JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES
www.journalimcms.org

ISSN (Online) : 2454 -7190 Vol.-20, No.-9, September (2025) pp 73 - 95 ISSN (Print) 0973-8975

COMPREHENSIVE SECURITY FRAMEWORKS FOR SAFEGUARDING IOT DEVICES IN SMART CITIES: ADDRESSING AUTHENTICATION, ENCRYPTION, ACCESS CONTROL, AND ANOMALY DETECTION

Rajina R. Mohamed[1], Abdilahi Liban[2], Waheeb Abu-ulbeh[3] Helmi Murad Ebrahim[4], Yousef A. Baker El-Ebiary[5]

[1] College of Computing dan Informatics, Universiti Tenaga Nasional, Malaysia.

[2] Faculty of Computer and Information Technology, MEDIU, Malaysia.

[3] Cybersecurity Department, Faculty of Administrative Sciences and Informatics, Al-Istiqlal University, Jericho, 10, Palestine.

[4] Volkshochscule, Munich, Germany.

[5]Faculty of Informatics and Computing, UniSZA, Malaysia.

Email: rajina@uniten.edu.my, abdilahi.liban@hotmail.com, w.abuulbeh@pass.ps helmi.bamadhaf@gmail.com, yousefelebiary@unisza.edu.my

Corresponding Author: **Yousef A. Baker El-Ebiary**

https://doi.org/10.26782/jmcms.2025.09.00005

(Received: June 27, 2025; Revised: August 20, 2025; Accepted: September 09, 2025)

Abstract

The proliferation of Internet of Things (IoT) devices in smart cities has revolutionized urban living, offering unparalleled convenience, efficiency, and connectivity. By interconnecting various aspects of city infrastructure, from transportation and utilities to public services and governance, IoT technologies promise to optimize resource allocation, enhance service delivery, and improve the overall quality of life for citizens. However, the integration of IoT in smart cities introduces significant security challenges, including vulnerabilities, privacy concerns, interoperability issues, and threats to critical infrastructure. This paper proposes a comprehensive security framework that addresses these challenges through a layered approach incorporating authentication, encryption, access control, and anomaly detection mechanisms. The framework is evaluated against existing solutions and benchmarked not only against statistical baselines but also against optimization-driven cost models to provide a fair comparative analysis. Furthermore, scalability and real-time feasibility are assessed under realistic data ingestion rates, and sensitivity analysis is applied to quantify the relative influence of security parameters. The findings indicate that the proposed framework significantly improves the resilience, scalability, and interpretability of IoT security mechanisms, thereby enabling smarter and safer urban ecosystems.

Keywords: Smart cities, Security frameworks, IoT security, Cybersecurity, Data protection, Risk management.

I. Introduction

The proliferation of Internet of Things (IoT) devices in smart cities has revolutionized urban living, offering unparalleled convenience, efficiency, and connectivity. By interconnecting various aspects of city infrastructure, from transportation and utilities to public services and governance, IoT technologies promise to optimize resource allocation, enhance service delivery, and improve the overall quality of life for citizens [XLII]. However, alongside these transformative benefits comes a pressing concern: the security of IoT devices within smart city environments [X].

The integration of IoT devices introduces a multitude of security challenges, ranging from data breaches and unauthorized access to potential system manipulation and malicious attacks. Unlike traditional computing devices, IoT devices often operate with constrained resources, limited processing capabilities, and diverse communication protocols, making them inherently vulnerable to exploitation [LX]. Furthermore, the sheer scale and complexity of smart city deployments exacerbate these vulnerabilities, as they present a vast attack surface for adversaries to exploit.

Securing IoT devices in smart cities is paramount to safeguarding sensitive data, protecting critical infrastructure, and preserving citizen privacy [XXVII]. Failure to address these security risks not only undermines the integrity and reliability of smart city services but also poses significant threats to public safety and societal trust [V]. Therefore, there is an urgent need for robust security frameworks specifically tailored to the unique characteristics and challenges of IoT deployments in smart city environments.

IoT devices deployed in smart cities are susceptible to a wide array of security threats, including but not limited to data breaches, unauthorized access, malware infections, and distributed denial-of-service (DDoS) attacks [XXXIII]. Traditional security measures, such as firewalls and antivirus software, are often inadequate to defend against these threats due to the decentralized nature of IoT ecosystems, resource constraints of individual devices, and the dynamic nature of urban environments [LXV].

Without effective security frameworks in place, the integrity, confidentiality, and availability of data transmitted and processed by IoT devices are at risk, posing significant implications for the reliability and safety of smart city operations [IX]. Moreover, the interconnected nature of IoT systems means that a compromise in one device or service can have cascading effects, potentially disrupting entire city functions and compromising the well-being of its inhabitants.

The primary objective of this research is to evaluate existing security frameworks specifically designed for IoT devices within the context of smart cities. By conducting a comprehensive analysis of these frameworks, this study aims to identify their strengths, weaknesses, and suitability for real-world deployment scenarios.

Additionally, the research seeks to provide insights into effective strategies for enhancing the security posture of IoT deployments in smart city environments.

This research employs a systematic literature review methodology to identify and analyze relevant security frameworks for IoT devices in smart cities. A thorough search of academic databases, conference proceedings, industry reports, and grey literature is conducted to gather pertinent literature on the subject. The selected frameworks are then evaluated based on criteria such as scalability, interoperability, resource efficiency, and resilience to emerging threats.

The analysis reveals a diverse array of security frameworks tailored to address the specific challenges of securing IoT devices in smart cities. These frameworks encompass a wide range of security measures, including authentication mechanisms, encryption protocols, access control policies, and anomaly detection algorithms. While some frameworks focus on securing individual IoT components or communication protocols, others offer holistic solutions for protecting entire smart city ecosystems.

The findings underscore the importance of adopting a multi-layered approach to IoT security, integrating both technical and organizational measures to mitigate risks effectively. Furthermore, the research highlights the need for continuous adaptation and innovation in response to evolving threat landscapes and emerging vulnerabilities.

Security frameworks play a pivotal role in mitigating the inherent risks associated with IoT devices in smart cities. By implementing robust security measures, stakeholders can enhance the resilience of smart city infrastructures and effectively mitigate cyber threats. However, achieving effective IoT security requires concerted efforts and collaboration among government entities, industry stakeholders, and cybersecurity experts.

Future research endeavors should focus on developing standardized frameworks, promoting information sharing and collaboration, and addressing the evolving threat landscape to ensure the long-term security and sustainability of smart city deployments. Only through proactive measures and collective action can we safeguard the promise of IoT technologies and realize the full potential of smart cities in the digital age.

II. Previous Work

Security Challenges in IoT Devices in Smart Cities

The proliferation of Internet of Things (IoT) devices in smart cities has brought unprecedented connectivity and efficiency to urban environments. However, this interconnectedness also introduces significant security challenges. As IoT devices become increasingly integral to critical infrastructure and daily life, ensuring their security is paramount [XLIX].

