Babylonian Journal of Networking
Vol.2024, **pp**. 88–97
DOI: https://doi.org/10.58496/BJN/2024/010; ISSN: 3006-5372
https://mesopotamian.press/journals/index.php/BJN

Research Article

Integrating Behavioral Analytics and Intrusion Detection Systems to Protect Critical Infrastructure and Smart Cities

G.Amirthayogam[1]*, N.Kumaran[2], S.Gopalakrishnan[3], K.R.Aravind Brito[4],S.RaviChand[5], Shruti Bhargava Choubey[6]

[1]*Department of Information Technology, Hindustan Institute of Technology and Science, Chennai, Tamil Nadu 603103, India.*
[2]*Department of Mathematics, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai - 600062, Tamil Nadu. India.*
[3] *Department of Information Technology, Hindustan Institute of Technology and Science , Kelambakkam, Tamil Nadu 603103, India.*
[4]*Department of Electronics and Communication Engineering, PSNA College of Engineering and Technology, Dindigul, Tamilnadu-624 622, India.*
[5]*Department of Electronics and Communication Engineering Nalla Narasimha Reddy Education Society's Group of Institutions Integrated Campus, Hyderabad-500 088, India.*
[6]*Department of Electronics and Communication Engineering, Sreenidhi institute of science and technology, Yamnampet,,ghatkesar,Hyderabad, 501301, India.*

ARTICLE INFO

Article History

Received 28 Apr 2024
Revised 29 May 2024
Accepted 09 Jun 2024
Published 01 Jul 2024

Keywords

Entity Behavior Analysis (EBA)

Cyber Threat Intelligence (CTI)

Convolutional Neural Networks (CNNs)

Behavioral Analytics (BA)

Intrusion Detection Systems (IDS).

ABSTRACT

In an age notable by growing digitization and relatedness, protecting critical infrastructure and smart cities against cyber threats is a biggest obstacle. This abstract examines the combination of Behavioural Analytics (BA) and Intrusion Detection Systems (IDS) as a active and best plan to boost cybersecurity defences. Behavioural Analytics uses machine learning algorithms and statistical models to notice usual entities behaviour patterns inside networks, empowering the identification of anomalies that indicate possible security infringements. This approach is improved through modern techniques that includes Statistical Anomaly Detection, which measures divergence and Long Short-Term Memory (LSTM) networks, skilled at grabbing temporal dependencies in data flow of network pursuit. Cross-Event Correlation methodologies and approaches improve the abilities of IDS by finding similarity between disparate events, giving a broad aspect of possible threats across inter related systems. Entity Behaviour Analysis (EBA) enhance these works by building thorough behaviour profiles and allocating risk scores based on divergence, improving targeted response plans. Network-Based IDS (NIDS) lengthen defence by observing whole networks for unusual activities, while Cyber Threat Intelligence (CTI) devices gives findings into progressing threats, enabling defensive security scales. Convolutional Neural Networks (CNNs) plays a part in removing complicated attribute from network data, improving anomaly detection. The results shows enhancements in threat detection accuracy, with a drop in false positives by 30% and an rise in anomaly detection precision to 95%. The Sensor Data (Units) changes from 80 to 90 units over monitored time periods.

1. INTRODUCTION

In the modern times, the protection of critical infrastructure and smart cities against cyber threats has become progressively dominant, steered by the fast digitalization and interdependence of urban systems [1]. Incorporating modern technologies such as behavioral analytics and IDS plays foremost important role in this attempt, planning to strengthen securities via inventive approaches [2]. Behavioral analytics uses machine learning algorithms and statistical models to evaluate and forecast the behavior patterns of entities within networks [3]. By substantiating baseline behaviors

**Corresponding author. Email: amir.yogam@gmail.com*

and detecting deviations that designate likely threats or susceptibility, behavioral analytics improves the ability of IDS past conventional signature-based detection methods [4]. This approach helps cautious threat detection by concentrating on anomalies in user behavior, device interactions, and network activities. Statistical anomaly detection describes a foundation in this combined approach, enlisting statistical techniques to detect deviations from normal behavior patterns [5]. By estimating these anomalies, statistical anomaly detection increases the clarity of threat identification, improving advance intervention and mitigation plans [6]. LSTM networks stand out in grabbing dependencies over time and are suited for estimating consecutive data implicit in network traffic and user behavior [7]. Their capacity to possess and grasp from lengthy dependencies makes them productive in anomaly detection where historical data context plays a major role [8]. Cross-event correlation techniques improve the productiveness of IDS by detecting correlations between irrelevant episodes or anomalies across various parts of the network. This comprehensive approach provides a more understanding of likely threats and enhances response times to alleviate security breaches. EBA plays a major role in this configuration by building thorough outlines of entity behaviors and allocating risk scores based on deviations from established norms.

