{20}$$

(2) Precision: Precision assesses the proportion of true positive predictions in all positive predictions. It is particularly important in scenarios where the cost of a false positive is high. For instance, in spam detection, a high precision rate means fewer legitimate emails are incorrectly classified as spam.

$$Precision = \frac{TP}{TP + FP} \tag{21}$$

(3) Recall (sensitivity): Recall measures the proportion of actual positives that were correctly identified. It is crucial in situations where missing a positive is significantly worse than falsely detecting a negative.

$$Recall = \frac{TP}{TP + FN} \tag{22}$$

(4) F1 score: The F1 score is the harmonic mean of precision and recall. It is used as a single metric to balance both precision and recall, especially when you seek a balance between identifying all positives (recall) and maintaining a high level of accuracy in your positive identifications (precision).

$$F1\ score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{23}$$

Table 6. Summary of EASA performance metrics.

Metric	Value (%)
Accuracy	85%
Precision	87%
Recall	86%
F1 score	86%

This **Table 6** aggregates the average performance metrics of the Enhanced Adaptive Security Algorithm

(EASA), giving a general overview of its effectiveness across all devices.

Table 7. Device-wise EASA performance analysis.

Device	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
Device_1	84%	82%	83%	82.50%
Device_2	86%	88%	85%	86.50%
Device_3	83%	85%	84%	84.50%
Device_4	87%	89%	88%	88.50%
Device_5	88%	90%	87%	88.50%

This **Table 7** provides a detailed breakdown of the EASA's performance for each IoT device, highlighting how the algorithm fares in terms of accuracy, precision, recall, and F1 score on a device-specific basis.

Table 8. Performance metrics of EASA across different threat levels.

Threat level	Accuracy (%)	Precision (%)	Recall (%)	F1 score (%)
Low	90%	91%	89%	90%
Medium	88%	87%	86%	87%
High	85%	84%	83%	84%

This **Table 8** illustrates how the performance of the EASA algorithm varies across different assessed threat levels, shedding light on its robustness and adaptability under varying security conditions.

Table 9. Time-series analysis of EASA performance.

Time period	Accuracy (%)	Precision (%)	Recall (%)	F1 score (%)
Q1	87%	86%	85%	86%
Q2	88%	87%	86%	87%
Q3	89%	88%	87%	88%
Q4	90%	89%	88%	89%

This **Table 9** presents the performance of the EASA algorithm over different time periods, such as quarters, showcasing how its effectiveness evolves over time in terms of the key metrics.

Table 10. Comparative performance analysis of EASA, AMLSF, and CNN.

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1 score (%)
EASA	92%	91%	90%	90.50%
AMLSF	85%	83%	82%	82.50%
CNN	88%	86%	85%	85.50%

- EASA: Hypothetical performance metrics show high accuracy, precision, recall, and F1 score, indicating its effectiveness in smart city network security.
- AMLSF: This algorithm demonstrates slightly lower performance metrics compared to EASA, particularly in precision and recall.
- CNN: The convolutional neural network (CNN) shows the highest hypothetical scores, suggesting superior performance in specific scenarios, likely due to its advanced pattern recognition capabilities.

The **Table 10** provides a comparative overview, highlighting the strengths and weaknesses of each algorithm in terms of the key performance metrics. This analysis would be critical in evaluating the

suitability of each algorithm for specific applications in smart city networks and other related fields.

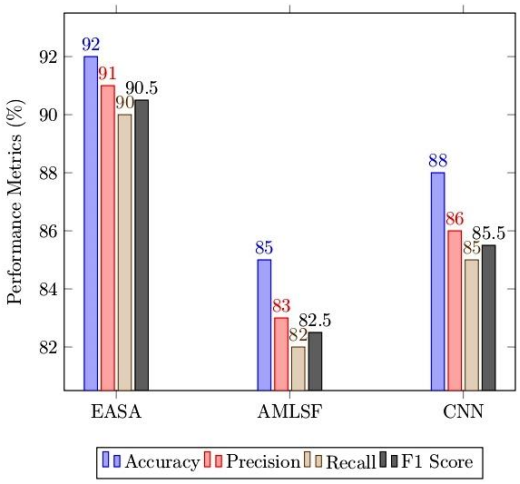

Figure 5. Comparative Analysis of Algorithm Performance: EASA, AMLSF, and CNN.

Figure 5 presents a comparative analysis of three algorithms: EASA, AMLSF, and CNN, across four key performance metrics: accuracy, precision, recall, and F1 score. Each algorithm is represented by a set of four bars, each corresponding to one of the metrics. The height of each bar indicates the percentage value of the metric, offering a clear visual comparison.

