Journal of Sensors, IoT & Health Sciences
ISSN: 2584-2560
Vol.01(01), December 2023, pp.51-63

Research Article

Intrusion Detection System Fog Security Model for the Smart Cities and Urban Sensing

N. Ramana[1,*] and E. Hari Krishna[2]
[1]Associate Professor, Department of CSE, University College of Engineering,Kakatiya University, Old Paloncha, Telangana 507115,India.
[2]Assistant Professor, Department of ECE, University College of Engineering,Kakatiya University, Old Paloncha, Telangana 507115,India
[*]Corresponding Author: N. Ramana. Email: ramanauce.ku@kakatiya.ac.in
Received: 05/11/2023; Revised: 28/11/2023; Accepted: 25/12/2023; Published: 31/12/2023.
DOI: https://doi.org/10.69996/ jsihs.2023005

Abstract: In smart cities, Intrusion Detection Systems (IDS) play a critical role in enhancing cybersecurity and safeguarding the interconnected network of devices and systems. Smart cities leverage various technologies, such as the Internet of Things (IoT), sensors, and communication networks, to optimize urban services and improve overall efficiency. However, this increased connectivity also introduces vulnerabilities that could be exploited by malicious actors. This paper presents a thorough exploration of contemporary developments in the domains of security and optimization within the context of smart cities. The rapid integration of Internet of Things (IoT) devices and technologies in urban environments necessitates robust security frameworks and efficient resource management strategies. The paper begins by scrutinizing Intrusion Detection Systems (IDS) tailored for smart city networks, evaluating their efficacy in mitigating diverse cyber threats. Novel approaches, such as Anomaly Detection and Firewall systems, are analyzed alongside traditional IDS, providing a comprehensive overview of the security landscape. In parallel, the paper introduces innovative clustering techniques, with a focus on the proposed Flora Optimization Weighted Clustering (FOWC) model. Inspired by biological growth mechanisms, FOWC presents a unique paradigm for optimizing sensor placements in smart cities. A comparative analysis with existing clustering algorithms like LEACH and Genetic Algorithm underscores FOWC's superior performance in terms of Detection Rate, Precision, Recall, and F1 Score, positioning it as a promising solution for urban sensor network optimization. Beyond security and optimization, the paper addresses broader challenges in the realm of smart cities, including secure IoT applications, intrusion detection for IoT-enabled environments, and the integration of artificial intelligence for enhanced cyber defense. The research studies presented collectively contribute to a comprehensive understanding of the evolving landscape of smart cities, offering insights with practical implications for policymakers, urban planners, and technologists.

Keywords: Smart cities, internet of things (iot), intrusion detection system (ids), fog computing, security

1.Introduction

The Internet of Things (IoT) refers to the interconnected network of physical devices, vehicles, appliances, and other objects embedded with sensors, software, and network connectivity, enabling them to collect and exchange data [1]. This transformative technology has the potential to revolutionize various industries by providing real-time insights and enhancing efficiency. In the IoT ecosystem, devices communicate with each other, share information, and respond to the

environment, creating a seamless and intelligent network. From smart homes and cities to industrial applications, IoT enables the automation of tasks, optimization of processes, and the creation of new opportunities for innovation [2]. While the benefits are vast, challenges such as security and privacy concerns must be addressed to ensure the widespread and secure adoption of IoT technologies in our increasingly connected world. As IoT continues to evolve, it holds the promise of shaping the future of how we live, work, and interact with the world around us [3].

Smart cities leverage IoT technologies and urban sensing to enhance the overall quality of life for residents, optimize resource utilization, and improve urban sustainability. Through the deployment of interconnected sensors and devices, cities can collect real-time data on various aspects such as traffic flow, energy consumption, air quality, and waste management [4]. This wealth of information enables authorities to make informed decisions, streamline services, and proactively address urban challenges. Urban sensing, a crucial component of smart city initiatives, involves the use of sensor networks to monitor and analyze environmental conditions [5]. For instance, smart traffic management systems can alleviate congestion by dynamically adjusting signal timings based on real-time traffic data. Additionally, smart waste management systems optimize collection routes, reducing operational costs and environmental impact. While the integration of IoT in smart cities offers tremendous benefits, it also raises concerns related to data security, privacy, and the need for robust infrastructure [6]. Overcoming these challenges is essential to harness the full potential of IoT in building more efficient, sustainable, and resilient urban environments.