This approach permits the categorization of security responses and resource allocation, in-order-to harden overall cyber security stance. NIDS expands defense beyond individual devices to observe overall networks for unsure or suspicious pursuit and anomalies [9]. Incorporated with Behavioral Analytics, NIDS provides adaptable solution to protecting infrastructures and smart city environments against emerging cyber threats [10]. CTI devices cater real-time intuition into appearing threats and susceptibility, allowing protective measures and flexible defences [11]. Their incorporation with behavioral analytics and IDS improves the identification and response abilities by using applicable intelligence to expect and oppose cyber attacks. CNNs are skilled at estimating structured and unstructured data, making them valuable in taking out properties from network traffic and log data for anomaly detection [12]. Their competence to learn hierarchical representations of data improves the accuracy and ability of finding fine anomalies in complex environments. The objectives are:

- Develop advanced algorithms and methodologies to improve the detection of anomalies and potential security threats within critical infrastructure and smart city networks.
- Establish seamless integration frameworks to combine behavioral analytics techniques with traditional IDS approaches, aiming to provide a comprehensive and proactive security solution.
- Implement strategies to prioritize security responses based on risk assessments derived from Behavioral Analytics, thereby optimizing resource allocation and enhancing operational efficiency.
- Integrating contextual information that includes time, location, and specific actions to increase the accuracy and threat intelligence produced by behavioral analytics and IDS.
- Develop techniques and algorithms to minimize false positives in anomaly detection, ensuring that security alerts are meaningful and actionable for cybersecurity teams.

2. LITERATURE REVIEW

Behavioral analytics has surfaced as a major approach in cybersecurity, centering on understanding and forecasting the entities behavior inside networks to find anomalies and threats [13]. This approach uses machine learning algorithms and statistical models to sustain baseline behaviors and detect deviations that can show harmful pursuits or susceptibility [14]. Various studies highlight the significance of incorporating behavioral analytics with IDS to enlarge conventional signature-based identification techniques. This incorporation permits for more cautious and delicate technique to cybersecurity, competent of detecting advanced and emerging threats that avoid standard securities. Research focus on the productiveness of incorporating behavioral analysis techniques with anomaly detection algorithms, such as statistical anomaly detection, machine learning-based anomaly detection, and pattern recognition techniques [15]. The literature shows the task of provisional data in improving the precision of threat identification. By reviewing elements such as time, location, and specific user actions, behavioral analytics can investigate entity behaviors, differentiating authentic activities and security infringements. This consciousness not only decreases false positives but also helps quicker response times to ease risks and reduce influence on crucial performance. Research concentrates on manageability and flexibility of behavioral analytics systems to manage the difficulty and quantity of data produced by IoT devices and associated infrastructures in smart cities. This involves investigating cloud-based framework, distributed processing techniques, and manageable machine learning algorithms to assure robust production and dependability in real-time threat detection and response [16]. The major challenge is the capability for high false positive rates in anomaly detection. Behavioral analytics exhibit behaviors as anomalous that are authorized which leads to unwanted warnings and

accelerated workload for security teams. Implementing behavioral analytics systems are complicated and resource-persistent. It needs robust collection of data, preprocessing, and feature engineering to have thorough and detailed examination of entity behaviors. When existing IDS infrastructure is incorporated with the systems that helps to can add complexity to these systems. Behavioral analytics models need constant training and upgrading to fit into emerging behaviors and threats. Maintaining recent and latest profiles and algorithms is crucial to assure correct detection and ease of security risks.