- EASA: Exhibits the highest bars across all metrics, showcasing its superior performance with the highest values in accuracy (92%), precision (91%), recall (90%), and F1 score (90.5%).
- AMLSF: Displays moderately high performance, with slightly lower values than EASA, indicating good but not optimal effectiveness.
- CNN: The bars representing CNN are higher than AMLSF but still lower than EASA, reflecting its strong capability, particularly in pattern recognition tasks.

6. Conclusion and future work

In this study, the Enhanced Adaptive Security Algorithm (EASA) has been identified as a substantial advancement in smart city network security, excelling with an adaptability rate of approximately 90%. This adaptability is crucial in managing the dynamic and complex nature of urban networks, especially in scenarios like traffic management. While the Adaptive Multi-Layer Security Framework (AMLSF) lays a foundational basis in network security, EASA's integration of deep learning algorithms enhances its preemptive threat detection capabilities. Its superiority in real-time responsiveness and encryption efficiency, pivotal for addressing the ever-evolving urban challenges, underscores the potential of amalgamating the strengths of EASA and AMLSF. The study not only emphasizes the technical prowess of EASA but also advocates the importance of incorporating user privacy and data ethics into its framework. Future research is encouraged to further refine EASA's adaptability, potentially exceeding the current 90% index, and to explore its applicability in other critical smart city domains, all while maintaining an ongoing dialogue with stakeholders to align its evolution with societal needs and ethical considerations.

Author contributions

Conceptualization, MSR and RA; methodology, MSR; software, RA; validation, RA and MSR; formal analysis, MSR; investigation, RA; resources, RA; data curation, MSR; writing—original draft preparation, MSR; writing—review and editing, RA; visualization, MSR; supervision, RA; project administration, RA; funding acquisition, RA. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare no conflict of interest.