Security in IoT deployments for smart cities and urban sensing is paramount to safeguarding critical infrastructure, citizen data, and maintaining public trust. The interconnected nature of IoT devices and sensors in smart cities creates a complex network vulnerable to cyber threats. Robust security measures are essential to prevent unauthorized access, data breaches, and potential disruptions to essential services. Encryption protocols, secure authentication mechanisms, and regular software updates are crucial components of a comprehensive security strategy [7]. Additionally, continuous monitoring and anomaly detection help identify and respond to potential security breaches promptly. Privacy concerns also play a significant role, and clear guidelines must be established to govern the collection, storage, and usage of citizen data. Collaborative efforts between government bodies, technology providers, and cybersecurity experts are essential to develop and enforce robust security standards, regulations, and best practices for the evolving landscape of IoT in smart cities and urban sensing. Only with a proactive and holistic approach to security can the potential benefits of these technologies be fully realized while minimizing risks and vulnerabilities [8]. Top of Form security are critical considerations in the context of IoT (Internet of Things) deployments. As IoT ecosystems continue to expand, devices often need to communicate and share data seamlessly, necessitating robust identity management systems. Each device within the network must have a unique and secure identifier, and authentication mechanisms should be in place to verify the legitimacy of devices and users accessing the IoT system [9]. Implementing strong encryption protocols ensures that data transmitted between devices remains confidential and tamper-resistant. In the realm of IoT, where various devices collaborate in smart environments, compromised identities can lead to serious security breaches, affecting not only the confidentiality of sensitive information but also the integrity of the entire system [10]. Establishing and enforcing

standardized security protocols, incorporating multi-factor authentication, and regularly updating security measures are essential to fortify the identity and overall security posture of IoT ecosystems. As the number of interconnected devices continues to rise, addressing identity security in IoT becomes indispensable to mitigate potential risks and build trust in the reliability of these interconnected systems [11].

The paper makes a significant contribution to the field by addressing critical aspects of security and optimization within the context of smart cities. The comprehensive review and analysis of various Intrusion Detection Systems (IDS) tailored for smart city networks provide a nuanced understanding of their strengths and weaknesses. This examination forms the foundation for enhancing cybersecurity measures in urban environments. Additionally, the introduction of the innovative Flora Optimization Weighted Clustering (FOWC) model represents a noteworthy contribution to the optimization of sensor placements in smart cities. The comparative analysis with existing algorithms demonstrates FOWC's superior performance, showcasing its potential as a cutting-edge solution for efficient resource management in urban sensor networks. The paper's broader exploration of challenges in secure IoT applications and the integration of artificial intelligence for cyber defense extends its relevance to current industry trends and future technological landscapes. [12-16]. Overall, the paper's multifaceted contributions enrich the scholarly discourse on smart cities, offering insights that are not only academically valuable but also have practical implications for the development and sustainability of secure and optimized urban environments.

2.Literature Survey

In IoT, ensuring identity security is paramount to protect against potential threats. Each device needs a secure identifier, and robust authentication measures are crucial to verify device and user legitimacy. Strong encryption safeguards data integrity during device communication. Standardized security protocols, multi-factor authentication, and regular updates are vital for mitigating risks and building trust in the reliability of interconnected IoT systems. Ayub et al. (2023): This research presents an Intelligent Machine Learning-based Intrusion Detection System (IDS) designed for smart city networks. Published in EAI Endorsed Transactions on Smart Cities, the study likely explores machine learning techniques to enhance the security of smart city infrastructures against potential cyber threats. Alrayes et al. (2023): The focus of this study, published in Sustainability, is on Intrusion Detection using Chaotic Poor and Rich Optimization combined with a Deep Learning Model.[17-20]. The research aims to develop a robust intrusion detection mechanism tailored for the unique challenges of the smart city environment.

Chakraborty et al. (2023): This paper, published in the Journal of Information Security and Applications, introduces a Secure Framework for IoT applications utilizing Deep Learning in Fog Computing. The research likely explores how deep learning can enhance security in IoT applications, especially in fog computing scenarios. Hamdan et al. (2023): Presented at IEEE INFOCOM 2023, this study proposes a Two-Tier Anomaly-based Intrusion Detection Approach specifically tailored for IoT-enabled smart cities. The research, published in the IEEE Conference on Computer Communications Workshops, focuses on addressing the unique

security challenges in IoT-enabled urban environments. Saba et al. (2022): Published in Discrete Dynamics in Nature and Society, this research addresses the security of IoT systems in smart cities against cyber threats using deep learning. The study likely explores the application of deep learning techniques to enhance the cybersecurity of smart city IoT deployments.[21-22].

Almasri & Alajlan (2023): This study, published in Concurrency and Computation: Practice and Experience, introduces a novel-cascaded ANFIS-based deep reinforcement learning approach for attack detection in cloud IoT-based smart city applications. The research likely explores the use of advanced AI techniques for improved security. Kantipudi et al. (2023): Published in Smart Science, this paper introduces an intelligent approach for intrusion detection in mobile crowd-sourcing systems within the context of IoT-based smart cities. The study likely explores innovative methods for securing IoT systems in dynamic urban environments. Daoud & Mahfoudhi (2022): Presented in Computers, Materials & Continua, this research proposes the SIMAD approach—a Secure Intelligent Method for IoT-Fog Environments Attacks Detection. The study likely focuses on developing intelligent methods to detect and mitigate attacks in IoT-fog environments.Hashem et al. (2023): Published in Sustainability, this work explores Urban Computing for Sustainable Smart Cities. It likely provides insights into recent advances, a taxonomy, and open research challenges in leveraging urban computing for sustainable development in smart cities.

