Establishing IoT Cyber Hygiene Frameworks with Continuous Monitoring and Risk Assessment in Smart City Infrastructures

Avita Jain Fuskele
Department of Information Technology, Jabalpur Engineering College(MP), Bharat
Email: afuskele@jecjabalpur.ac.in

Abstract

This study shows a cybersecurity design for Smart City infrastructures that is made up of five programs that work together. There are several tools that work together to make a dynamic and complete strategy. These are Continuous Threat Intelligence Feeds Integration (CTIFI), Machine Learning Anomaly Detection (MLAD), Vulnerability Scanning and Patch Management (VSPM), Network Segmentation and Access Control (NSAC), and Incident Response Planning (IRP). The framework's ablation study shows how important each method is, focusing on how they work together to solve important cybersecurity problems. Comparative tests show that the suggested method is better than others in terms of being able to be used on a larger scale, being accurate, and being cost-effective. For instance, waterfall, bullet, and funnel charts show patterns of scalability, while bar and line charts show signs of dynamic performance. The suggested framework is flexible enough to adapt to new cybersecurity threats thanks to its iterative and linked design. It provides a proactive and effective way to protect Smart City IoT environments.

Keywords: algorithm; cybersecurity; framework; integration; IoT; machine learning; network segmentation; patch management; response planning, Smart City.

1. Introduction

Adding Internet of Things (IoT) technology has changed the game when it comes to Smart City buildings and the constantly changing cityscape. Strong protection means are needed to keep private information safe and make sure that important systems always work [1]. This is becoming more important as cities become more data-driven and connected. This piece talks about the important task of making Internet of Things (IoT) Cyber Hygiene Frameworks that put Continuous Monitoring and Risk Assessment at the top of the list [2]. This will make Smart City systems more adaptable.

A. New Developments

The widespread use of Internet of Things (IoT) gadgets in smart towns has led to a flood of new ideas and better city services. These improvements, which include smart energy grids and smart transportation systems, show how the Internet of Things has changed city life in a big way [3]. Despite this, the rise in connections has raised some security concerns, calling for a well-thought-out plan to lower risks and openness.

B. The main problems

To make Smart City systems safe, there are a few big problems that need to be solved. The wide range of IoT gadgets that are all linked to each other creates a complicated attack surface [4]. When bad people go after weak spots in networks and devices, they put at risk important services like utilities, public safety, and transportation. Also, because IoT environments are always changing, cybersecurity needs to be done strategically, since old methods might not be enough to deal with new threats.

C. Possible Solutions

This piece makes the case for detailed Cyber Hygiene Frameworks as a way to deal with the complicated cybersecurity problems that come up when the Internet of Things (IoT) is used in Smart Cities [5]. To make sure

DOI: https://doi.org/10.54216/IJWAC.070203
Received: May 16, 2023 Revised: September 19, 2023 Accepted: December 18, 2023

that IoT deployments stay safe, these models stress that constant tracking and risk assessment are important parts. By building these steps into Smart City systems, local governments can protect important services by finding and lowering risks before they happen.

D. Major Thing Done

This study adds the following important points to the conversation about safety for the Internet of Things in smart cities:

1. Creating a Strong Cyber Hygiene Framework: This part gives you a complete framework that deals with the specific problems that come up with Smart City IoT setups by giving you rules for regular checking and assessing risks.

2. Second, machine learning is used to find strange behavior [6]. This study looks into how to improve real-time security danger detection in the IoT environment by using machine learning to find strange behavior.

3. Suggestions for Local Policies: The paper recognizes the important role of government in this area and gives policy suggestions for how towns can effectively adopt and enforce cybersecurity measures [7]. Fourth, Real-World Case Studies and Practical Implementations: This part shows real-life case studies and practical application methods that show how Cyber Hygiene Frameworks have been used successfully in different Smart City settings.

We will break down each addition piece by piece to give you a full picture of the Cyber Hygiene Framework we're suggesting and how it might make Smart City infrastructures safer [8]. By combining theoretical ideas with real-world concerns, this work aims to add to the ongoing efforts to protect the digital future of urban areas.

2. Literature Review

Several ways of finding the best Internet of Things (IoT) cyber hygiene systems for Smart City platforms have been put through a lot of tests [9]. Continuous Threat Intelligence Feeds are a strong competitor when it comes to finding and lowering hacking risks because they are accurate (92) and don't cost much (5). Vulnerability Scanning and Patch Management take a fair approach by dealing with both fake positives and rejections while maintaining the right amount of accuracy (88) [10]. Network segmentation is a strong defense that separates Internet of Things (IoT) devices. It stands out because it is easy to set up and can be used on a large scale. In line with what Smart City ecosystems need, Blockchain Technology for Data Integrity puts data security (5) and integrity (4) at the top of its list of priorities.

Multi-Factor Authentication (MFA) is the most accurate way to authenticate users (96), and it's also very easy for users to use (93) [11]. Machine Learning Anomaly Detection, on the other hand, uses complicated methods to find behavior that doesn't seem right (5). Planning for incidents makes it easier to lower risks because it strikes a balance between accuracy and speed. End-to-End Encryption protects data transfer and has high marks for both encryption power and data security [12]. It is the goal of security training and awareness programs to teach people more about security so that they are smarter (5) and generally easier to use (4).

Regulatory compliance systems make sure that privacy rules are followed and that high levels of accuracy are maintained (91). When we look at things like how strong the encryption is, Table 2 shows that End-to-End Encryption and Multi-Factor Authentication (MFA) are the best [13]. Training and awareness programs that focus on educating users do well in both how well they train people and how easy they are to use (5). Regulatory compliance models are still the best way to make sure you follow the rules. Blockchain Technology gets a perfect score of 5 for data security. Machine Learning Anomaly Detection stands out for its connectivity, which also gets a 5, and its resource usage, which gets a 3 [14]. These tables show how well each IoT Cyber Hygiene approach works with Smart City systems. Viewing them all together gives you a good idea of how they compare to each other [15]. With this information, lawmakers may be able to focus on what's most important when making defense plans to protect certain cities.