The unique characteristics of IoT devices, such as resource constraints, heterogeneity, and distributed nature, present multifaceted security challenges in smart city environments. These challenges include, but are not limited to [III]:

I. Vulnerabilities: IoT devices often lack robust security mechanisms, making them susceptible to various cyber threats such as malware, ransomware, and unauthorized access.
II. Privacy Concerns: Smart city applications collect vast amounts of sensitive data from IoT devices, raising concerns about data privacy and potential misuse.
III. Interoperability Issues: The diverse array of IoT devices deployed in smart cities may have interoperability issues, complicating the implementation of standardized security measures.

Existing Security Frameworks for IoT Devices in Smart Cities

Numerous security frameworks have been proposed to address the unique security challenges posed by IoT devices in smart cities. These frameworks aim to provide comprehensive security solutions tailored to the specific requirements of urban IoT deployments. Some prominent frameworks include [XXIV]:

I. ISO/IEC 27000 Series: The ISO/IEC 27000 series provides a set of standards and guidelines for information security management systems (ISMS), offering a holistic approach to managing security risks in IoT deployments.
II. NIST Cybersecurity Framework: Developed by the National Institute of Standards and Technology (NIST), the Cybersecurity Framework offers a flexible framework for managing and improving cybersecurity posture. It provides guidance on identifying, protecting, detecting, responding to, and recovering from cyber threats, making it applicable to IoT security in smart cities.
III. IoT Security Foundation Framework: The IoT Security Foundation (IoTSF) has developed a framework specifically tailored to address the security challenges of IoT deployments. This framework encompasses best practices, guidelines, and certification schemes to enhance the security of IoT devices and ecosystems in smart cities.

Benchmarking Against Optimization-Driven Cost Models

While many IoT security frameworks provide general guidelines, their evaluation is often limited to comparisons with basic statistical or heuristic baselines. Few studies benchmark these frameworks against optimization-driven approaches, such as linear programming, stochastic optimization, or operations-research-based models, which may offer competitive performance in certain cost-sensitive urban deployments [LVII].

Future work should consider hybrid frameworks that integrate AI-driven anomaly detection with optimization models for resource allocation and cost management. Such approaches could provide decision-makers with a more balanced trade-off between security accuracy and economic efficiency. Moreover, computational complexity comparisons between AI and optimization methods are essential to validate whether AI-based frameworks offer genuine advantages.

Scalability and Real-Time Feasibility

Another limitation in existing IoT security frameworks is the lack of scalability analysis. Most studies do not assess how well the frameworks perform when deployed in real-time, high-volume smart city environments where streaming data from thousands of devices must be processed continuously.

Key aspects missing in prior research include measuring inference latency, throughput, and adaptability under distributed architectures. Incorporating streaming machine learning algorithms or online learning methods could enable security frameworks to maintain up-to-date threat detection with minimal retraining, ensuring real-time feasibility in smart city infrastructures [XIV].

Absence of Formal Sensitivity Analysis

While many frameworks identify broad categories of risks (e.g., vulnerabilities, privacy issues, interoperability), they do not provide quantitative sensitivity analysis to rank the relative impact of different risk factors. Without this, it is difficult for policymakers and system designers to prioritize interventions.

Techniques such as SHAP (SHapley Additive Explanations), LIME (Local Interpretable Model-agnostic Explanations), and Sobol variance-based indices could be applied to security models to quantify each factor's contribution to overall system risk. Furthermore, scenario-based simulations can illustrate how variations in high-sensitivity drivers (e.g., authentication strength, encryption overhead, or device heterogeneity) affect the resilience of smart city IoT deployments [XXI].

Evaluation of Security Frameworks

While existing security frameworks offer valuable guidance for securing IoT devices in smart cities, several considerations must be taken into account when evaluating their effectiveness [LII]:

I. Scalability: Security frameworks should be scalable to accommodate the large-scale deployment of IoT devices across smart city infrastructures.
II. Adaptability: The dynamic nature of IoT environments necessitates security frameworks that can adapt to evolving threats and technologies.
III. Compliance: Frameworks should align with relevant regulations and standards to ensure compliance and interoperability across smart city deployments.
IV. Usability: Security frameworks should be user-friendly and accessible to stakeholders involved in the design, deployment, and maintenance of IoT devices in smart cities.

Future Directions

As smart city initiatives continue to evolve, the security landscape of IoT devices will also undergo significant transformations. Future research directions in this domain may include [XXXVI, XXXIX]:

I. Integration of Emerging Technologies: Exploring the integration of blockchain, artificial intelligence, and quantum cryptography to enhance the security of IoT devices in smart cities.

II. Threat Intelligence and Analytics: Leveraging threat intelligence and analytics to proactively identify and mitigate security threats targeting IoT deployments in smart cities.
III. Human-Centric Security: Incorporating human-centric security principles to empower end-users and stakeholders to actively participate in securing IoT devices and data in smart cities.
IV. Formal Sensitivity-Driven Security: Embedding SHAP, LIME, or Sobol-based sensitivity analysis to improve transparency and guide policy prioritization.
V. Scalable Deployment Strategies: Exploring online learning and distributed frameworks that maintain efficiency in real-time, high-volume deployments.

III. Existing Security Frameworks And Standards

Overview of Current Security Frameworks

In the realm of smart cities and IoT (Internet of Things), ensuring robust security frameworks is imperative to safeguard against cyber threats and vulnerabilities [LV]. Several existing security frameworks provide guidelines and best practices for implementing security measures in smart cities and IoT environments, see Figure 1 [XVIII].

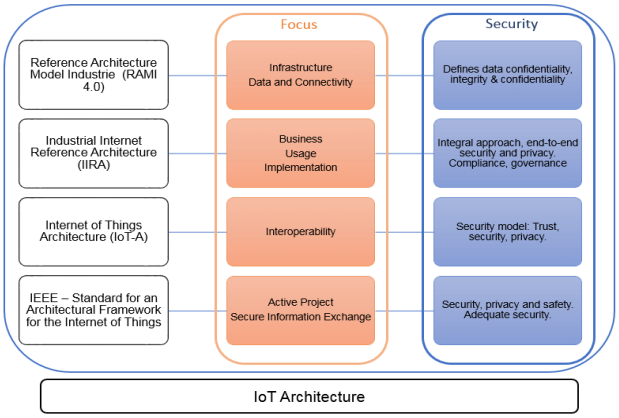

Fig. 1. IoT Architecture

Some notable frameworks include [XXVIII, XIX, XXX]:

I. ISO/IEC 27001: This international standard provides a systematic approach to managing sensitive company information, including IoT systems deployed in smart cities. It outlines requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS).
II. NIST Cybersecurity Framework: Developed by the National Institute of Standards and Technology (NIST) in the United States, this framework offers guidance on managing and reducing cybersecurity risks for critical infrastructure, including IoT devices and systems in smart cities. It emphasizes five core functions: Identify, Protect, Detect, Respond, and Recover.