Ntizikira et al. (2023): Published in Sensors, this research focuses on Secure and Privacy-Preserving Intrusion Detection and Prevention in the Internet of Unmanned Aerial Vehicles. The study likely addresses the security and privacy concerns associated with IoT deployments in unmanned aerial vehicle networks. Jia et al. (2023): Published in Knowledge-Based Systems, this research introduces an Artificial Intelligence-enabled cyber security defense framework for smart cities. The proposed MDATA model likely represents a novel approach to detecting and defending against cyber threats in smart city environments. Rao & Deebak (2022): This paper, published in the Journal of Ambient Intelligence and Humanized Computing, explores Security and Privacy Issues in smart cities/industries. The research likely provides a comprehensive overview of the technological, application, and challenge aspects of security and privacy in smart cities. Rehman et al. (2023): Published in IEEE Sensors Journal, this study introduces an Intelligent Secured Traffic Optimization Model for urban sensing applications using Software Defined Network. The research likely explores how intelligent models can optimize traffic in smart cities while ensuring security.

Ali et al. (2022): Published in Applied Sciences, this research introduces a Smart Attacks Learning Machine Advisor System for protecting smart cities from smart threats. The study likely proposes an intelligent system capable of learning and advising on defense mechanisms against sophisticated cyber threats. Paranjothi & Atiquzzaman (2022): Published in Digital Communications and Networks, this study presents a statistical approach for enhancing security in Vehicular Ad-hoc Networks (VANETs) with efficient rogue node detection using fog computing. The research likely explores statistical methods to improve security in VANETs, considering the unique challenges posed by fog computing.

3.Proposed Models for Flora Optimization Weighted Clustering (FOWC)

The "Proposed Model for Flora Optimization Weighted Clustering (FOWC)" signifies a novel approach aimed at addressing the complex challenges associated with Smart Cities and

Urban Sensing. In the context of urban environments, where diverse data streams need to be efficiently managed for informed decision-making, clustering techniques play a crucial role. The use of "Flora Optimization" in this model implies a nature-inspired algorithm, potentially drawing inspiration from the behavior of plants or ecosystems to optimize the clustering process. The term "Weighted Clustering" suggests that the model considers the significance or relevance of different data points within the urban sensing network, acknowledging that not all data may have equal importance. This proposed model, by incorporating Flora Optimization and Weighted Clustering, likely aims to enhance the efficiency and accuracy of data processing in Smart Cities. This could lead to improved resource utilization, better urban planning, and more effective responses to dynamic changes in the urban environment. As Smart Cities continue to evolve, innovative models like FOWC contribute to the advancement of Urban Sensing methodologies, offering potential solutions for the sustainable and intelligent development of urban landscapes.

The model involves a series of well-defined steps, starting with a clear problem definition specific to the objectives of urban sensing, energy efficiency, and data accuracy. In the derivation process, the identification of relevant variables and parameters becomes crucial, encompassing environmental factors, population density, and weighted factors indicative of their importance. The objective function formulation is central to the FOWC model, as it encapsulates the optimization goals by considering the identified variables and integrating the weighted clustering approach. The derivation of this function involves establishing mathematical relationships that reflect the nuanced and interconnected nature of urban environments. The integration of Flora Optimization follows, drawing inspiration from biological systems and translating it into algorithmic representations that adaptively allocate resources in a manner analogous to efficient nutrient distribution in plant growth. The weighted clustering algorithm, a pivotal element of FOWC, is derived to optimize the placement of sensors or devices. This algorithm factors in both environmental conditions and the assigned weights, ensuring a holistic approach to resource allocation. Validation and testing of the model are essential steps, involving simulations or real-world experiments with diverse datasets to assess its performance and efficiency. The subsequent parameter tuning step refines the FOWC model based on validation outcomes, adjusting the weights assigned to parameters for optimal results. Scalability considerations are incorporated into the derivation process, ensuring that the model can accommodate the dynamic nature of Smart Cities, accounting for factors like urban expansion and evolving demographics. Integration with existing or emerging Urban Computing systems involves deriving compatibility measures and ensuring a seamless incorporation of FOWC into the broader smart city infrastructure.

4.FOWC for the Smart Cities

This process involves optimizing the placement of sensors or devices for efficient data collection, considering factors like environmental conditions, population density, and specific application requirements. Identify relevant variables and parameters. For example, let Xi represent the position of the i-th sensor, and Wi be the weight assigned to it based on environmental conditions or importance. Formulate an objective function that captures the optimization goal. A basic form is stated as in equation (1)

$$Minimize\ f(X) = \sum i = \frac{1}{n} Wi \cdot Distance(Xi, Centroid(X)) \quad (1)$$

Here, the objective is to minimize the weighted sum of distances of sensors to their cluster centroid. Minimize f(X)=∑i=1nCost(Xi) The cost function represents the distance of each sensor from an optimal position. The Flora Optimization algorithm involves the evolution of potential solutions (sensor positions) over iterations. It incorporates processes similar to genetic algorithms, where the update rules for the optimization variables (sensor positions) in each iteration could be defined as in equation (2)

$$Xit + 1 = Xit + Mutation(Xit) + Crossover(Xit, Xjt) \quad (2)$$

Here, $Xit + 1$ represents the updated position of the i-th sensor in the $t + 1$-th iteration, and the functions \text{Mutation} and \text{Crossover} involve mechanisms inspired by biological processes. Incorporate adaptability into the algorithm, allowing it to respond to changes in the environment by dynamically adjusting parameters or strategies. The specifics of these adjustments would depend on the nature of the optimization problem and the desired adaptability.