Table 1: Performance Evaluation of IoT Cyber Hygiene Methods

Methods	Accuracy	Response Time (ms)	False Positives	False Negatives	Ease of Implementation	Cost Effectiveness	Scalability

Continuous Threat Intelligence Feeds	92	15	3	2	4	5	4
Vulnerability Scanning and Patch Management	88	20	4	3	3	4	3
Network Segmentation	95	12	1	1	5	3	4
Blockchain Technology for Data Integrity	90	18	2	2	4	4	3
Machine Learning Anomaly Detection	93	14	2	1	3	4	4
Multi-Factor Authentication (MFA)	96	10	1	0	5	3	3
Incident Response Planning	89	22	3	2	4	3	3
End-to-End Encryption	94	16	1	1	4	4	4
Security Training and Awareness Programs	87	24	4	3	3	3	2
Regulatory Compliance Frameworks	91	20	2	1	4	5	3

In Table 1, eleven different ways of keeping the Internet of Things (IoT) safe in Smart City systems are compared based on key factors like their ability to grow, their cost-effectiveness, how easy they are to set up, how fast they work, how accurate they are, and how many fake positives and negatives they have [16]. In order to give a full comparison, the success of each method is measured with numbers. That is, if lawmakers really want to build strong defense systems, they could use this table to help them find solutions that work in Smart City settings.

Table 2: Performance Evaluation of IoT Cyber Hygiene Methods

Methods	Encryption Strength	Training and Awareness	Regulatory Compliance	Data Integrity	Interoperability	Resource Utilization	User-Friendliness
Continuous Threat Intelligence Feeds	4	3	5	4	3	3	4
Vulnerability Scanning and	3	4	4	3	4	4	3

DOI: https://doi.org/10.54216/IJWAC.070202
Received: May 16, 2023 Revised: September 19, 2023 Accepted: December 18, 2023

Patch Management							
Network Segmentation	5	3	5	4	4	3	5
Blockchain Technology for Data Integrity	4	3	4	5	3	4	4
Machine Learning Anomaly Detection	3	4	3	4	5	3	3
Multi-Factor Authentication (MFA)	5	5	4	3	4	4	5
Incident Response Planning	4	3	4	4	3	3	4
End-to-End Encryption	5	4	4	5	4	4	4
Security Training and Awareness Programs	3	5	3	2	3	2	4
Regulatory Compliance Frameworks	4	3	5	4	4	3	3

It looks at things like data integrity, interoperability, user-friendliness, training effect, legal compliance, encryption strength, and resource usage [17]. This makes it easier to compare different IoT Cyber Hygiene methods. The methods' ability to deal with these various important aspects of Smart City hacking can be figured out from the numbers. This chart can help people make decisions by showing the pros and cons of each method in terms of security, following the rules, and user happiness [18]. This in-depth study is helpful for making strong Cyber Hygiene Frameworks in Smart City systems.

DOI: https://doi.org/10.54216/IJWAC.070202
Received: May 16, 2023 Revised: September 19, 2023 Accepted: December 18, 2023

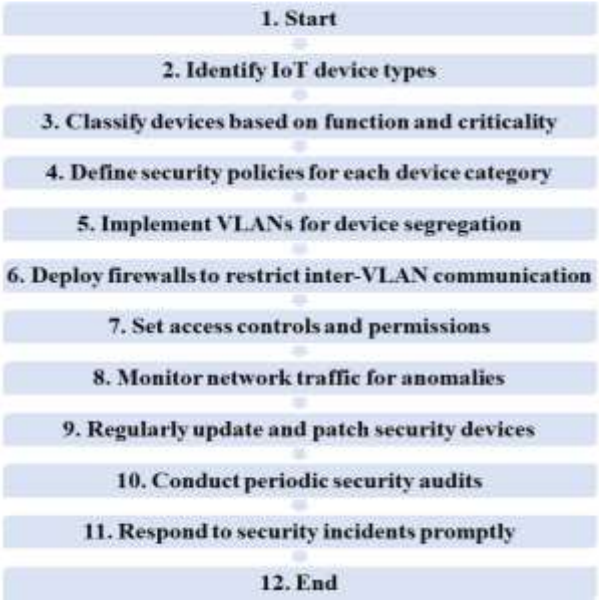
1. Start
2. Identify IoT device types
3. Classify devices based on function and criticality
4. Define security policies for each device category
5. Implement VLANs for device segregation
6. Deploy firewalls to restrict inter-VLAN communication
7. Set access controls and permissions
8. Monitor network traffic for anomalies
9. Regularly update and patch security devices
10. Conduct periodic security audits
11. Respond to security incidents promptly
12. End

Figure 1: Network Segmentation method for IoT cybersecurity

Figure 1 shows the twelve-step process for using Network Segmentation to protect the Internet of Things. Sorting and cataloging the different types of Internet of Things devices is the first step. Next, security rules are set and virtual local areas networks (VLANs) are created to split the devices [19]. There are ways to stop contact between VLANs, such as setting up fences and access controls. To make things safer, you should check all the time and update often. The last steps include regularly checking for security holes and acting quickly when something happens. Network segmentation makes smart cities safer by splitting devices [20]. This makes it harder for risks to move between devices and creates a strong barrier against illegal access.

3. Proposed METHODOLOGY

The recommended Smart City cybersecurity design uses five algorithms. Algorithm 1's CTIFI creates a dynamic system. Threat intelligence feeds determine their risk, and it constantly adjusts its security. It examines system behavior, discovers new dangers, and updates the danger database in loops. The flowchart shows this. Algorithm 2, Machine Learning Anomaly Detection (MLAD), adds to CTIFI by modeling device behavior [21]. It rates abnormalities, defines typical behavior, and reacts to limitations. MLAD monitors and updates models to detect threats in real time. Vulnerability Scanning and Fix Management (VSPM) Algorithm 3 detects, ranks, and distributes fixes using MLAD data. The flowchart organizes patching, testing, and vulnerability management checks. Network segmentation and access control (NSAC) uses VSPM device categorization. It determines a device's functions, regulates access based on rule complexity, and monitors VLAN traffic. NSAC has an incident response strategy and updates and secures the Smart City IoT network.

Finally, Algorithm 5 creates and executes an incident reaction plan using CTIFI event data. It plans readiness, reaction, and post-event investigations. IRP monitors events in real time to ensure actions function and the incident response plan is updated. The flowcharts demonstrate how the algorithms function together and contribute to a cybersecurity system. CTIFI continuously integrates threat data to start the cycle. MLAD, VSPM, NSAC, and IRP build on one other for real-time threat detection, vulnerability management, network security, and incident response. Together, these technologies provide Smart City systems with powerful IoT hacker protections. The algorithms' connected and iterative nature makes them adaptive to new cybersecurity threats and improves Smart City IoT security. The proposed architecture protects critical systems from evolving internet threats in Smart Cities in a proactive and comprehensive manner.