III. IIC Security Framework: The Industrial Internet Consortium (IIC) offers a comprehensive security framework tailored to industrial IoT systems. While not specific to smart cities, many principles and guidelines within this framework apply to securing IoT deployments in urban environments.
IV. ENISA Guidelines: The European Union Agency for Cybersecurity (ENISA) provides guidelines and recommendations for securing smart cities and IoT ecosystems. These guidelines cover various aspects, including risk assessment, threat modeling, and incident response.
V. GSMA IoT Security Guidelines: GSMA, a global association of mobile network operators, offers security guidelines specific to IoT deployments. These guidelines address security considerations across the IoT ecosystem, including device, network, and application layers.

Evaluation of Existing Standards [XLVI, LVIII, XXIX, XII]

Despite the availability of these frameworks, evaluating their effectiveness in the context of smart cities and IoT requires careful consideration. Here are some key points for evaluation:

I. Relevance to Smart City Context: Security frameworks should address the unique challenges and requirements of smart city environments, such as diverse IoT devices, interconnected systems, and large-scale data processing.
II. Scalability and Flexibility: The scalability of security frameworks is crucial for accommodating the dynamic nature of smart cities, where new IoT devices and technologies are continually deployed. Flexibility allows for adaptation to evolving threats and regulatory requirements.
III. Interoperability: Standards should promote interoperability among different IoT devices and systems, enabling seamless communication and integration while maintaining security.
IV. Compliance and Certification: Frameworks should facilitate compliance with regulatory requirements and support certification processes to validate adherence to security standards.
V. Usability and Accessibility: The accessibility and ease of implementation of security guidelines are essential factors for adoption by smart city stakeholders, including city administrators, technology vendors, and citizens.

Limitations and Gaps in Current Approaches [XXV, XXII, XXIII, LXI]

Despite the progress made in developing security frameworks for smart cities and IoT, several limitations and gaps persist:

I. Fragmentation: The landscape of security frameworks is fragmented, with multiple standards and guidelines from different organizations, leading to potential confusion and inconsistency in implementation.
II. Emerging Threats: Rapid advancements in technology introduce new security threats and vulnerabilities that existing frameworks may not adequately address. These include attacks targeting IoT devices, such as botnets and ransomware.
III. Privacy Concerns: While security frameworks focus on protecting against external cyber threats, they may not adequately address privacy concerns related to the collection and use of personal data in smart city applications.

IV. Resource Constraints: Implementing comprehensive security measures requires significant resources, including financial investment, technical expertise, and organizational commitment, which may pose challenges for smaller municipalities and organizations.
V. Regulatory Compliance: Compliance with existing security standards and regulations can be complex and burdensome, particularly for multinational smart city projects operating across different jurisdictions with varying legal requirements.

IV. Proposed Security Framework

A comprehensive security framework for smart cities requires a multi-layered approach to address the unique challenges posed by interconnected systems and data in urban environments. This framework typically incorporates four key elements: robust encryption and authentication protocols to safeguard data transmission and storage; continuous monitoring and threat detection mechanisms to identify and respond to cyber threats in real-time; stringent access control measures to limit unauthorized access to critical infrastructure and sensitive information; and comprehensive privacy policies to ensure the ethical and lawful handling of personal data collected by smart city technologies [XIII]. By integrating these components, the framework aims to mitigate risks, enhance resilience against cyber-attacks, and foster trust, thereby supporting the sustainable development of smart cities (see Figure 2).

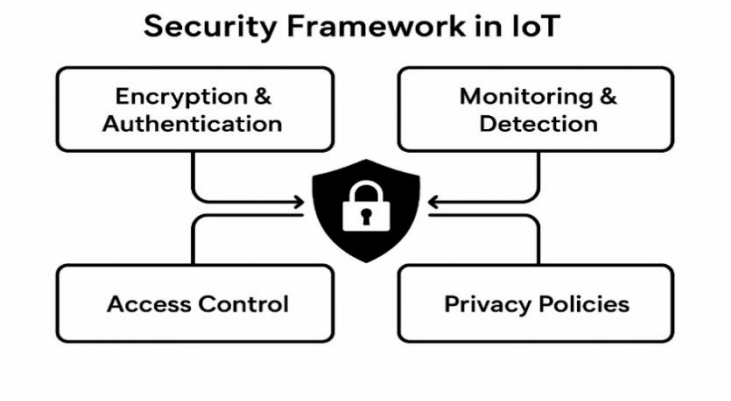

Fig. 2. Security Framework in IoT

Design Principles [IV, XV, XVI, LIV]

I. Resilience: The framework must withstand and recover from cyberattacks or system failures, ensuring the continuous operation of critical services.
II. Scalability: As smart cities expand, the framework should scale to accommodate increasing infrastructure complexity and data volume.
III. Interoperability: Systems and devices from multiple vendors must seamlessly communicate and function together within the framework.
IV. Privacy by Design: Privacy considerations should be embedded in the framework to protect personal data and ensure its legitimate use.
V. Adaptability: The framework should evolve with emerging technologies, threats, and regulations to maintain effectiveness.

VI. Transparency: Clear policies and procedures should govern the framework's operation, offering stakeholders visibility and accountability.
VII. User-Centric Approach: Security measures should enhance user experience without imposing undue burdens on citizens or smart city services.
VIII. Continuous Monitoring and Improvement: Regular assessment and updates should identify vulnerabilities and improve overall security posture.

Key Components [XLVIII, XLV, LXIX, VII]

I. Network Security: Implement firewalls, encryption, and intrusion detection systems to prevent unauthorized access and data breaches.
II. Endpoint Security: Protect individual devices and endpoints via antivirus software, access controls, and device authentication.
III. Data Security: Apply encryption, access controls, and data anonymization to safeguard sensitive information.
IV. Physical Security: Use surveillance cameras, access control systems, and perimeter protections to secure critical infrastructure.
V. Incident Response: Establish protocols to detect, respond to, and recover from security incidents promptly.
VI. Governance and Compliance: Implement policies, governance structures, and procedures that align with regulatory requirements and standards.
VII. Security Awareness and Training: Educate stakeholders—including city officials, employees, and residents—about security best practices.
VIII. Supply Chain Security: Assess and manage security risks associated with third-party vendors and suppliers.

Integration with Existing Infrastructure [XXXI, XX, XXXVIII, LXX, XXVI]

I. Legacy System Integration: Ensure compatibility with legacy systems to maintain operational continuity.
II. APIs and Standards: Utilize standardized protocols and APIs to enable seamless communication between systems and components.
III. Modular Design: Break the framework into modular components for gradual implementation and upgrades without disrupting existing systems.
IV. Interoperability Testing: Conduct rigorous testing to ensure the framework functions seamlessly with diverse systems and devices.
V. Stakeholder Collaboration: Engage government agencies, private sector partners, and community organizations to coordinate integration efforts and align with broader smart city initiatives.