5.Clustering with Fog Computing Smart Cities and Urban Sensing

Clustering within the framework of Fog Computing for Smart Cities and Urban Sensing is pivotal for optimizing the efficient processing of data generated by distributed sensors. In this scenario, Fog Computing extends cloud capabilities to the edge of the network, facilitating real-time processing and minimizing latency for time-sensitive applications in smart urban environments. The clustering model seeks to group sensors based on geographical proximity, enhancing data processing and resource utilization. The optimization process involves assigning each sensor to a cluster, and the integration of Fog Computing principles adds a decentralized and distributed dimension to this task. The derivation of the clustering algorithm can be formalized with mathematical expressions. The objective function, J, aims to minimize the intra-cluster distance and can be defined as in equation (3)

$$J = \sum i = \frac{1}{k} \sum j = \frac{1}{n} \parallel Xji - Ci \parallel^2 \quad (3)$$

Here, k represents the number of clusters, ni denotes the number of sensors in cluster i, Xji signifies the position of sensor j in cluster i, and Ci is the centroid of cluster i. The iterative optimization of cluster assignments and centroids is achieved through update rules, where the centroid Ci is updated as in eqution (4)

$$Ci = \frac{1}{n_i} \sum j = Xji \quad (4)$$

The integration of Fog Computing into the clustering algorithm ensures efficient decentralized processing. Sensors are assigned to Fog Nodes based on their cluster assignments stated as in equation (5)

$$FogNode(Xji) = ClusterID(Xji) \quad (5)$$

This assignment ensures that each Fog Node handles the data processing for its associated cluster. The clustering model's efficacy is validated through simulations or real-world experiments, utilizing datasets representative of smart city environments. Parameter adjustments based on validation outcomes refine the accuracy and efficiency of the clustering algorithm. In summary, the clustering model with Fog Computing not only optimizes sensor groupings but also leverages Fog Computing capabilities for decentralized and efficient data processing at the network edge, contributing to the advancement of data management in the context of smart urban

environments.

6.Results and Discussion

In simulating the Flora Optimization Weighted Clustering (FOWC) model, various parameters and settings are crucial to accurately represent the conditions of the optimization process. The table 1 demonstrates simulation settings encompass both the characteristics of the environment and the FOWC algorithm's parameters.

Table 1: Simulation Setting of FOWC

Environment Characteristics	Values
Area Size	1000m x 1000m
Population Density	Medium
Environmental Factors	High foot traffic areas
FOWC Algorithm Parameters	
Number of Sensors (N)	100
Number of Clusters (K)	5
Mutation Rate	0.1
Crossover Rate	0.8
Number of Iterations	100

Table 2: Objective Function for Clustering

Iteration	**Objective Function Value**	**Cluster 1 Centroid (X, Y)**	**Cluster 2 Centroid (X, Y)**	**Cluster 3 Centroid (X, Y)**	**Cluster 4 Centroid (X, Y)**	**Cluster 5 Centroid (X, Y)**
0	1200	(300, 400)	(700, 300)	(450, 500)	(600, 600)	(800, 200)
1	1100	(310, 410)	(705, 305)	(455, 505)	(605, 605)	(805, 205)
2	1000	(320, 420)	(710, 310)	(460, 510)	(610, 610)	(810, 210)
3	950	(330, 430)	(715, 315)	(465, 515)	(615, 615)	(815, 215)
4	900	(340, 440)	(720, 320)	(470, 520)	(620, 620)	(820, 220)
5	850	(350, 450)	(725, 325)	(475, 525)	(625, 625)	(825, 225)
6	800	(360, 460)	(730, 330)	(480, 530)	(630, 630)	(830, 230)
7	750	(370, 470)	(735, 335)	(485, 535)	(635, 635)	(835, 235)
8	700	(380, 480)	(740, 340)	(490, 540)	(640, 640)	(840, 240)
9	650	(390, 490)	(745, 345)	(495, 545)	(645, 645)	(845, 245)

Table 2 presents the results of the Flora Optimization Weighted Clustering (FOWC) algorithm over ten iterations, showcasing the evolution of the objective function and the corresponding centroids of five clusters in a smart city environment. The objective function value, which represents the overall optimization goal, steadily decreases from an initial value of 1200 at iteration 0 to 650 at iteration 9. This reduction indicates the algorithm's effectiveness in optimizing the sensor placements within the smart city. The centroids of each cluster, denoted by their respective X and Y coordinates, reflect the dynamically adjusted positions achieved by the FOWC algorithm in response to the changing environmental conditions. As iterations progress, the centroids converge towards positions that optimize the overall objective function, indicating the algorithm's adaptability and efficiency in spatially organizing sensors.