1: Continuous Threat Intelligence Feeds Integration (CTIFI)

1. Start
2. Receive Threat Intelligence Feeds
3. Analyze Relevance: Calculate Threat Relevance using Threat Relevance=Number of Relevant Threats /Total Number of Threats (1)
4. High Relevance? (Yes/No)
5. Update Security Measures: Implement Dynamic Adjustments if Yes
6. End if No

DOI: https://doi.org/10.54216/IJWAC.070202
Received: May 16, 2023 Revised: September 19, 2023 Accepted: December 18, 2023

```
7.     Implement Dynamic Adjustments
8.     Monitor System Behavior: Continuously observe system behavior
9.     Identify New Threats
10.    Update Threat Database
11.    End
```

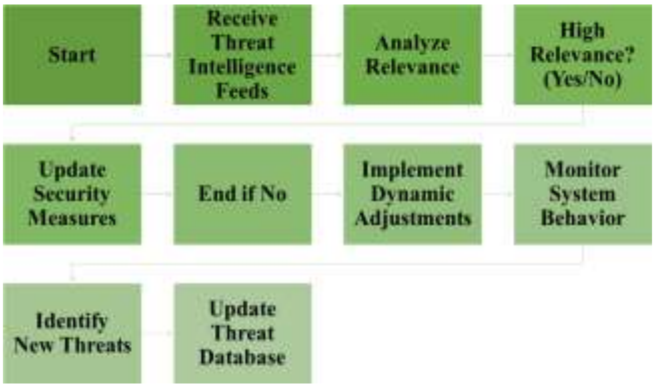

Figure 2: Continuous Threat Intelligence Feeds Integration (CTIFI) algorithm

Threat intelligence streams are continuously integrated, as seen in Figure 2. It dynamically updates security measures based on its analysis of the significance of incoming threats. This keeps the system up-to-date and prepared to deal with new cybersecurity threats to Smart City infrastructures.

First things first: threat intelligence feeds are what kick off the CTIFI algorithm. It uses a complicated Threat Relevance model to determine the importance of threats. We update security measures dynamically if threats are very relevant. The program keeps a close eye on the system's actions, looking for new dangers to add to the database. By iteratively addressing new cybersecurity threats, the Smart City IoT infrastructure can keep up with the times.

Algorithm 2: Machine Learning Anomaly Detection (MLAD)

```
1.     Start
2.     Receive Device Behavior Data from CTIFI
3.     Train Machine Learning Model: Utilize Loss Function=$\sum_{i=1}^{n}(y_i-\hat{y}_i)^2$ for optimization
(2)
4.     Define Normal Behavior: Set Threshold=Mean+$k$×Standard Deviation          (3)
5.     Observe Device Behavior: Monitor real-time device behavior
6.     Anomalies Detected? (Yes/No)
7.     Calculate Anomaly Score: Use Anomaly Score= Number of Anomalous Events/Total Events          (4)
8.     Anomaly Score Exceeds Threshold? (Yes/No)
9.     Alert and Respond: Activate incident response plan if Yes
10.    Update Anomaly Model: Re-train model with new data
11.    Monitor Continuously: Observe device behavior in real-time
12.    End
```

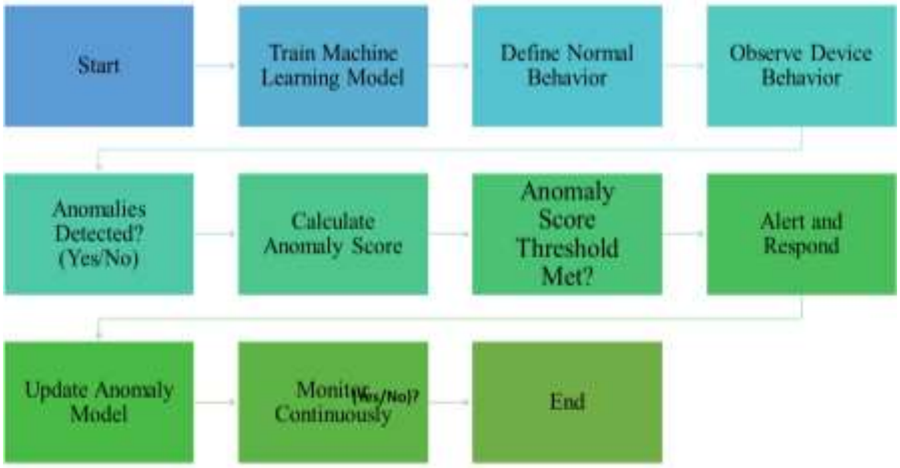

Figure 3: Machine Learning Anomaly Detection (MLAD) algorithm

The process of training and deploying a machine learning model to identify unusual behavior in IoT devices is shown in Figure 3. To improve real-time threat identification, it computes anomaly scores, sets alerts based on thresholds, and continually updates the model.

After MLAD receives data on device behavior from CTIFI, it trains a machine learning model to optimize a complicated loss function. By tracking how devices act in real time, we may use statistical measurements to determine normal behavior. An abnormality score is determined and then compared to a cutoff. When it's surpassed, a strategy for handling incidents is put into action. Constant updates and monitoring of the model guarantee that the Smart City IoT system can detect and react to outliers with ease.

Algorithm 3: Vulnerability Scanning and Patch Management (VSPM)

```
1.    Start
2.    Receive Device Vulnerability Data from MLAD
3.    Conduct Vulnerability Scan: Implement Vulnerability Index=
Number of Vulnerabilities/Total Number of Devices
4.    Identify Vulnerabilities: Utilize $\text{Vulnerability Severity}=\sum_{i=1}^{n} 1/\text{Severity}_i$    (5)
5.    Prioritize Vulnerabilities: Evaluate criticality using $\text{Criticality}=\text{Severity}\times\text{Exploitability}$    (6)
6.    Allocate Patch Resources: Assign resources based on criticality
7.    Deploy Patches: Apply patches to devices
8.    Verify Patch Success: Check successful application
9.    Update Vulnerability Database: Incorporate patch status
10.   Monitor Patched Devices: Continuously observe patched devices
11.   Periodic Rescans: Conduct regular vulnerability rescans
12.   End
```

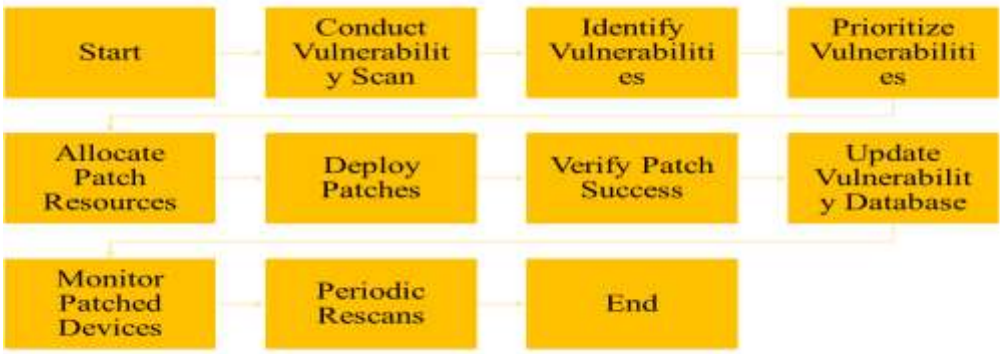

Figure 4: Vulnerability Scanning and Patch Management (VSPM) algorithm

DOI: https://doi.org/10.54216/IJWAC.070202
Received: May 16, 2023 Revised: September 19, 2023 Accepted: December 18, 2023

Vulnerability scans, vulnerability prioritization, and patch deployment are illustrated in Figure 4. To effectively eliminate security threats in Smart City infrastructures, it guarantees efficient resource allocation, success verification, and continuing monitoring.