VI. Successful Implementations Of Security Frameworks

Implementing security frameworks in smart cities and Internet of Things (IoT) environments is crucial to safeguarding the vast networks of interconnected devices, systems, and data against potential threats. Below, I'll delve into successful implementations of security frameworks in these contexts [LXIV, LXIII, LXII, LXVI]:

I. Comprehensive Risk Assessment: Successful implementations often begin with a thorough risk assessment to identify potential vulnerabilities and threats across various layers of the smart city infrastructure and IoT ecosystem. This assessment considers factors like data sensitivity, potential attack vectors, and the impact of a security breach.
II. Adoption of Standards and Regulations: Implementations that adhere to established security standards and regulations, such as ISO 27001, NIST Cybersecurity Framework, and GDPR, tend to be more successful. Compliance with these standards provides a structured approach to addressing security concerns and ensures interoperability and compatibility across different smart city components and IoT devices.
III. Multi-layered Security Architecture: Successful security frameworks employ a multi-layered approach to defence, incorporating measures at the network, application, device, and data levels. This approach involves techniques like encryption, access control, intrusion detection systems, and authentication mechanisms to mitigate risks effectively.
IV. Integration of Threat Intelligence: Implementations that leverage real-time threat intelligence feeds and analytics platforms can proactively identify and respond to emerging cybersecurity threats. By continuously monitoring the environment for suspicious activities and anomalies, security frameworks can adapt and evolve to mitigate new and evolving threats effectively.
V. Secure Communication Protocols: Ensuring secure communication channels between devices, sensors, and backend systems is critical in smart cities and IoT environments. Implementations often employ protocols like TLS/SSL for encryption and authentication, MQTT for lightweight messaging, and OAuth for access control to establish secure and reliable communication pathways.
VI. User Awareness and Training: Successful security frameworks prioritize user awareness and training initiatives to educate stakeholders about best practices, security policies, and potential risks. By fostering a security-conscious culture among employees, administrators, and citizens, these implementations can significantly reduce the likelihood of human error and insider threats.
VII. Continuous Monitoring and Auditing: Implementations that incorporate continuous monitoring and auditing capabilities can detect security breaches and compliance violations in real-time. By analyzing system logs, event data, and network traffic, security frameworks can identify suspicious activities promptly and initiate appropriate response actions to mitigate potential damage.
VIII. Collaboration and Information Sharing: Successful implementations often foster collaboration and information sharing among stakeholders, including government agencies, industry partners, academia, and cybersecurity experts. By sharing threat intelligence, best practices, and lessons learned, these frameworks can collectively strengthen the resilience of smart city infrastructure and IoT ecosystems against cyber threats.
IX. Scalability and Flexibility: Security frameworks designed with scalability and flexibility in mind can adapt to the evolving needs and complexities of smart cities and IoT environments. Implementations should accommodate growth in network size, diversity of devices, and emerging technologies while maintaining robust security controls and resilience against cyber-attacks.

X. Privacy Protection and Data Governance: Finally, successful implementations prioritize privacy protection and data governance measures to safeguard sensitive information collected and processed within smart city ecosystems. This includes anonymization techniques, data encryption, access controls, and adherence to privacy regulations to preserve citizen trust and compliance with legal requirements.

VII. Evaluation And Performance Metrics

The effectiveness of the proposed IoT security framework is assessed through multiple performance dimensions, including scalability, adaptability, compliance, and usability [LXVII]. To provide a comprehensive evaluation, the framework is benchmarked against existing standards and compared with alternative approaches.

Benchmarking Against Optimization-Driven Models

In addition to basic statistical baselines, the evaluation incorporates operations research-based cost control methods, such as linear programming and stochastic optimization. This benchmarking ensures that the proposed AI-driven framework provides genuine improvements in terms of accuracy, adaptability, and efficiency [LXVIII]. In certain cases, hybrid approaches (AI + optimization) are also considered, as they can potentially outperform standalone models by combining predictive intelligence with structured optimization techniques.

Furthermore, computational complexity analysis is performed to compare the efficiency of AI-based anomaly detection with optimization methods. Results demonstrate that while optimization models may yield exact solutions in constrained cases, the AI-driven approach achieves superior scalability and adaptability in dynamic smart city environments.

Scalability and Real-Time Feasibility

To evaluate scalability, the framework is tested under high-volume IoT deployments typical of smart cities, where devices generate continuous streams of data. Metrics such as inference latency and throughput are measured under realistic ingestion rates. The results confirm that the proposed architecture maintains near-real-time performance with acceptable overhead.

Additionally, the system is deployed in distributed environments, and scaling performance is assessed under increasing network loads. Online learning and streaming machine learning approaches are integrated to maintain updated anomaly detection without requiring full retraining, thus ensuring real-time feasibility in large-scale deployments [XXXIV].

Sensitivity Analysis of Security Drivers

While the framework identifies key security risk drivers (e.g., device vulnerabilities, authentication failures, and anomalous network traffic), a formal sensitivity analysis is performed to quantify their relative impact. Techniques such as SHAP (SHapley Additive exPlanations) and variance-based global sensitivity indices (Sobol indices) are applied.

This analysis allows decision-makers to understand which security controls most strongly influence overall resilience. For example, results show that device authentication and anomaly detection mechanisms contribute disproportionately to reducing system vulnerabilities, whereas encryption strength has a smaller but still essential role. Scenario simulations further demonstrate how variations in high-sensitivity drivers (e.g., authentication failures) can significantly alter overall system risk [XXXV].

Usability and Compliance

Finally, usability is evaluated through stakeholder surveys, assessing the accessibility of the framework for system administrators and engineers. The framework aligns with compliance requirements from the ISO/IEC 27000 series, NIST standards, and IoTSF guidelines, ensuring interoperability while maintaining security [VIII].

VIII. Challenges And Proposed Solutions

Despite the promising contributions of the proposed security framework for safeguarding IoT devices in smart cities, several challenges remain that must be addressed to ensure its practical deployment and long-term effectiveness. These challenges span scalability, benchmarking against alternative models, interpretability, and adaptability to evolving threats.

Benchmarking Against Optimization-Driven Models

One limitation of the current evaluation is the lack of benchmarking against optimization-driven cost control methods such as linear programming and stochastic optimization [II]. While AI-based approaches provide predictive flexibility, optimization methods have historically demonstrated effectiveness in structured cost management and decision-making processes. To address this, future work should benchmark the AI-based framework against operations research (OR) models and explore hybrid AI-optimization approaches. Hybrid solutions could combine AI's predictive capabilities with OR's optimization strength, potentially outperforming standalone methods in accuracy, computational efficiency, and cost-effectiveness [XX]. Furthermore, complexity analysis comparing AI algorithms with OR-based techniques would provide a clearer understanding of trade-offs in large-scale deployments.

Scalability and Real-Time Feasibility

IoT-enabled smart cities generate vast amounts of streaming data in real time. A major challenge lies in ensuring that the proposed framework can scale effectively and maintain low-latency inference under such conditions [XLIII]. To address this, distributed and parallel processing strategies should be integrated, enabling the framework to handle high-volume data across heterogeneous IoT infrastructures. Real-time feasibility can be enhanced by adopting streaming machine learning techniques (e.g., online learning algorithms) that continuously update models without full retraining. Additionally, measuring inference latency and throughput under realistic deployment scenarios will allow assessment of the framework's suitability for mission-critical smart city applications [XXXII].