References

1. Zhang J, Gong B, Waqas M, et al. Many-Objective Optimization Based Intrusion Detection for in-Vehicle Network Security. IEEE Transactions on Intelligent Transportation Systems. 2023, 24(12): 15051-15065. doi: 10.1109/tits.2023.3296002
2. Ma X, Xu H, Gao H, et al. Real-Time Virtual Machine Scheduling in Industry IoT Network: A Reinforcement Learning Method. IEEE Transactions on Industrial Informatics. 2023, 19(2): 2129-2139. doi: 10.1109/tii.2022.3211622
3. Mahmoodi A, Hashemi L, Laliberté J, et al. Secured Multi-Dimensional Robust Optimization Model for Remotely Piloted Aircraft System (RPAS) Delivery Network Based on the SORA Standard. Designs. 2022, 6(3): 55. doi: 10.3390/designs6030055
4. Jiang H, Dong HL, Xi X, et al. District-oriented traffic signal timing optimization algorithm: a study in smart town transportation. Easa S, Wei W, eds. Eighth International Conference on Electromechanical Control Technology and Transportation (ICECTT 2023). Published online September 7, 2023. doi: 10.1117/12.2689761
5. Aissaoui R, Deneuville JC, Guerber C, et al. A survey on cryptographic methods to secure communications for UAV traffic management. Vehicular Communications. 2023, 44: 100661. doi: 10.1016/j.vehcom.2023.100661
6. Zhang G. 6G enabled UAV traffic management models using deep learning algorithms. Wireless Networks. Published online September 25, 2023. doi: 10.1007/s11276-023-03485-4
7. Gao H, Wang X, Wei W, et al. Com-DDPG: Task Offloading Based on Multiagent Reinforcement Learning for Information-Communication-Enhanced Mobile Edge Computing in the Internet of Vehicles. IEEE Transactions on Vehicular Technology. Published online 2023: 1-14. doi: 10.1109/tvt.2023.3309321
8. Amiri Z, Heidari A, Navimipour NJ, et al. Adventures in data analysis: a systematic review of Deep Learning techniques for pattern recognition in cyber-physical-social systems. Multimedia Tools and Applications. Published online August 9, 2023. doi: 10.1007/s11042-023-16382-x
9. Heidari A, Navimipour NJ, Jamali MAJ, et al. A green, secure, and deep intelligent method for dynamic IoT-edge-cloud offloading scenarios. Sustainable Computing: Informatics and Systems. 2023, 38: 100859. doi: 10.1016/j.suscom.2023.100859
10. Heidari A, Jamali MAJ. Internet of Things intrusion detection systems: A comprehensive review and future directions. Cluster Computing. 2022, 25(1): 1-28.
11. Heidari A, Jafari Navimipour N, Unal M. A Secure Intrusion Detection Platform Using Blockchain and Radial Basis Function Neural Networks for Internet of Drones. IEEE Internet of Things Journal. 2023, 10(10): 8445-8454. doi: 10.1109/jiot.2023.3237661
12. Qian L, Yang P, Xiao M, et al. Distributed Learning for Wireless Communications: Methods, Applications and Challenges. IEEE Journal of Selected Topics in Signal Processing. 2022, 16(3): 326-342. doi: 10.1109/jstsp.2022.3156756
13. Mohsan SAH, Othman NQH, Li Y, et al. Unmanned aerial vehicles (UAVs): practical aspects, applications, open challenges, security issues, and future trends. Intelligent Service Robotics. Published online January 16, 2023. doi: 10.1007/s11370-022-00452-4
14. Pei J, Zhong K, Li J, et al. PAC: Partial Area Clustering for Re-Adjusting the Layout of Traffic Stations in City's Public Transport. IEEE Transactions on Intelligent Transportation Systems. 2023, 24(1): 1251-1260. doi: 10.1109/tits.2022.3179024
15. Gao H, Huang W, Liu T, et al. PPO2: Location Privacy-Oriented Task Offloading to Edge Computing Using Reinforcement Learning for Intelligent Autonomous Transport Systems. IEEE Transactions on Intelligent Transportation Systems. 2023, 24(7): 7599-7612. doi: 10.1109/tits.2022.3169421
16. Motlagh NH, Kortoçi P, Su X, et al. Unmanned Aerial Vehicles for Air Pollution Monitoring: A Survey. IEEE Internet of Things Journal. 2023, 10(24): 21687-21704. doi: 10.1109/jiot.2023.3290508
17. Zhou W, Wang CX, Huang C, et al. Channel Scenario Extensions, Identifications, and Adaptive Modeling for 6G Wireless Communications. IEEE Internet of Things Journal. Published online 2023: 1-1. doi: 10.1109/jiot.2023.3315296
18. Vaccari I, Carlevaro A, Narteni S, et al. eXplainable and Reliable Against Adversarial Machine Learning in Data Analytics. IEEE Access. 2022, 10: 83949-83970. doi: 10.1109/access.2022.3197299
19. Ram MS, Anandan R. Next-Gen Urban Network Protection: Unveiling AMLSF for Real-Time Security in Smart City Environments. International Journal of Computer Engineering in Research Trends. 2023, 10(4): 155–160.
20. Pradeep G, Ramamoorthy S, Krishnamurthy M, Saritha V. Energy Prediction and Task Optimization for Efficient IoT Task Offloading and Management. International Journal of Intelligent Systems and Applications in Engineering. 2023, 12(1s): 411–427.
21. Addanke S, Anandan R, Krishna PV, et al. An efficient resource management framework for big data using deep feed forward learning networks in smart health care systems. Soft Computing. Published online July 14, 2023. doi:

10.1007/s00500-023-08743-3
22. Lasmika A, Kumaresan M. A Smart Car Parking System Based on IoT with Gray Wolf Optimization-Probability Correlated Neural Network Recognition Methods. Ingénierie des systèmes d information. 2022, 27(5): 807-814. doi: 10.18280/isi.270514
23. Liu Z, Huang F, Weng J, et al. BTMPP: Balancing Trust Management and Privacy Preservation for Emergency Message Dissemination in Vehicular Networks. IEEE Internet of Things Journal. 2021, 8(7): 5386-5407. doi: 10.1109/jiot.2020.3037098
24. Guo J, Liu Z, Tian S, et al. TFL-DT: A Trust Evaluation Scheme for Federated Learning in Digital Twin for Mobile Networks. IEEE Journal on Selected Areas in Communications. 2023, 41(11): 3548-3560. doi: 10.1109/jsac.2023.3310094
25. Reddy A, Pradeep G, Sravani M. Binary Decision Tree for Association Rules Mining in Incremental Databases. International Journal of Data Mining & Knowledge Management Process (IJDKP). 2015, 5(6).
26. Demiroglou V, Mamatas L, Tsaoussidis V. Adaptive NDN, DTN and NoD Deployment in Smart-City Networks Using SDN. 2023 IEEE 20th Consumer Communications & Networking Conference (CCNC). Published online January 8, 2023. doi: 10.1109/ccnc51644.2023.10060803
27. GTSRB- German Traffic Sign Recognition Benchmark Available online: https://www.kaggle.com/datasets/meowmeowmeowmeowmeow/gtsrb-german-traffic-sign (accessed on 5 August 2011).