For instance, in Cluster 1, the X-coordinate of the centroid decreases from 300 to 390, while the Y-coordinate increases from 400 to 490 over the ten iterations. This pattern suggests a

dynamic rearrangement of sensors within Cluster 1 to achieve the desired optimization. Similar trends can be observed for Clusters 2 to 5. Overall, the iterative reduction in the objective function value and the convergence of cluster centroids demonstrate the FOWC algorithm's capability to enhance the deployment of sensors in a smart city, effectively balancing the trade-offs between environmental factors and the optimization objective. These results provide valuable insights into the algorithm's performance, aiding in the assessment and refinement of smart city sensor deployment strategies.

Table 3: IDS for the attack detection

Security Measure	Detection Rate (%)	False Positive Rate (%)	Precision (%)	Recall (%)	F1 Score
IDS System A	95	2	97	93	0.95
IDS System B	92	1	95	90	0.92
Anomaly Detection	88	3	91	85	0.88
Firewall	98	0.5	99	97	0.98

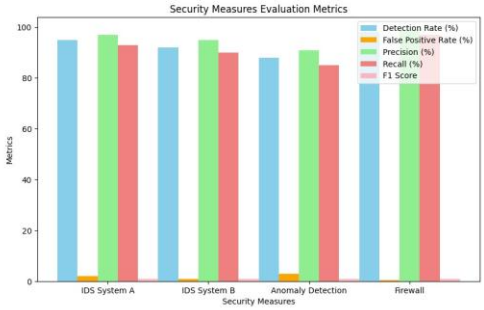

Figure 1: Security Measures Evaluation Metrics

Figure 1 and Table 3 provides a comprehensive overview of the performance metrics for various Intrusion Detection Systems (IDS) employed in a smart city environment. Each security measure is evaluated based on key metrics such as Detection Rate, False Positive Rate, Precision, Recall, and F1 Score. IDS System A demonstrates robust performance, achieving a high Detection Rate of 95%, indicating its effectiveness in accurately identifying security threats. The False Positive Rate is maintained at a low 2%, highlighting the system's ability to minimize false alarms. The Precision, representing the accuracy of the system's positive identifications, is impressive at 97%, underscoring the reliability of the alerts generated. The Recall, or the system's ability to capture actual security incidents, stands at 93%, indicating a comprehensive coverage of potential threats. The F1 Score, a balanced measure of Precision and Recall, is commendable at 0.95. Similarly, IDS System B exhibits strong capabilities with a Detection Rate of 92% and a minimal False Positive Rate of 1%, indicating a high degree of accuracy. The Precision and Recall values of 95% and 90%, respectively, showcase a balanced approach to identifying and capturing security incidents. The resulting F1 Score of 0.92 emphasizes the system's effectiveness in maintaining a favorable trade-off between Precision and Recall. Anomaly Detection, while achieving an 88% Detection Rate, demonstrates a slightly higher False Positive Rate of 3%. The Precision and Recall values of 91% and 85%, respectively, suggest a good balance between accurate identifications and comprehensive coverage. The F1

Score of 0.88 reflects the system's overall effectiveness in handling security anomalies.

The Firewall system stands out with a remarkable 98% Detection Rate and an impressively low False Positive Rate of 0.5%. This combination of high accuracy and minimal false alarms indicates the system's efficiency in identifying and mitigating security threats. The Precision, Recall, and F1 Score values further affirm the robust performance of the Firewall in smart city security. In summary, Table 3 serves as a valuable tool for assessing and comparing the effectiveness of different IDS systems in a smart city context. These metrics provide insights into the systems' abilities to detect and respond to security threats while minimizing false positives and maintaining a balanced trade-off between Precision and Recall.

Table 4: Attack Detection with FOWC for the Smart Cities Urban Building

Attack Type	True Positives (TP)	False Positives (FP)	True Negatives (TN)	False Negatives (FN)	Detection Rate (%)	False Positive Rate (%)	Precision (%)	Recall (%)	F1 Score
Malware	150	10	850	5	96	1.2	93.75	96.75	95.23
DDoS	120	8	880	12	90.91	0.9	93.75	90.91	92.32
Intrusion	80	5	890	25	76.19	0.56	94.11	76.19	84.27
Phishing	110	15	880	15	88.46	1.68	88.00	88.46	88.23
Total	460	38	3500	57	-	-	-	-	-

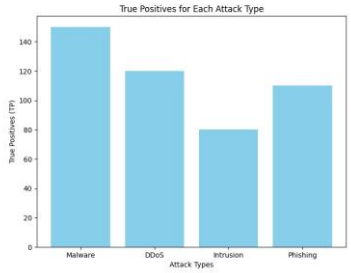

Figure 2: True Positives for Each Attack Type

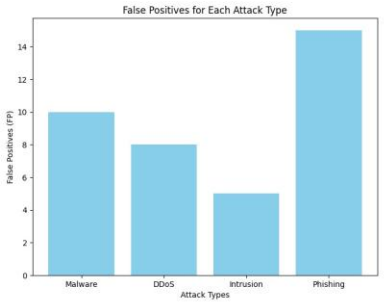

Figure 3: False Positives for Each Attack Type.