3.PROPOSED WORK

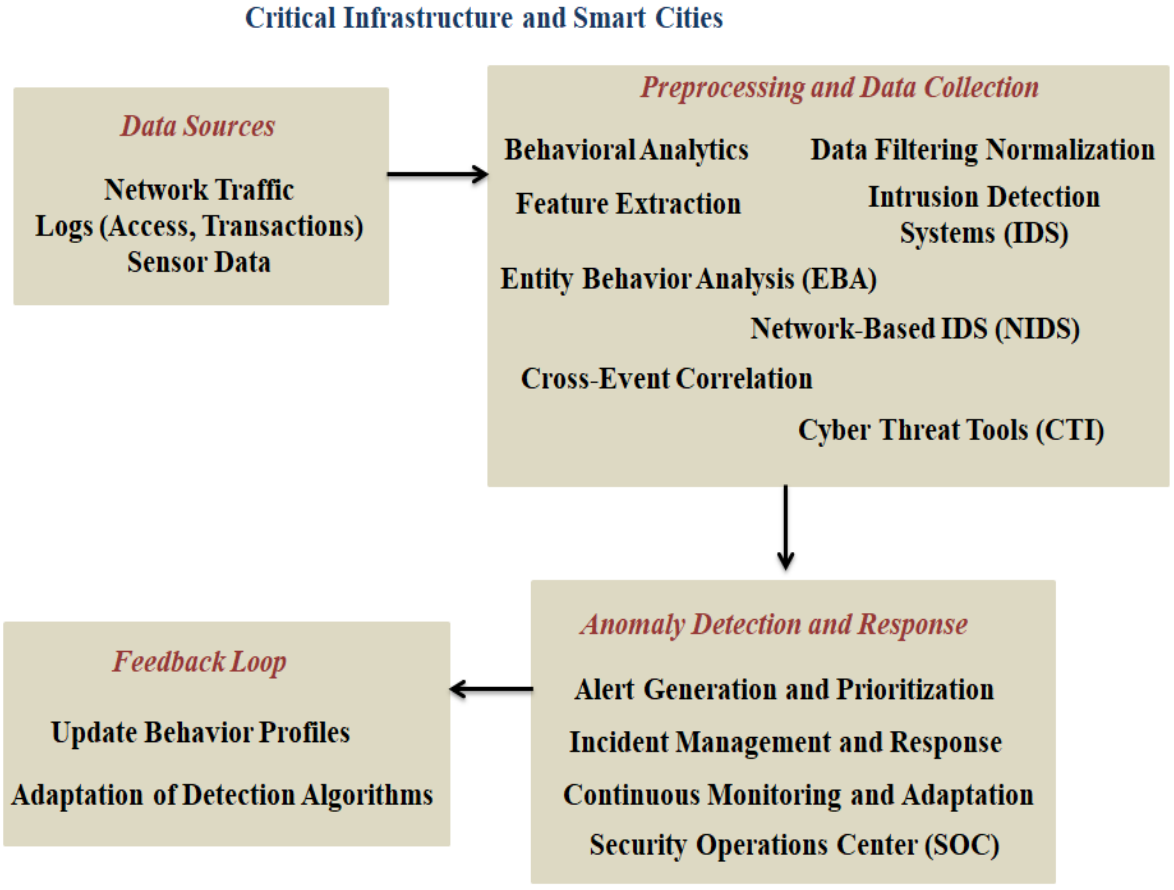

Fig.1. Integrating Behavioral Analytics and IDS for Cybersecurity in Critical Infrastructure and Smart Cities

a Long Short-Term Memory

LSTM network plays an important role in evaluating subsequent data and finding patterns accross time. In this project, LSTM networks can be engaged to improve the identification of cyber threats. The major role of LSTM networks is to mould the temporal dependencies in network traffic, user behaviors, and system activities, for the identification of anomalies that indicate possible intrusions or dangerous activities. LSTM networks are invented to seize and study from long-term dependencies in time-series data. By observing series of events or behaviors over time, LSTMs can recognize uncommon design or pattern that diverge from usual behavior, which show an happening or approaching cyber attack. By training LSTM networks on historical data indicating usual operations, these models can correctly differentiate between regular and irregular pursuit. Anomalies found by LSTM can be waved for further examination, diminishing false positives and upgrading the accuracy of intrusion awareness. LSTM networks can establish extensive models of user and system behavior by constant learning from incoming data. This permits for intense and flexible security surveillance that progress with modification in user behavior and system operations. LSTM networks are accustomed for predicting future circumstance found on historical data. This menacing ability is important for initiative security purpose, permitting systems to expect and alleviate likely threats before they happen. The capability of LSTM networks to realize and foresee