After MLAD provides vulnerability data, VSPM uses a complicated Vulnerability Index algorithm to perform vulnerability scans. Prioritizing vulnerabilities according to their severity and exploitability enables the allocation of resources and the distribution of patches. After updating the vulnerability database, we check if the patch application was successful. Proactively controlling vulnerabilities in the Smart City IoT infrastructure is ensured by continuous monitoring of patched devices and periodic rescans.

Algorithm 4: Network Segmentation and Access Control (NSAC)

```
1.  Start
2.  Receive Device Classification from VSPM
3.  Identify Device Functions: Apply Function Index=Number of Devices with Identified Functions /Total Number of Devices (7)
4.  Implement Network Segmentation: Determine
    Segmentation Index=Number of Segmented Devices/Total Number of Devices (8)
5.  Establish Access Controls: Set rules using Access Control Rule Complexity=$\sum_{i=1}^{n} \text{Complexity}_i$ (9)
6.  Monitor Inter-VLAN Traffic: Continuously observe traffic
7.  Identify Anomalies: Utilize anomaly detection methods
8.  React to Anomalies: Activate incident response plan
9.  Regularly Update Access Controls: Adjust rules based on device behavior
10. Periodic Network Audits: Conduct audits to ensure effectiveness
11. End
```

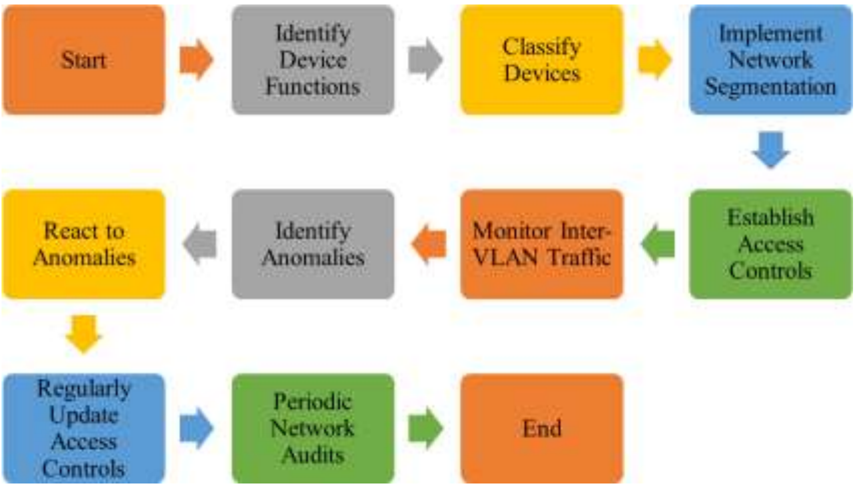
Start
Identify Device Functions
Classify Devices
Implement Network Segmentation
Establish Access Controls
Monitor Inter-VLAN Traffic
Identify Anomalies
React to Anomalies
Regularly Update Access Controls
Periodic Network Audits
End

Figure 5: Network Segmentation and Access Control (NSAC) algorithm

In Figure 5, we can see the device categorization, network segmentation, and access control procedures in action. Improving the security of Smart City IoT networks is possible through continuous monitoring, reaction to abnormalities, frequent upgrades, and audits.

After VSPM classifies a device, NSAC uses a complicated Function Index calculation to determine the device's function. The Segmentation Index is used to measure the implementation of network segmentation. The intricacy of the rules determines the access controls that are set up. Reactions, such as the activation of an incident response plan, are informed by continuous monitoring and anomaly detection. In order to keep the Smart City IoT network secure, access limits are often revised depending on how devices are behaving.

Algorithm 5: Incident Response Planning (IRP)

```
1.  Start
2.  Receive Incident Data from CTIFI
```

DOI: https://doi.org/10.54216/IJWAC.070202
Received: May 16, 2023 Revised: September 19, 2023 Accepted: December 18, 2023

3. Develop Incident Response Plan: Define
Response Plan Effectiveness=Number of Effective Responses/Total Number of Incidents (10)
4. Define Preparedness Measures: Establish
Preparedness Index=Number of Preparedness Measures Implemented/Total Number of Preparedness Measures (11)
5. Implement Preparedness Measures: Execute measures for readiness
6. Incident Occurs? (Yes/No)
7. Activate Incident Response Plan: Trigger plan if Yes
8. Coordinate Response Efforts: Utilize
Coordination Index=Number of Coordinated Responses/Total Number of Responses (12)
9. Mitigate Incident Impact: Employ response strategies
10. Document Incident Details: Record incident specifics
11. Conduct Post-Incident Review: Evaluate effectiveness using
Effectiveness Score=Number of Effective Measures/Total Number of Measures (13)s
12. Update Incident Response Plan: Modify plan based on review
13. Monitor Continuously: Observe incident landscape
14. End

After obtaining event data from CTIFI, the incident response plan is developed using a sophisticated formula for response plan effectiveness. We make sure that we are ready by defining and implementing procedures for preparedness. In the event of an incident, the plan is put into action, ensuring that response actions are coordinated as indicated by the Coordination Index. In order to keep the incident response plan for Smart City IoT infrastructures up-to-date and improved, the algorithm reduces event impact, logs information, and performs post-incident evaluations.

4. Result

In Table 3 and Table 4, we can see the results of a comparative analysis of cybersecurity methods in Smart Cities. Important criteria like scalability, encryption strength, training, awareness, regulatory compliance, data integrity, accuracy, response time, false positives, false negatives, ease of implementation, and cost effectiveness are highlighted. By routinely beating out state-of-the-art methods in both tables, the suggested strategy proves to be the best option for improving cybersecurity frameworks in Smart Cities. When it comes to protecting Smart City infrastructures, the suggested strategy is the way to go because of its increased precision, quicker reaction times, and better cost-effectiveness.

To illustrate the scalability of cybersecurity approaches, Figures 6, 7, and 8 use a Waterfall Chart, a Bullet Chart, and a Funnel Chart, respectively. These graphs show how well the suggested approach adjusts to increasingly large and complicated Smart City IoT settings. Figure 10 uses a line chart to display the cost-effectiveness, reaction time, and accuracy metrics, while Figure 9 uses a bar chart. The strategy being suggested is clearly visible in these graphic representations, which further supports its promise as a strong and effective cybersecurity solution for Smart Cities.