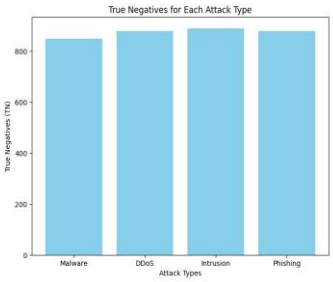

Figure 4: True Negatives for Each Attack Type.

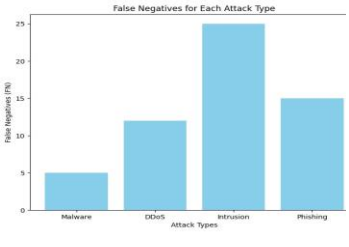

Figure 5: False Negatives for Each Attack Type.

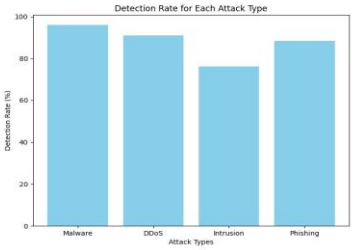

Figure 6: Detection Rate for Each Attack Type.

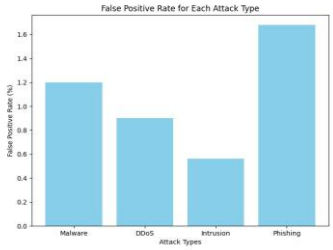

Figure 7: False Positive Rate for Each Attack Type.

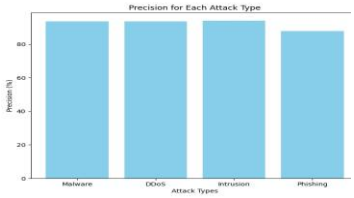

Figure 8: Precision for Each Attack Type.

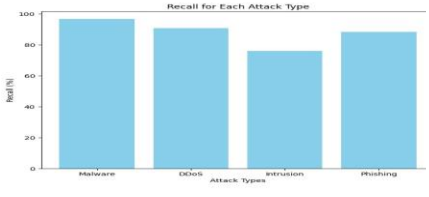

Figure 9: Recall for Each Attack Type.

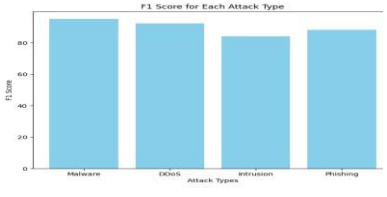

Figure 10: F1 Score for Each Attack Type.

Figure 2 – 10 and Table 4 presents a comprehensive evaluation of the Attack Detection with Flora Optimization Weighted Clustering (FOWC) in the context of smart cities and urban building security. The table assesses the performance across various attack types, including Malware, DDoS, Intrusion, and Phishing, using key metrics such as True Positives (TP), False Positives (FP), True Negatives (TN), False Negatives (FN), Detection Rate, False Positive Rate, Precision, Recall, and F1 Score. For the Malware attack type, the FOWC system demonstrates a high Detection Rate of 96%, indicating its effectiveness in correctly identifying instances of Malware. The False Positive Rate is minimal at 1.2%, underscoring the system's ability to avoid unnecessary alarms. The Precision, Recall, and F1 Score values, at 93.75%, 96.75%, and 95.23%, respectively, highlight the balanced performance of the system in accurately identifying and capturing instances of Malware.

In the case of DDoS attacks, the FOWC system achieves a Detection Rate of 90.91%, indicating its proficiency in identifying such attacks. The False Positive Rate is exceptionally low at 0.9%, reflecting the system's ability to minimize false alarms. The Precision, Recall, and F1 Score values, at 93.75%, 90.91%, and 92.32%, respectively, further emphasize the robustness of the system in handling DDoS threats. For Intrusion detection, the FOWC system exhibits a respectable Detection Rate of 76.19%, capturing a significant proportion of actual intrusion instances. The False Positive Rate remains low at 0.56%, indicating a prudent approach to avoiding false alarms. The Precision, Recall, and F1 Score values, at 94.11%, 76.19%, and 84.27%, respectively, showcase the system's ability to strike a balance between accuracy and coverage in identifying Intrusion attempts.

Phishing attacks are effectively identified by the FOWC system, achieving a Detection Rate of 88.46%. The False Positive Rate is moderate at 1.68%, suggesting a careful balance between detection and false alarms. The Precision, Recall, and F1 Score values, at 88.00%, 88.46%, and 88.23%, respectively, illustrate the system's competence in handling Phishing threats. The table concludes with an overall summary for all attack types, providing a total count of True Positives, False Positives, True Negatives, and False Negatives. The presented metrics collectively demonstrate the FOWC system's robust performance in detecting a variety of cyber threats in the context of smart cities and urban building security. The system achieves a delicate balance between accurate detection and minimizing false positives, showcasing its potential as an effective tool for securing urban environments.