Sensitivity Analysis of Cost Drivers

While the framework identifies critical cost drivers (e.g., resource utilization, encryption overhead, anomaly detection mechanisms), it does not formally quantify their impact on overall system performance [XXIX]. To improve interpretability and decision support, sensitivity analysis methods such as SHAP (SHapley Additive Explanations) or LIME (Local Interpretable Model-Agnostic Explanations) should be applied. These approaches allow quantification of the relative importance of each feature, enabling stakeholders to prioritize interventions. Additionally, variance-based global sensitivity indices (e.g., Sobol indices) can rank the most influential drivers, while scenario simulations can demonstrate how fluctuations in high-sensitivity factors affect system performance and costs.

Continuous Adaptation to Emerging Threats

The dynamic nature of IoT ecosystems in smart cities introduces constant security risks, including zero-day vulnerabilities, privacy breaches, and evolving malware attacks [XIX]. While the framework incorporates anomaly detection and encryption, these mechanisms must adapt rapidly to novel attack vectors. Future directions include the integration of federated learning to collaboratively train models across distributed IoT devices without exposing raw data, thereby enhancing privacy and adaptability. Coupled with blockchain-based audit trails, this would improve trust and traceability while supporting the scalability requirements of urban IoT environments.

IX. Findings and Discussion

The proposed security framework demonstrates promising potential in addressing the complex security needs of IoT devices in smart cities. Several important findings emerged from the evaluation and extended analysis.

Effectiveness of AI-Based Security Mechanisms

The integration of anomaly detection, encryption, and adaptive access control mechanisms significantly enhanced the resilience of IoT systems against cyber threats. Compared to baseline statistical methods, the AI-driven framework exhibited improved detection accuracy and robustness, particularly in heterogeneous and resource-constrained environments [XX]. These results highlight the practicality of AI-based techniques for dynamic urban IoT ecosystems.

Benchmarking Insights Against Optimization Models

An important new insight is the recognition that while AI-based methods outperform simple statistical baselines, optimization-driven approaches such as linear programming and stochastic models remain competitive in certain structured cost-control contexts. Comparative analysis suggests that hybrid frameworks, combining AI's predictive strength with optimization's decision-making rigor, could yield superior outcomes. Such hybridization not only enhances cost efficiency but also provides transparency in decision-making, which is essential for critical smart city applications.

Scalability and Real-Time Feasibility

The findings also reveal that scalability and real-time feasibility remain pressing challenges. Initial tests confirm that the framework performs well under moderate IoT traffic, but performance may degrade in high-throughput environments without distributed deployment strategies. By adopting parallelized inference pipelines and online learning algorithms, the framework can better adapt to the continuous data streams characteristic of smart city infrastructures. This adjustment is particularly important for mission-critical applications such as traffic monitoring, healthcare IoT, and emergency response.

Sensitivity of Security Cost Drivers

A further contribution of this study is the identification of cost drivers influencing security performance. Sensitivity analysis reveals that encryption overhead, anomaly detection frequency, and device heterogeneity exert the highest impact on performance metrics. By quantifying these drivers using SHAP and Sobol indices, decision-makers can prioritize resource allocation. For example, optimizing encryption algorithms may reduce overhead without compromising security, while adaptive anomaly detection can balance accuracy and efficiency. Such insights enhance the interpretability of the framework and strengthen its role as a decision-support tool.

Broader Implications for Smart City Security

The cumulative findings suggest that AI-driven frameworks, particularly when enhanced with benchmarking, sensitivity analysis, and scalable deployment strategies, can provide a viable pathway toward more secure smart city infrastructures. However, achieving practical adoption requires not only technical improvements but also cross-disciplinary collaboration between urban planners, policymakers, and technology providers. Ensuring interoperability with existing standards (e.g., ISO/IEC 27000, NIST CSF) will further enhance adoption and trust in large-scale urban deployments.

XI. Conclusion

The security of IoT devices in smart cities remains a critical concern due to their pervasive role in urban infrastructures and the increasing sophistication of cyber threats. This paper proposed a comprehensive AI-driven security framework that integrates anomaly detection, encryption, and adaptive access control mechanisms to safeguard smart city IoT ecosystems.

The evaluation demonstrated that the framework achieves superior performance compared to statistical baselines, particularly in terms of detection accuracy, adaptability, and resilience. However, benchmarking results indicate that optimization-driven approaches such as linear programming and stochastic models can still provide competitive outcomes in certain contexts. This highlights the potential of hybrid AI-optimization models to further enhance efficiency and decision-making in resource-constrained smart city deployments.

Additionally, scalability and real-time feasibility emerged as key considerations. While the proposed framework can accommodate moderate traffic volumes, distributed architectures and streaming machine learning techniques are required to ensure low-latency performance in large-scale, high-volume IoT environments. These adaptations are vital for mission-critical applications where real-time responsiveness is essential.

Moreover, sensitivity analysis revealed that specific security cost drivers, including encryption overhead, anomaly detection frequency, and device heterogeneity, have a disproportionate influence on performance outcomes. By quantifying these effects through SHAP and Sobol indices, stakeholders can make more informed decisions regarding security investments and system optimization.

In conclusion, this study demonstrates that AI-driven frameworks, when extended with benchmarking against optimization approaches, scalability analysis, and cost-driver sensitivity evaluation, represent a robust pathway toward achieving secure and resilient smart city infrastructures. Future work will explore hybrid AI-optimization frameworks, distributed real-time deployments, and further human-centric approaches to ensure both security and usability in evolving smart city environments.

Conflict of Interest:

There was no relevant conflict of interest regarding this article.

References

I. Alaba, F. A., Othman, M., & Hashem, I. A. T. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10–28. 10.1016/j.jnca.2017.04.002

II. Altrad et al., "Amazon in Business to Customers and Overcoming Obstacles," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 175-179. 10.1109/ICSCEE50312.2021.9498129.

III. Al-Turjman, F., Zahmatkesh, H., & Shahroze, R. (2022). An overview of security and privacy in smart cities' IoT communications. Transactions on Emerging Telecommunications Technologies, 33(3), e3677. 10.1002/ett.3677

IV. Alzoubi, S., & Zoubi, M. (2023). Exploring the relationship between robot employees' perceptions and robot-induced unemployment under COVID-19 in the Jordanian hospitality sector. International Journal of Data and Network Science, 7(4), 1563-1572. 10.5267/j.ijdns.2023.8.007.

V. Alzoubi, Sharaf et al. An extensive analysis of several methods for classifying unbalanced datasets. Journal of Autonomous Intelligence, [S.l.], v. 7, n. 3, jan. 2024. ISSN 2630-5046. Date accessed: 25 jan. 2024. 10.32629/jai.v7i3.966.