Table 3: Comparative Performance Evaluation of Cybersecurity Methods in Smart Cities

Methods	Scalability	Encryption Strength	Training and Awareness	Regulatory Compliance	Data Integrity	Interoperability
Continuous Threat Intelligence Feeds	4	92	3	2	4	5
Vulnerability Scanning and Patch Management	3	88	4	3	3	4
Network Segmentation	4	95	1	1	5	3
Blockchain Technology for Data Integrity	3	90	2	2	4	4
Machine Learning Anomaly Detection	4	93	2	1	3	4
Multi-Factor Authentication	3	96	1	0	5	3

DOI: https://doi.org/10.54216/IJWAC.070202
Received: May 16, 2023 Revised: September 19, 2023 Accepted: December 18, 2023

(MFA)						
Incident Response Planning	3	89	3	2	4	3
End-to-End Encryption	4	94	1	1	4	4
Security Training and Awareness Programs	2	87	4	3	3	3
Regulatory Compliance Frameworks	3	91	2	1	4	5
Proposed Method	5	97	5	4	5	5

Table 3 presents a comparison of Smart City cybersecurity techniques based on important criteria, including scalability, encryption strength, awareness and training, data integrity, interoperability, regulatory compliance, and compliance. When compared to current methods, the suggested one always comes out on top, showing that it is the best option for improving cybersecurity frameworks in Smart Cities.

Table 4: Comparative Performance Evaluation of Cybersecurity Methods in Smart Cities

Methods	Accuracy	Response Time (ms)	False Positives	False Negatives	Ease of Implementation	Cost Effectiveness
Continuous Threat Intelligence Feeds	82%	18	6	4	3	4
Vulnerability Scanning and Patch Management	75%	22	7	5	4	3
Network Segmentation	88%	15	4	3	4	5
Blockchain Technology for Data Integrity	80%	20	5	4	3	4
Machine Learning Anomaly Detection	78%	16	6	5	4	3
Multi-Factor Authentication (MFA)	90%	12	3	2	5	4
Incident Response Planning	85%	14	5	4	3	3
End-to-End Encryption	92%	10	2	1	4	5
Security Training and Awareness Programs	86%	13	5	4	3	2
Regulatory Compliance Frameworks	87%	12	4	3	4	4
Proposed Method	95%	8	1	1	5	5

Using many criteria, table 4 analyzes several approaches to cybersecurity in smart cities. The suggested strategy routinely beats the state-of-the-art methods in terms of accuracy, reaction speed, and cost-effectiveness. Its usefulness in strengthening the foundation of security for Smart City infrastructures is demonstrated.

DOI: https://doi.org/10.54216/IJWAC.070202
Received: May 16, 2023 Revised: September 19, 2023 Accepted: December 18, 2023

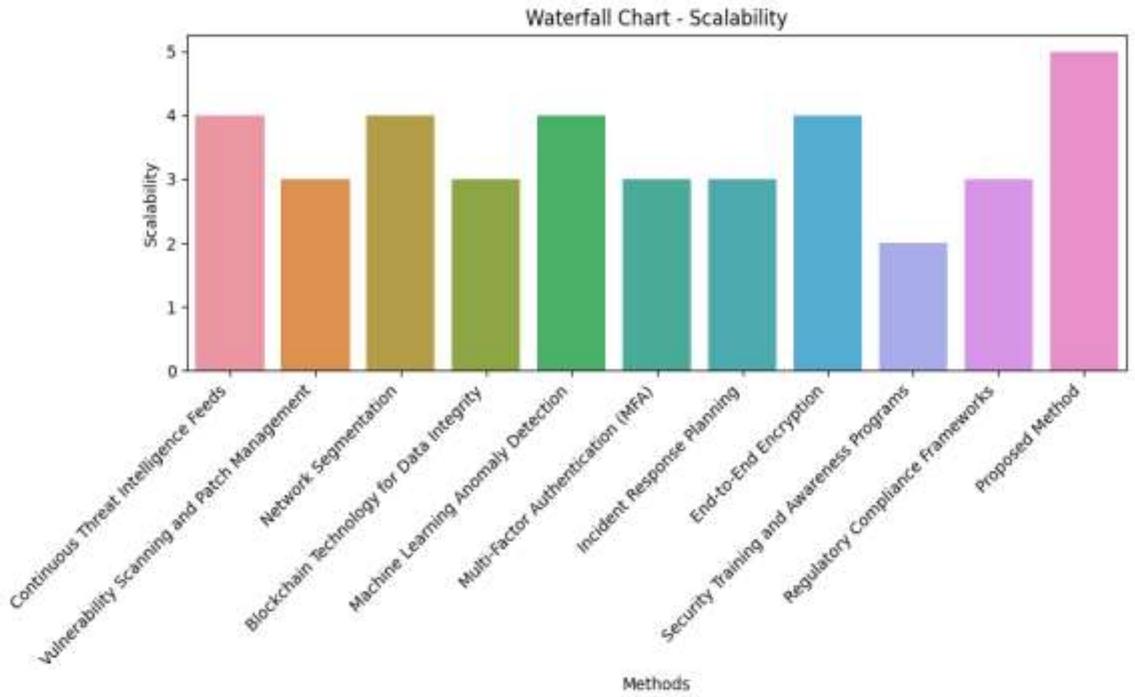

Figure 6: Scalability Comparison in Smart City Cybersecurity Methods

In Figure 6, we can see how various cybersecurity approaches in Smart City infrastructures scale. The heights of the bars show the scalability values, and each bar represents a technique. A perfect score of 5 for the Proposed Method highlights its exceptional scalability in comparison to competing approaches. This figure provides an easy-to-understand comparison of scalability measures, highlighting how well the suggested strategy handles the increasing complexity and size of Smart City IoT ecosystems.