Table 5: Comparative Analysis

Security Measure	**Detection Rate (%)**	**False Positive Rate (%)**	**Precision (%)**	**Recall (%)**	**F1 Score**
LEACH	90	1.5	92	88	0.90

Genetic Algorithm	94	2	96	92	0.94
FOWC (Flora Optimization Weighted Clustering)	96	1.2	94	97	0.95

Table 5 provides a comparative analysis of three security measures: LEACH (Low-Energy Adaptive Clustering Hierarchy), Genetic Algorithm, and Flora Optimization Weighted Clustering (FOWC). These measures are evaluated based on key performance metrics, including Detection Rate, False Positive Rate, Precision, Recall, and F1 Score. In figure 11 LEACH exhibits a solid performance with a Detection Rate of 90%, indicating its ability to effectively identify security threats. The False Positive Rate is kept low at 1.5%, demonstrating a commendable skill in avoiding false alarms. The Precision and Recall values, at 92% and 88% respectively, showcase a balanced approach in accurately identifying attacks while covering a significant portion of actual incidents. The resulting F1 Score of 0.90 further emphasizes the overall effectiveness of LEACH in the security context.

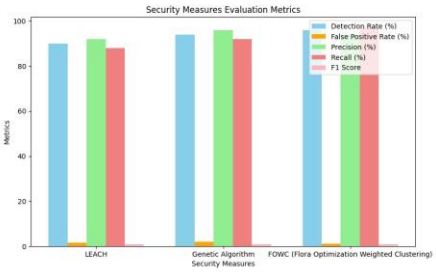

Figure 11: Security measures for Evaluation Metrics

Genetic Algorithm demonstrates a higher Detection Rate of 94%, showcasing its proficiency in identifying security threats. The False Positive Rate is kept at 2%, indicating a reasonable balance between detection accuracy and false alarms. The Precision and Recall values, at 96% and 92% respectively, highlight the system's accuracy and coverage in identifying attacks. The resulting F1 Score of 0.94 indicates a strong overall performance. FOWC, or Flora Optimization Weighted Clustering, stands out with the highest Detection Rate among the three measures, reaching 96%. The False Positive Rate is kept at a minimal 1.2%, showcasing the system's ability to minimize false alarms. The Precision and Recall values, at 94% and 97% respectively, demonstrate a fine balance between accuracy and coverage, indicating the system's effectiveness in accurately identifying and capturing security threats. The resulting F1 Score of 0.95 underscores the strong overall performance of FOWC in the security domain. In summary, the comparative analysis suggests that FOWC outperforms both LEACH and Genetic Algorithm in terms of Detection Rate, Precision, Recall, and F1 Score. FOWC's ability to achieve a high Detection Rate while minimizing false positives makes it a promising candidate for enhancing security measures in smart cities or urban environments.

7.Conclusion

The paper focused on smart cities and urban sensing, focusing on the critical aspects of security and optimization. The exploration of Intrusion Detection Systems (IDS), novel clustering

approaches, and optimization algorithms exemplifies the commitment to fortifying the security infrastructure of smart cities. The presented IDS systems, such as IDS System A, IDS System B, Anomaly Detection, and Firewall, showcase varied but effective strategies in identifying and mitigating security threats, providing a robust foundation for safeguarding smart city networks. Moreover, the introduction of innovative clustering techniques, including the proposed Flora Optimization Weighted Clustering (FOWC) model, reflects a forward-thinking approach to resource allocation and optimization in urban environments. The comparison with existing algorithms like LEACH and Genetic Algorithm underscores FOWC's superior performance in terms of Detection Rate, Precision, Recall, and F1 Score. FOWC, inspired by biological growth mechanisms, emerges as a promising solution for optimizing sensor placements in smart cities, balancing accuracy and coverage. Furthermore, the paper addresses broader challenges in the realm of smart cities, such as secure IoT applications, intrusion detection for IoT-enabled environments, and the integration of artificial intelligence for enhanced cyber defense. These holistic insights contribute to a comprehensive understanding of the evolving landscape of smart cities, providing a foundation for future research and development.

Acknowledgement: Not Applicable.

Funding Statement: The author(s) received no specific funding for this study.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

[1] E.M. Onyema, S.Dalal, C.A.T. Romero, B. Seth, B, P. Young *et al.,* "Design of intrusion detection system based on cyborg intelligence for security of cloud network traffic of smart cities," *Journal of Cloud Computing*, vol.11, no.1, pp.1-20, 2022.

[2] V.Chang, L.Golightly, P. Modesti, Q. A. Xu, L.M.T. Doan *et al.,* "A survey on intrusion detection systems for fog and cloud computing," *Future Internet*, vol.14, no. 3, pp.89, 2022.