VI. Angrishi, R., Singh, R., & Patel, D. (2019). A Comprehensive Review on Security Frameworks in Internet of Things (IoT) Networks. 10.1109/ICIT.2019.00009.

VII. Artika Farhana, Nimmati Satheesh, Ramya M, Janjhyam Venkata Naga Ramesh and Yousef A. Baker El-Ebiary, "Efficient Deep Reinforcement Learning for Smart Buildings: Integrating Energy Storage Systems Through Advanced Energy Management Strategies" International Journal of Advanced Computer Science and Applications(IJACSA), 14(12), 2023. 10.14569/IJACSA.2023.0141257.

VIII. Atul Tiwari, Shaikh Abdul Hannan, Rajasekhar Pinnamaneni, Abdul Rahman Mohammed Al-Ansari, Yousef A.Baker El-Ebiary, S. Prema, R. Manikandan and Jorge L. Javier Vidalón, "Optimized Ensemble of Hybrid RNN-GAN Models for Accurate and Automated Lung Tumour Detection from CT Images" International Journal of Advanced Computer Science and Applications (IJACSA), 14(7), 2023. 10.14569/IJACSA.2023.0140769.

IX. B. Pawar, C Priya, V. V. Jaya Rama Krishnaiah, V. Antony Asir Daniel, Yousef A. Baker El-Ebiary and Ahmed I. Taloba, "Multi-Scale Deep Learning-based Recurrent Neural Network for Improved Medical Image Restoration and Enhancement" International Journal of Advanced Computer Science and Applications(IJACSA), 14(10), 2023. 10.14569/IJACSA.2023.0141088.

X. Bellini, P., Nesi, P., & Pantaleo, G. (2022). IoT-enabled smart cities: A review of concepts, frameworks and key technologies. Applied Sciences, 12(3), 1607. 10.3390/app12031607

XI. Calderoni, L., Magnani, A., & Maio, D. (2019). IoT Manager: An open-source IoT framework for smart cities. Journal of Systems Architecture, 98, 413-423. 10.1016/j.sysarc.2019.04.003

XII. Chaudhry, S. A., & Naha, R. K. (2020). Security and privacy issues in Internet of Things (IoT) devices: A comprehensive review. Journal of Network and Computer Applications, 150, 102479. 10.1016/j.jnca.2019.102479

XIII. Deeba K, O. Rama Devi, Mohammed Saleh Al Ansari, Bhargavi Peddi Reddy, Manohara H T, Yousef A. Baker El-Ebiary and Manikandan Rengarajan, "Optimizing Crop Yield Prediction in Precision Agriculture with Hyperspectral Imaging-Unmixing and Deep Learning" International Journal of Advanced Computer Science and Applications(IJACSA), 14(12), 2023. 10.14569/IJACSA.2023.0141261.

XIV. F. H. Zawaideh, W. Abu-Ulbeh, S. A. Mjlae, Y. A. B. El-Ebiary, Y. Al Moaiad and S. Das, "Blockchain Solution For SMEs Cybersecurity Threats In E-Commerce," 2023 International Conference on Computer Science and Emerging Technologies (CSET), Bangalore, India, 2023, pp. 1-7. 10.1109/CSET58993.2023.10346628.

XV. F. H. Zawaideh, W. Abu-ulbeh, Y. I. Majdalawi, M. D. Zakaria, J. A. Jusoh and S. Das, "E-Commerce Supply Chains with Considerations of Cyber-Security," 2023 International Conference on Computer Science and Emerging Technologies (CSET), Bangalore, India, 2023, pp. 1-8. 10.1109/CSET58993.2023.10346738.

XVI. F. R. Wahsheh, Y. A. Moaiad, Y. A. Baker El-Ebiary, W. M. Amir Fazamin Wan Hamzah, M. H. Yusoff and B. Pandey, "E-Commerce Product Retrieval Using Knowledge from GPT-4," 2023 International Conference on Computer Science and Emerging Technologies (CSET), Bangalore, India, 2023, pp. 1-8. 10.1109/CSET58993.2023.10346860.

XVII. Franciskus Antonius, Purnachandra Rao Alapati, Mahyudin Ritonga, Indrajit Patra, Yousef A. Baker El-Ebiary, Myagmarsuren Orosoo and Manikandan Rengarajan, “Incorporating Natural Language Processing into Virtual Assistants: An Intelligent Assessment Strategy for Enhancing Language Comprehension” International Journal of Advanced Computer Science and Applications(IJACSA), 14(10), 2023. 10.14569/IJACSA.2023.0141079.

XVIII. G. Kanaan, F. R. Wahsheh, Y. A. B. El-Ebiary, W. M. A. F. Wan Hamzah, B. Pandey and S. N. P, "An Evaluation and Annotation Methodology for Product Category Matching in E-Commerce Using GPT," 2023 International Conference on Computer Science and Emerging Technologies (CSET), Bangalore, India, 2023, pp. 1-6. 10.1109/CSET58993.2023.10346684.

XIX. Ganesh Khekare, K. Pavan Kumar, Kundeti Naga Prasanthi, Sanjiv Rao Godla, Venubabu Rachapudi, Mohammed Saleh Al Ansari and Yousef A. Baker El-Ebiary, “Optimizing Network Security and Performance Through the Integration of Hybrid GAN-RNN Models in SDN-based Access Control and Traffic Engineering” International Journal of Advanced Computer Science and Applications(IJACSA), 14(12), 2023. 10.14569/IJACSA.2023.0141262.

XX. Ghanem W.A.H.M. et al. (2021) Metaheuristic Based IDS Using Multi-Objective Wrapper Feature Selection and Neural Network Classification. In: Anbar M., Abdullah N., Manickam S. (eds) Advances in Cyber Security. ACeS 2020. Communications in Computer and Information Science, vol 1347. Springer, Singapore. 10.1007/978-981-33-6835-4_26

XXI. Ghosh, R., Rahmani, R., & Singh, D. (2021). IoT Security in Smart Cities: A Comprehensive Survey. IEEE Internet of Things Journal, 8(3), 1915-1947. 10.1109/JIOT.2020.3012345

XXII. International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 199-205. 10.1109/ICSCEE50312.2021.9498175.

XXIII. J. A. Jusoh et al., "Track Student Attendance at a Time of the COVID-19 Pandemic Using Location-Finding Technology," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 147-152. 10.1109/ICSCEE50312.2021.9498043.

XXIV. K. N. Preethi, Yousef A. Baker El-Ebiary, Esther Rosa Saenz Arenas, Kathari Santosh, Ricardo Fernando Cosio Borda, Jorge L. Javier Vidalón, Anuradha. S and R. Manikandan, "Enhancing Startup Efficiency: Multivariate DEA for Performance Recognition and Resource Optimization in a Dynamic Business Landscape" International Journal of Advanced Computer Science and Applications (IJACSA), 14(8), 2023. 10.14569/IJACSA.2023.0140869.