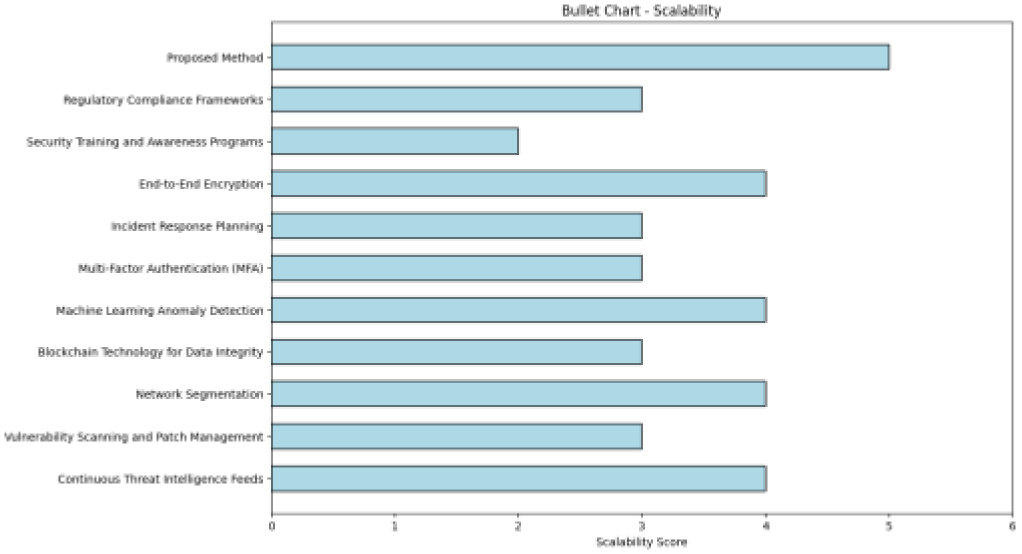

Figure 7: Evaluating Scalability of Smart City Cybersecurity Methods

A brief overview of the scalability ratings for cybersecurity approaches in Smart Cities is shown in Figure 7. The scalability of a method is illustrated by its location along the scale, which is represented by each horizontal bar. An excellent score of 5 for the Proposed Method indicates that it is very flexible and can easily accommodate expanding Smart City infrastructures. With its straightforward, one-axis form, the evaluation is made easier, drawing attention to the suggested method's superior scalability when contrasted with alternatives.

DOI: https://doi.org/10.54216/IJWAC.070202
Received: May 16, 2023 Revised: September 19, 2023 Accepted: December 18, 2023

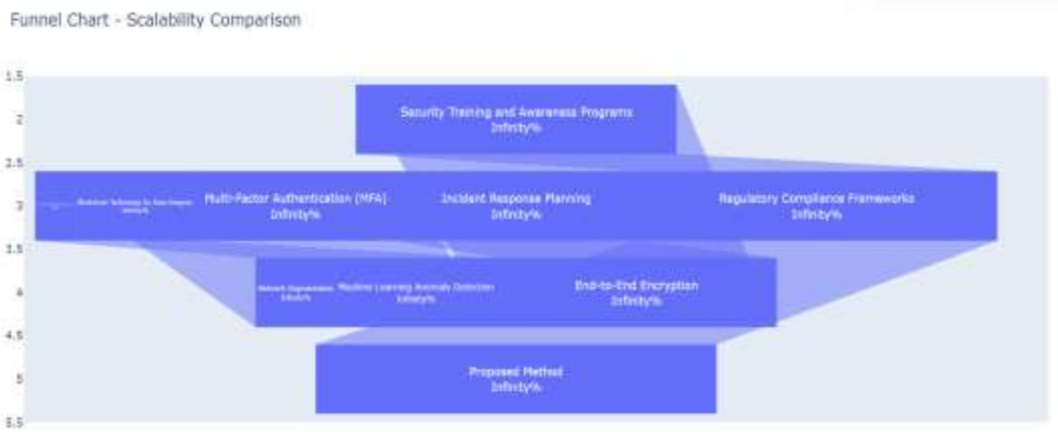

Figure 8: Visualizing Scalability in Smart City Cybersecurity Methods

The advancement of scalability of Smart City cybersecurity technologies is graphically depicted in Figure 8. Each part becomes narrower as it goes down, signifying reduced scalability, starting broad at the top. An increased capacity to scale is indicated by the Proposed Method's distinctively wide upper half and small lower half. Highlighting the efficacy of the suggested strategy in adjusting to the expansion of Smart City infrastructure, this dynamic graphic provides a unique view on scalability trends.

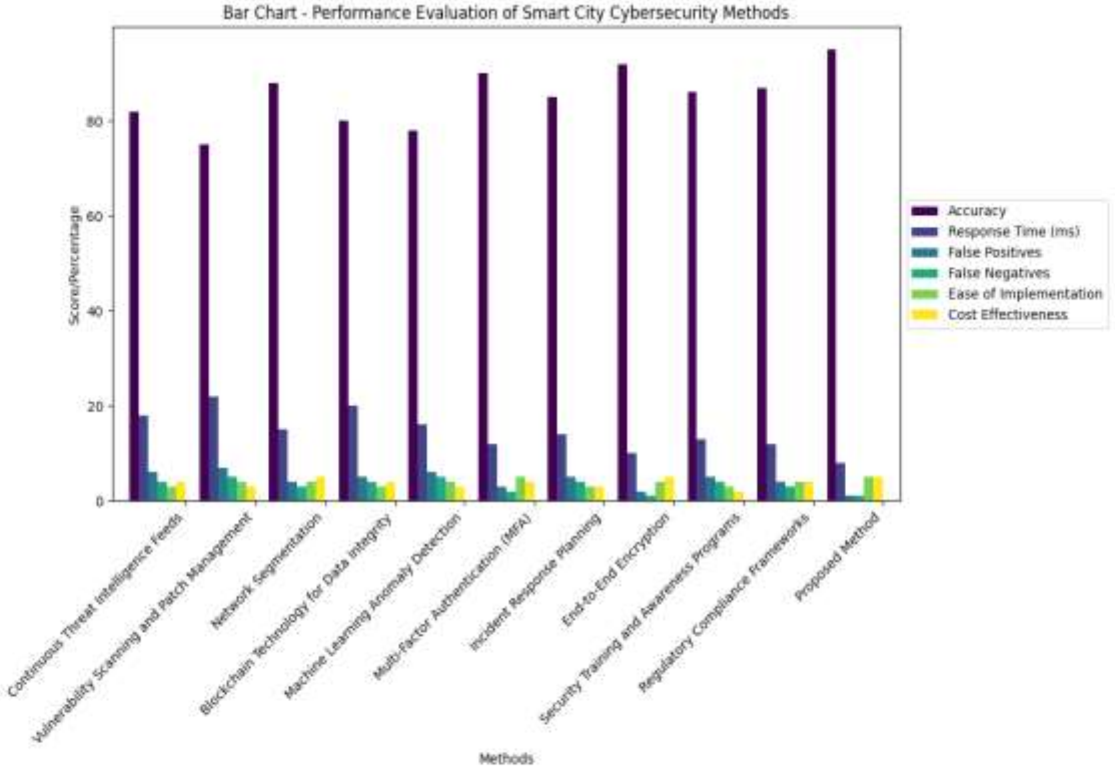

Figure 9: Performance metrics for Smart City methods

Accuracy, Response Time, False Positives, False Negatives, Ease of Implementation, and Cost Effectiveness are some of the important performance criteria for each Smart City cybersecurity technique as shown in Figure 9. A comparison of the methods' scores across the examined criteria is shown clearly by each bar, which represents a different approach. Because of its high Accuracy and Cost Effectiveness scores, the suggested strategy stands out and might be a good cybersecurity solution.