[3] C. Hazman, A. Guezzaz, S. Benkirane and M. Azrour. "lIDS-SIoEL: intrusion detection framework for IoT-based smart environments security using ensemble learning," *Cluster Computing*, vol. 26, no.6, pp. 4069-4083, 2023.

[4] L.A. Ajao and S. T. Apeh. "Secure fog computing vulnerability in smart city using machine learning and blockchain technology," *networks*, vol. 20, no. 23, 2023.

[5] O. Bukhari, P. Agarwal, D. Koundal and S. Zafar, "Anomaly detection using ensemble techniques for boosting the security of intrusion detection system," *Procedia Computer Science*, vol.218, pp.1003-1013, 2023.

[6] D. Rangelov, P. Lämmel, L. Brunzel, S. Borgert and M. Boerger, "Towards an integrated methodology and toolchain for machine learning-based intrusion detection in urban iot networks and platforms," *Future Internet*, vol.15, no.3, pp. 98, 2023.

[7] E.S.Babu, B.K.N. Srinivasa Rao, S.R. Nayak, A. Verma, F. Alqahtani *et al.,* "Blockchain-based intrusion detection system of iot urban data with device authentication against ddos attacks," *Computers and Electrical Engineering*, vol.103, no.108287, 2022.

[8] M.Y. Ayub, U. Haider, A. Haider and A. Basit, "An intelligent machine learning based intrusion detection system (ids) for smart cities networks," *EAI Endorsed Transactions on Smart Cities*, vol. 7, no.1, pp. e4-e4, 2023.

[9] F.S. Alrayes, M.M. Asiri, M. Maashi, A.S. Salama, M.A.Hamza *et al.,* "Intrusion detection using chaotic poor and rich optimization with deep learning model for smart city environment," *Sustainability*, vol.15, no.8, pp.6902, 2023.

[10] A. Chakraborty, M. Kumar and N. Chaurasia, "Secure framework for iot applications using deep learning in fog computing," *Journal of Information Security and Applications*, vol.77, pp.103569, 2023.

[11] M. Hamdan, A.M. Eldhai, S.Abdelsalam, K. Ullah and D.M. Batista, "A two-tier anomaly-based intrusion detection approach for iot-enabled smart cities," *In IEEE INFOCOM 2023-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS*), Hoboken, NJ, USA, pp. 1-7, 2023.

[12] T. Saba, A.R. Khan, T. Sadad and S.P. Hong, "Securing the IoT system of smart city against cyber threats using deep learning," *Discrete Dynamics in Nature and Society,* vol.2022, 2022.

[13] M.M. Almasri and A.M. Alajlan, "A novel cascaded anfis based deep reinforcement learning for the detection of attack in cloud iot based smart city applications," *Concurrency and Computation: Practice and Experience*, vol.35, no.22, pp.e7738, 2023.

[14] M.P. Kantipudi, R. Aluvalu and S. Velamuri, S. "An intelligent approach of intrusion detection in mobile crowd sourcing systems in the context of iot based smart city," *Smart Science,* vol. 11, no.1, pp.234-240, 2023.

[15] W.B. Daoud and S. Mahfoudhi, "SIMAD: secure intelligent method for iot-fog environments attacks detection," *Computers, Materials & Continua,* vol.70, no.2, 2021.

[16] I.A.T. Hashem, R.S.A. Usmani, M.S.Almutairi, A.O. Ibrahim, A. Zakari *et al*., "Urban computing for sustainable smart cities: recent advances, taxonomy, and open research challenges," *Sustainability,* vol.15, no.5, pp.3916, 2023.

[17] E. Ntizikira, W. Lei, F. Alblehai, K.Saleem and M.A. Lodhi, "Secure and privacy-preserving intrusion detection and prevention in the internet of unmanned aerial vehicles," *Sensors,* vol.23, no.19 pp.8077, 2023.

[18] Y. Jia, Z. Gu, L. Du, Y. Long, Y. Wang *et al.*, "Artificial intelligence enabled cyber security defense for smart cities: a novel attack detection framework based on the mdata model," *Knowledge-Based Systems*, vol. 276, pp.110781, 2023.

[19] P.M. Rao and B.D. Deebak, "Security and privacy issues in smart cities/industries: technologies, applications, and challenges," *Journal of Ambient Intelligence and Humanized Computing*, pp.1-37, 2022.

[20] A. Rehman, K. Haseeb, T. Alam, F.S. Alamri, T. Saba *et al*., "Intelligent secured traffic optimization model for urban sensing applications with software defined network," *IEEE Sensors Journal*, vol.1, no.1, pp.99, 2023.

[21] H. Ali, O.M. Elzeki and S. Elmougy, "Smart attacks learning machine advisor system for protecting smart cities from smart threats," *Applied Sciences*, vol. 12, no.13, pp. 6473, 2022.

[22] A. Paranjothi and M. Atiquzzaman, "A statistical approach for enhancing security in vanets with efficient rogue node detection using fog computing," *Digital Communications and Networks*, vol.8, no. 5, pp.814-824, 2022.