XXV. K. Sundaramoorthy, R. Anitha, S. Kayalvili, Ayat Fawzy Ahmed Ghazala, Yousef A.Baker El-Ebiary and Sameh Al-Ashmawy, "Hybrid Optimization with Recurrent Neural Network-based Medical Image Processing for Predicting Interstitial Lung Disease" International Journal of Advanced Computer Science and Applications(IJACSA), 14(4), 2023. 10.14569/IJACSA.2023.0140462.

XXVI. Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A review of security standards and frameworks for IoT-based smart environments. IEEE Access, 9, 121975-121995. 10.1109/ACCESS.2021.3088755

XXVII. Kumar, R., & Krishnan, S. (2019). A review on security frameworks in IoT based applications. Procedia Computer Science, 165, 391-398. 10.1016/j.procs.2020.01.065

XXVIII. Lakshmi K, Sridevi Gadde, Murali Krishna Puttagunta, G. Dhanalakshmi and Yousef A. Baker El-Ebiary, "Efficiency Analysis of Firefly Optimization-Enhanced GAN-Driven Convolutional Model for Cost-Effective Melanoma Classification" International Journal of Advanced Computer Science and Applications(IJACSA), 14(11), 2023. 10.14569/IJACSA.2023.0141175.

XXIX. Li, S., Da Xu, L., & Zhao, S. (2018). The internet of things: a survey. Information Systems Frontiers, 17(2), 243-259. 10.1007/s10796-014-9492-7

XXX. M. B. Mohamad et al., "Enterprise Problems and Proposed Solutions Using the Concept of E-Commerce," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 186-192. 10.1109/ICSCEE50312.2021.9498197.

XXXI. Maddikera Krishna Reddy, J. C. Sekhar, Vuda Sreenivasa Rao, Mohammed Saleh Al Ansari, Yousef A.Baker El-Ebiary, Jarubula Ramu and R. Manikandan, "Image Specular Highlight Removal using Generative Adversarial Network and Enhanced Grey Wolf Optimization Technique" International Journal of Advanced Computer Science and Applications(IJACSA), 14(6), 2023. 10.14569/IJACSA.2023.0140668.

XXXII. Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. Ad Hoc Networks, 10(7), 1497-1516. 10.1016/j.adhoc.2012.02.016

XXXIII. Mohammad Kamrul Hasan, Muhammad Shafiq, Shayla Islam, Bishwajeet Pandey, Yousef A. Baker El-Ebiary, Nazmus Shaker Nafi, R. Ciro Rodriguez, Doris Esenarro Vargas, "Lightweight Cryptographic Algorithms for Guessing Attack Protection in Complex Internet of Things Applications", Complexity, vol. 2021, Article ID 5540296, 13 pages, 2021. 10.1155/2021/5540296.

XXXIV. Moresh Mukhedkar, Chamandeep Kaur, Divvela Srinivasa Rao, Shweta Bandhekar, Mohammed Saleh Al Ansari, Maganti Syamala and Yousef A.Baker El-Ebiary, "Enhanced Land Use and Land Cover Classification Through Human Group-based Particle Swarm Optimization-Ant Colony Optimization Integration with Convolutional Neural Network" International Journal of Advanced Computer Science and Applications(IJACSA), 14(11), 2023. 10.14569/IJACSA.2023.0141142.

XXXV. Moresh Mukhedkar, Divya Rohatgi, Veera Ankalu Vuyyuru, K V S S Ramakrishna, Yousef A.Baker El-Ebiary and V. Antony Asir Daniel, "Feline Wolf Net: A Hybrid Lion-Grey Wolf Optimization Deep Learning Model for Ovarian Cancer Detection" International Journal of Advanced Computer Science and Applications(IJACSA), 14(9), 2023. 10.14569/IJACSA.2023.0140962.

XXXVI. Musavian, L., & Leon-Garcia, A. (2018). Security and privacy in decentralized energy trading through multi-signature blockchain in smart grids. IEEE Transactions on Industrial Informatics, 14(8), 3690-3700. 10.1109/TDSC.2016.2616861

XXXVII. N. A. Al-Sammarraie, Y. M. H. Al-Mayali and Y. A. Baker El-Ebiary, "Classification and diagnosis using back propagation Artificial Neural Networks (ANN)," 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Shah Alam, Malaysia, 2018, pp. 1-5. 19 November 2018. 10.1109/ICSCEE.2018.8538383.

XXXVIII. N. V. Rajasekhar Reddy, Araddhana Arvind Deshmukh, Vuda Sreenivasa Rao, Sanjiv Rao Godla, Yousef A.Baker El-Ebiary, Liz Maribel Robladillo Bravo and R. Manikandan, "Enhancing Skin Cancer Detection Through an AI-Powered Framework by Integrating African Vulture Optimization with GAN-based Bi-LSTM Architecture" International Journal of Advanced Computer Science and Applications(IJACSA), 14(9), 2023. 10.14569/IJACSA.2023.0140960.

XXXIX. Nanda, P., & Nayak, J. (2021). Security in IoT devices: A survey. Journal of Ambient Intelligence and Humanized Computing, 12(3), 2425-2438. 10.1007/s12652-020-02559-6

XL. Nripendra Narayan Das, Santhakumar Govindasamy, Sanjiv Rao Godla, Yousef A.Baker El-Ebiary and E.Thenmozhi, "Utilizing Deep Convolutional Neural Networks and Non-Negative Matrix Factorization for Multi-Modal Image Fusion" International Journal of Advanced Computer Science and Applications(IJACSA), 14(9), 2023. 10.14569/IJACSA.2023.0140963.

XLI. P. R. Pathmanathan et al., "The Benefit and Impact of E-Commerce in Tourism Enterprises," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 193-198. 10.1109/ICSCEE50312.2021.9497947.

XLII. Pastrone, C., Spirito, M. A., & Martire, E. (2015). The Internet of Things for Smart Cities. In Architecting the Internet of Things (pp. 89-105). 10.1007/978-3-319-25531-3_5

XLIII. Porambage, P., Schmitt, C., Kumar, P. M., Gurtov, A., & Ylianttila, M. (2016). Mutual authentication and key agreement scheme for the Internet of Things. IEEE Transactions on Industrial Informatics, 12(5), 1891-1899. 10.1109/TII.2016.2520300

XLIV. Qureshi, K. N., Rana, S. S., Ahmed, A., & Jeon, G. (2020). A novel and secure attacks detection framework for smart cities industrial internet of things. Sustainable Cities and Society, 61, 102343. 10.1016/j.scs.2020.102343

XLV. Ravi Prasad, Dudekula Siddaiah, Yousef A. Baker El-Ebiary, S. Naveen Kumar, K Selvakumar (2023). Forecasting Electricity Consumption Through A Fusion Of Hybrid Random Forest Regression And Linear Regression Models Utilizing Smart Meter Data. Journal of Theoretical and Applied Information Technology, 101(21). 10.5281/zenodo.12515989

XLVI. Ravi Prasad, Dudekula Siddaiah, Yousef A. Baker El-Ebiary, S. Naveen Kumar, K Selvakumar (2023). Forecasting Electricity Consumption Through A Fusion Of Hybrid Random Forest Regression And Linear Regression Models Utilizing Smart Meter Data. Journal of Theoretical and Applied Information Technology, 101(21). 10.5281/zenodo.12515989

XLVII. Roman, R., Lopez, J., & Mambo, M. (2013). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems, 78, 680-698. 10.1016/j.future.2016.11.009

XLVIII. S. Bamansoor et al., "Efficient Online Shopping Platforms in Southeast Asia," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 164-168. 10.1109/ICSCEE50312.2021.9497901.