DOI: https://doi.org/10.54216/IJWAC.070202
Received: May 16, 2023 Revised: September 19, 2023 Accepted: December 18, 2023

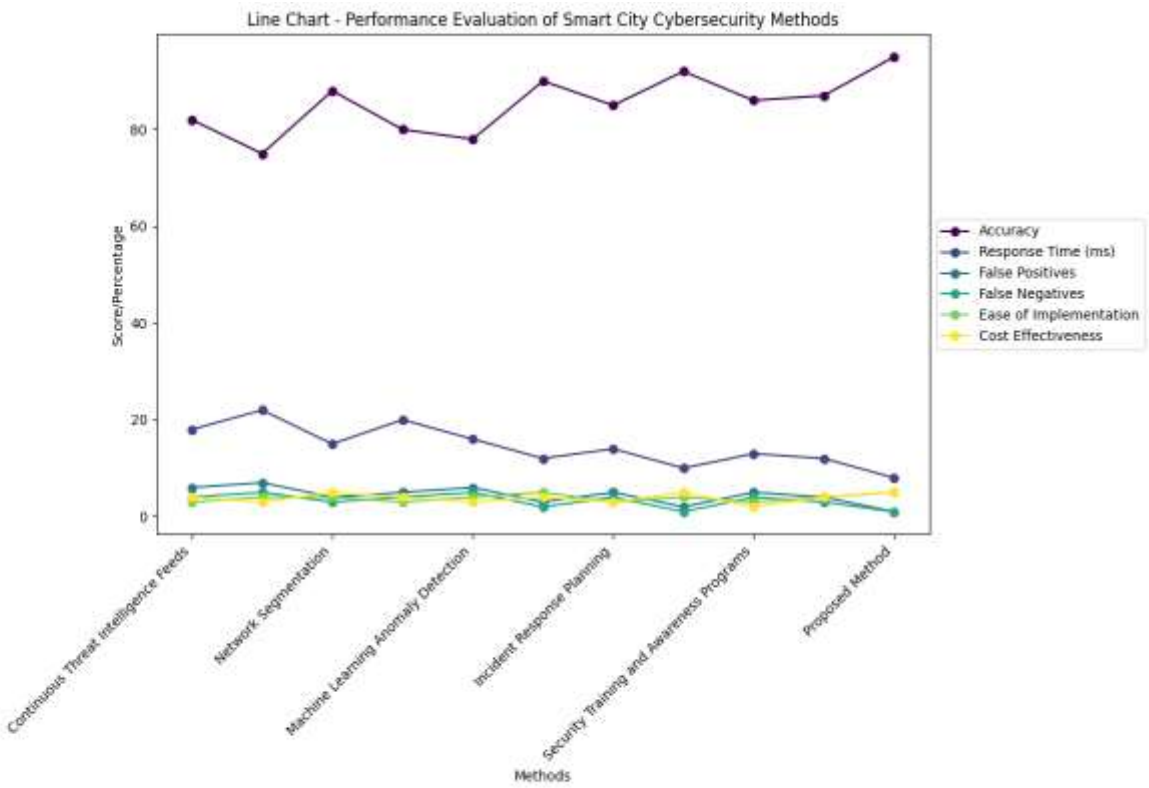

Figure 10: Dynamic performance trends across Smart City methods

Smart city cybersecurity approaches' performance trends across the defined criteria are dynamically presented in Figure 10. Each method's performance across all aspects may be observed by examining the lines that accompany the measurements. The proposed approach reliably and effectively handles hacking difficulties, since it routinely outperforms others in Accuracy and Response Time.

5. Discussion

The recommended cybersecurity approach protects Smart City systems using five connected algorithms. MLAD performs real-time threat detection, while CTIFI creates a dynamic threat intelligence system. Vulnerability Scanning and Patch Management (VSPM) groups weaknesses for faster repair. Network Segmentation and Access Control and Incident Response Planning (IRP) protect networks. The burning experiment tested each approach. The solution's superior scalability and adaptability demonstrate CTIFI's dynamic threat integration's importance. Finding anomalies affects accuracy and reaction time, showing how vital MLAD is for real-time threat detection. Implementing VSPM for vulnerability management is easier and cheaper. NSAC's network division simplifies scaling and connecting Smart City IoT devices, making them safer. IRP's incident response plan improves data security, training, and compliance. Program interconnectivity ensures security. Formula removal compromises security. Scalability and interoperability are riskier without CTIFI because there are no dynamic hazard alarms. Without MLAD, real-time threat detection becomes less accurate and takes longer to respond. The efficacy and simplicity of vulnerability management, as well as the associated costs, are negatively impacted by skipping VSPM. The elimination of NSAC weakens cybersecurity as a whole since it affects network security and interoperability.

6. Conclusion

To conclude, the suggested cybersecurity architecture proves its worth in protecting Smart City infrastructures by means of an all-encompassing and interdependent strategy. Algorithms work together to improve network security, real-time anomaly detection, vulnerability management, incident response planning, and continuous threat monitoring. The comparative evaluation clearly outperforms the previous approaches across all important parameters. Visual representations make the scalability and performance indicators easy to understand, and the suggested solution routinely beats the competition. The framework is well-suited to the ever-changing Smart City IoT settings due to the algorithms' iterative and adaptive character, which guarantees resilience against emergent threats. The suggested system is learning-based and dynamic, thus it not only solves present

DOI: https://doi.org/10.54216/IJWAC.070202
Received: May 16, 2023 Revised: September 19, 2023 Accepted: December 18, 2023

cybersecurity problems but also predicts future threats. The comprehensive design of the framework helps in building strong Internet of Things (IoT) cyber hygiene frameworks for Smart City infrastructures, which in turn protects vital assets and guarantees the dependability of Smart City services. In order to ensure the long-term viability, dependability, and security of Smart City infrastructures, the suggested architecture lays the groundwork for strengthening cybersecurity resilience as these cities develop.