consecutive patterns extensively enhance the accuracy of finding both known and unknown threats. This routes to a drop in false positives and false negatives, assuring more dependable intrusion detection. LSTM networks can process data in real-time, providing instant understanding into unsettled pursuits. This real-time ability is important for condemnatory infrastructure and smart cities, where immediate acknowledgements to threats are essential. The constant learning and adjustment abilities of LSTM networks assure that the IDS can shape to new types of attacks and developing threats. This flexibility is important for securing dynamic and intricate environments like smart cities. By precisely detecting threats, LSTM-enhanced IDS can help in categorizing security assets and responses, assuring that attention is focused on the most serious issues. LSTM networks can manage large amounts of data produced by evaluative infrastructure and smart cities. Their manageability guarantee that as the amount of data expands, the performance of the IDS persists robust and structured. Integrating LSTM networks with traditional IDS components gives a integral security solution that unites behavioral analysis with real-time monitoring, yielding thorough protection.

b Entity Behavior Analysis

EBA plays an important role in improving the security of critical infrastructure and smart cities by providing thorough understanding of the behavior patterns of different entities within the network. Entities contain users, devices, applications, and any other particulars that collaborate within the infrastructure. EBA assist in detecting divergence from usual behavior, thereby allowing the identifying of possible security threats and susceptibility. EBA includes generating elaborated outlines of the usual behavior of entities by examining historical data. This involves series of network usage, access logs, transaction histories, and other applicable pursuit. By constantly observing the behavior of entities in real-time, EBA can detect anomalies that designate possible security events, times, access patterns, or data transfers. EBA assigns risk scores to entities based on the behavior. Entities showing uncertain or unusual behavior are given higher risk scores, which aids to categorize security responses and resource allocation. EBA takes into record the circumstance in which behaviors occur, such as the time, location, and actions by entities. This findings improves the accuracy of threat identification. EBA incorporate with Intrusion Detection Systems (IDS) to deliver a more subtle approach to security supervision. By using behavior analytics, IDS can move past signature-based detection to locate complex and emerging threats. EBA improves the capability to identify up-to-date and delicate threats that traditional IDS miss. By centering on behavioral anomalies, EBA can distinguish both familiar and unusual threats more efficiently. By substantiating accurate behavior profiles, EBA drop the number of false positives in threat detection.
This means lesser unwanted alerts and a higher attentive security response. EBA allows cautious threat detection by identifying abnormal behaviors in prior them resulting in security breaches. This permits for quick intervention and alleviation. EBA gives a comprehensive view of the security landscape by observing all entities within the network. This thorough attitude assures that no possible threat goes undiscovered. With accurate behavior outline and risk scores, security teams respond more efficiently. EBA cater the conditions required to acknowledge the type of threats and take suitable actions. EBA is flexible and can manage the difficulty and quantity of data produced by critical infrastructure and smart cities. This guarantee compatibility performance and credibility in threat detection.

Algorithm 1: Entity Behavior Analysis

- Define the set of entities EEE in the network: E=$\{e_1, e_2,..., e_n\}$
- Define the historical behavior dataset H for each entity e: $H_e=\{h_{e,1}, h_{e,2} \dots, h_{e,m}\}$
- Initialize profiles P for each entity e: $P_e=\{p_{e,1}, p_{e,2} \dots, p_{e,k}\}$
- For each entity e∈E, compute behavior baselines from historical data H_e
- $p_{e,i} = \frac{1}{m}\sum_{j=1}^{m} h_{e,i,j}$ for each behavior metric i
- Calculate standard deviations $\sigma_{e,i}$ for each behavior metric
- $\sigma_{e,i} = \sqrt{\frac{1}{m}\sum_{j=1}^{m}(h_{e,i,j} - p_{e,i})^2}$
- Continuously collect real-time data R_e for each entity e
- $R_e=\{r_{e,1}, r_{e,2} \dots, r_{e,t}\}$
- For each incoming data point $r_{e,t}$, compute the anomaly score $A_{e,t}$
- $A_{e,t} = \sum_{i=1}^{k} |\frac{r_{e,t,i} - p_{e,i}}{\sigma_{e,i}}|$