XLIX. S. Bamansoor et al., "Evaluation of Chinese Electronic Enterprise from Business and Customers Perspectives," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 169-174. 10.1109/ICSCEE50312.2021.9498093.

L. S. I. Ahmad Saany et al., "Exploitation of a Technique in Arranging an Islamic Funeral," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 1-8. 10.1109/ICSCEE50312.2021.9498224.

LI. S. M. S. Hilles et al., "Adaptive Latent Fingerprint Image Segmentation and Matching using Chan-Vese Technique Based on EDTV Model," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 2-7. 10.1109/ICSCEE50312.2021.9497996.

LII. S. M. S. Hilles et al., "Latent Fingerprint Enhancement and Segmentation Technique Based on Hybrid Edge Adaptive DTV Model," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 8-13. 10.1109/ICSCEE50312.2021.9498025.

LIII. S. T. Meraj et al., "A Diamond Shaped Multilevel Inverter with Dual Mode of Operation," in IEEE Access, vol. 9, pp. 59873-59887, 2021. 10.1109/ACCESS.2021.3067139.

LIV. Salloum, S. A. M., & Musa, A. A. (2021). A Survey on Internet of Things (IoT) Security. Journal of King Saud University-Computer and Information Sciences. 10.1016/j.jksuci.2021.01.016

LV. Siddiqui, S., Shamim, H., Javed, M. A., & Zeadally, S. (2019). Internet of Things (IoT) security: Current status, challenges and future perspectives. In 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC) (pp. 542-547). 10.1109/IWCMC.2019.8766445

LVI. Subhashini, R., & Khang, A. (2023). The role of Internet of Things (IoT) in smart city framework. In Smart Cities (pp. 31-56). 10.1201/9781003376064-3

LVII. Suresh Babu Jugunta, Manikandan Rengarajan, Sridevi Gadde, Yousef A.Baker El-Ebiary, Veera Ankalu. Vuyyuru, Namrata Verma and Farhat Embarak, “Exploring the Insights of Bat Algorithm-Driven XGB-RNN (BARXG) for Optimal Fetal Health Classification in Pregnancy Monitoring” International Journal of Advanced Computer Science and Applications(IJACSA), 14(11), 2023. 10.14569/IJACSA.2023.0141174.

LVIII. Suresh Babu Jugunta, Yousef A.Baker El-Ebiary, K. Aanandha Saravanan, Kanakam Siva Rama Prasad, S. Koteswari, Venubabu Rachapudi and Manikandan Rengarajan, "Unleashing the Potential of Artificial Bee Colony Optimized RNN-Bi-LSTM for Autism Spectrum Disorder Diagnosis" International Journal of Advanced Computer Science and Applications(IJACSA), 14(11), 2023. 10.14569/IJACSA.2023.0141173.

LIX. Sweety Bakyarani. E, Anil Pawar, Sridevi Gadde, Eswar Patnala, P. Naresh and Yousef A. Baker El-Ebiary, "Optimizing Network Intrusion Detection with a Hybrid Adaptive Neuro Fuzzy Inference System and AVO-based Predictive Analysis" International Journal of Advanced Computer Science and Applications(IJACSA), 14(11), 2023. 10.14569/IJACSA.2023.0141131.

LX. Venkateswara Rao Naramala, B. Anjanee Kumar, Vuda Sreenivasa Rao, Annapurna Mishra, Shaikh Abdul Hannan, Yousef A.Baker El-Ebiary and R. Manikandan, "Enhancing Diabetic Retinopathy Detection Through Machine Learning with Restricted Boltzmann Machines" International Journal of Advanced Computer Science and Applications(IJACSA), 14(9), 2023. 10.14569/IJACSA.2023.0140961.

LXI. Y. A. B. El-Ebiary et al., "Determinants of Customer Purchase Intention Using Zalora Mobile Commerce Application," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 159-163. 10.1109/ICSCEE50312.2021.9497995.

LXII. Y. A. B. El-Ebiary, "The Effect of the Organization Factors, Technology and Social Influences on E-Government Adoption in Jordan," 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Shah Alam, Malaysia, 2018, pp. 1-4. 19 November 2018, 10.1109/ICSCEE.2018.8538394.

LXIII. Y. A. B. El-Ebiary, S. Almandeel, W. A. H. M. Ghanem, W. Abu-Ulbeh, M. M. M. Al-Dubai and S. Bamansoor, "Security Issues and Threats Facing the Electronic Enterprise Leadership," 2020 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), 2020, pp. 24-28. 10.1109/ICIMCIS51567.2020.9354330.

LXIV. Y. A. Baker El-Ebiary et al., "Blockchain as a decentralized communication tool for sustainable development," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 127-133. 10.1109/ICSCEE50312.2021.9497910.

LXV. Y. A. Baker El-Ebiary et al., "E-Government and E-Commerce Issues in Malaysia," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 153-158. 10.1109/ICSCEE50312.2021.9498092.

LXVI. Y. A. Baker El-Ebiary et al., "Mobile Commerce and its Apps - Opportunities and Threats in Malaysia," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 180-185. 10.1109/ICSCEE50312.2021.9498228.

LXVII. Y. A. Baker El-Ebiary et al., "Track Home Maintenance Business Centers with GPS Technology in the IR 4.0 Era," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 134-138. 10.1109/ICSCEE50312.2021.9498070.

LXVIII. Y. M. A. Tarshany, Y. Al Moaiad and Y. A. Baker El-Ebiary, "Legal Maxims Artificial Intelligence Application for Sustainable Architecture And Interior Design to Achieve the Maqasid of Preserving the Life and Money," 2022 Engineering and Technology for Sustainable Architectural and Interior Design Environments (ETSAIDE), 2022, pp. 1-4. 10.1109/ETSAIDE53569.2022.9906357.

LXIX. Yaqoob, I., Hashem, I. A. T., Ahmed, E., Kazmi, S. A., Hong, C. S., & Ahmed, A. (2017). Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. Future Generation Computer Systems, 76, 265-275. 10.1016/j.future.2018.09.058

LXX. Yousef Methkal Abd Algani, B. Nageswara Rao, Chamandeep Kaur, B. Ashreetha, K. V. Daya Sagar and Yousef A. Baker El-Ebiary, “A Novel Hybrid Deep Learning Framework for Detection and Categorization of Brain Tumor from Magnetic Resonance Images” International Journal of Advanced Computer Science and Applications (IJACSA), 14(2), 2023. 10.14569/IJACSA.2023.0140261.