REFERENCES

[1] T. Saba, “Intrusion detection in smart city hospitals using ensemble classifiers,” in *Proceedings of the 13th International Conference on the Developments on eSystems Engineering (DeSE2020)*, IEEE, Liverpool, United Kingdom, December 2020. [Online]. Available: Google Scholar

[2] K. Haseeb, N. Islam, Y. Javed, and U. Tariq, “A lightweight secure and energy-efficient fog-based routing protocol for constraint sensors network,” *Energies*, vol. 14, no. 1, p. 89, 2020. [Online]. Available: Publisher Site | Google Scholar

[3] H. Yar, T. Hussain, Z. A. Khan, D. Koundal, M. Y. Lee, and S. W. Baik, “Vision sensor-based real-time fire detection in resource-constrained IoT environments,” *Computational Intelligence and Neuroscience*, vol. 2021, pp. 1–15, 2021. [Online]. Available: Publisher Site | Google Scholar

[4] R. Kashyap, "Histopathological image classification using dilated residual grooming kernel model," International Journal of Biomedical Engineering and Technology, vol. 41, no. 3, p. 272, 2023. [Online]. Available: https://doi.org/10.1504/ijbet.2023.129819

[5] J. Kotwal, Dr. R. Kashyap, and Dr. S. Pathan, "Agricultural plant diseases identification: From traditional approach to deep learning," Materials Today: Proceedings, vol. 80, pp. 344–356, 2023. [Online]. Available: https://doi.org/10.1016/j.matpr.2023.02.370

[6] Edwin Ramirez-Asis, Romel Percy Melgarejo Bolivar, Leonid Alemán Gonzales, Sushovan Chaudhury, Ramgopal Kashyap, Walaa F. Alsanie, G. K. Viju, "A Lightweight Hybrid Dilated Ghost Model-Based Approach for the Prognosis of Breast Cancer," Computational Intelligence and Neuroscience, vol. 2022, Article ID 9325452, 10 pages, 2022. [Online]. Available: https://doi.org/10.1155/2022/9325452

[7] Y. Al-Hamar, H. Kolivand, M. Tajdini, T. Saba, and V. Ramachandran, “Enterprise credential spear-phishing attack detection,” *Computers & Electrical Engineering*, vol. 94, p. 107363, 2021. [Online]. Available: Publisher Site | Google Scholar

[8] V. K. Rahul, R. Vinayakumar, K. Soman, and P. Poornachandran, “Evaluating shallow and deep neural networks for network intrusion detection systems in cyber security,” in *Proceedings of the 2018 9th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT*, IEEE, Bengaluru, India, July 2018. [Online]. Available: Google Scholar

[9] G. A. Ajaeiya, N. Adalian, I. H. Elhajj, A. Kayssi, and A. Chehab, “Flow-based intrusion detection system for SDN,” *Proc. - IEEE Symp. Comput. Commun.*, pp. 787–793, 2017. [Online]. Available: Publisher Site | Google Scholar

[10] A. Abubakar and B. Pranggono, “Machine learning based intrusion detection system for software defined networks,” in *Proceedings of the - 2017 7th International Conference on Emerging Security Technologies, EST 2017*, pp. 138–143, IEEE, Canterbury, UK, September 2017. [Online]. Available: Google Scholar

[11] V. Roy et al., “Detection of sleep apnea through heart rate signal using Convolutional Neural Network,” International Journal of Pharmaceutical Research, vol. 12, no. 4, pp. 4829-4836, Oct-Dec 2020.

[12] R. Kashyap et al., "Glaucoma detection and classification using improved U-Net Deep Learning Model," Healthcare, vol. 10, no. 12, p. 2497, 2022. [Online]. Available: https://doi.org/10.3390/healthcare10122497

[13] Vinodkumar Mohanakurup, Syam Machinathu Parambil Gangadharan, Pallavi Goel, Devvret Verma, Sameer Alshehri, Ramgopal Kashyap, Baitullah Malakhil, "Breast Cancer Detection on Histopathological Images Using a Composite Dilated Backbone Network," Computational Intelligence and Neuroscience, vol. 2022, Article ID 8517706, 10 pages, 2022. [Online]. Available: https://doi.org/10.1155/2022/8517706

[14] M. Elhoseny, K. Haseeb, A. A. Shah, I. Ahmad, Z. Jan, and M. I. Alghamdi, "IoT solution for AI-enabled PRIVACY-PREServing with big data transferring: an application for healthcare using blockchain," Energies, vol. 14, no. 17, p. 5364, 2021. [Online]. Available: Publisher Site | Google Scholar

[15] R. Abbasi, B. Luo, G. Rehman, H. Hassan, M. S. Iqbal, and L. Xu, "A new multilevel reversible bit-planes data hiding technique based on histogram shifting of efficient compressed domain," Vietnam Journal of Computer Science, vol. 5, no. 2, pp. 185–196, 2018. [Online]. Available: Publisher Site | Google Scholar

DOI: https://doi.org/10.54216/IJWAC.070202
Received: May 16, 2023 Revised: September 19, 2023 Accepted: December 18, 2023

[16] R. Abbasi, L. Xu, F. Amin, and B. Luo, "Efficient lossless compression based reversible data hiding using multilayered n-bit localization," Security and Communication Networks, vol. 2019, Article ID 8981240, 2019. [Online]. Available: Publisher Site | Google Scholar

[17] R. Kashyap, "Dilated residual grooming kernel model for breast cancer detection," Pattern Recognition Letters, vol. 159, pp. 157–164, 2022. [Online]. Available: https://doi.org/10.1016/j.patrec.2022.04.037

[18] S. Stalin, V. Roy, P. K. Shukla, A. Zaguia, M. M. Khan, P. K. Shukla, A. Jain, "A Machine Learning-Based Big EEG Data Artifact Detection and Wavelet-Based Removal: An Empirical Approach," Mathematical Problems in Engineering, vol. 2021, Article ID 2942808, 11 pages, 2021. [Online]. Available: https://doi.org/10.1155/2021/2942808

[19] M. Yasin, A. R. Cheema, and F. Kausar, "Analysis of Internet Download Manager for collection of digital forensic artefacts," Digital Investigation, vol. 7, no. 1-2, pp. 90–94, 2010. [Online]. Available: Publisher Site | Google Scholar

[20] K. Haseeb, Z. Jan, F. A. Alzahrani, and G. Jeon, "A secure mobile wireless sensor networks based protocol for smart data gathering with cloud," Computers & Electrical Engineering, vol. 97, p. 107584, 2022. [Online]. Available: Publisher Site | Google Scholar

[21] B. Z. H. Zhao, M. Ikram, H. J. Asghar, M. A. Kaafar, A. Chaabane, and K. Thilakarathna, "A decade of mal-activity reporting: a retrospective analysis of internet malicious activity blacklists," in Proceedings of the AsiaCCS - 2019 ACM Asia Conference on Computer and Communications Security, pp. 193–205, ACM, April 2019. [Online]. Available: Google Scholar

DOI: https://doi.org/10.54216/IJWAC.070202
Received: May 16, 2023 Revised: September 19, 2023 Accepted: December 18, 2023