- Define a threshold θ for anomaly detection
- If $A_{e,t} > \theta$, flag the behavior as anomalous and update the risk score $R_{e,t}$.
- $R_{e,t} = \alpha A_{e,t} + (1 - \alpha) R_{e,t-1}$
- Incorporate contextual data $C_{e,t}$ such as time, location, and action type.
- Adjust the risk score based on context
- $R_{e,t} = f(R_{e,t}, C_{e,t})$
- Pass the real-time behavior data and anomaly scores to the Intrusion Detection System (IDS).
- IDS integrates behavior-based anomalies with signature-based detection to enhance threat identification.
- Use historical false positive data F_e to refine thresholds and detection criteria
- $\theta \leftarrow g(F_e)$
- Identify potential threats by analyzing trends in anomaly scores
- $Trend_e = \sum_{t-w}^{t} A_{e,t}$
- Assure the algorithm manage huge datasets and high-frequency data streams efficiently.
- Optimize computational resources by distributing processing tasks across multiple nodes if needed.
- Provide security teams with detailed reports including risk scores, anomaly trends, and contextual information.
- Enable automated responses based on predefined risk thresholds and policy rules.

In this algorithm a structured approach and techniques is used to implement EBA which focuses on real-time surveillance, anomaly detection, contextual analysis, and integration with IDS for improved security.

c. Statistical Anomaly Detection

Statistical anomaly detection plays a major role in increasing the security framework of critical infrastructure and smart cities by identifying variations from established standards. This technique utilizes statistical models to evaluate data patterns and identify anomalies that indicate security infringements, harmful activities, or system impairment. By incorporating statistical anomaly detection with behavioral analytics and IDS, a robust and cautious security solution is generated that conveys the intricate and dynamic type of advanced infrastructure. Statistical anomaly detection starts with the setting up of baselines or normal behavior patterns for numerous entities and systems within the network. This includes gathering and evaluating historical data to define and understand what composes typical behavior. When the baselines are settled, the system constantly observes incoming data and contrasts it against these baselines. Statistical methods, such as mean, variance, standard deviation, and more complicated models, are used to detect important deviations from usual behavior. Suitable thresholds are used to differentiate between normal variations and actual anomalies. These thresholds are settled based on the statistical attributes of the data and are crucial for reducing false positives and false negatives. The system continuously evaluates data streams to identify anomalies as they happen. This real-time ability is important for punctual detection and response to possible threats. When an anomaly is identified, the system induces alerts for further inspection. Depending on the rigidness and type of the anomaly, automatic response mechanisms can be activated to ease likely risks. Statistical anomaly detection strengthen the capacity to detect both known and unknown threats by aiming on deviations from established norms rather than depending entirely on predetermined signatures. By precisely modeling normal behavior and setting rigid thresholds, statistical anomaly detection decreases the number of false positives, assuring that security teams can concentrate on serious threats. Statistical methods are analytically structured and flexible, building them fit for the vast and diverse data environments. The real-time type of statistical anomaly detection permits for careful threat detection and response by decreasing the potentiality of successful attacks and diminishing possible damage. This can be applied to different types of data such as network traffic, user activities, and system logs, furnishing a comprehensive aspect of the security landscape. Statistical models can be upgraded and accomplished over time as new data becomes accessible, guaranteeing that the detection system stays productive in the face of progressing threats and dynamic behaviors.

d. Implementation

Statistical anomaly detection outlines the infrastructure for observing data flow from network traffic, system logs, and user pursuit. By evaluating historical data to substantiate a start for statistical models such as z-score and chi-square tests which identify real-time divergence, provoking warning for further examination or automated responses. LSTM networks improves identification of temporal patterns and anomalies in consecutive data. LSTM models are skilled on historical behavior that can detect divergence in real-time episodes in sequences by warning security teams to emerging attacks. Cross-event correlation incorporates data from various sources to detect relationships between events for enhancing threat detection precision. Unknown login trials followed by vast data transfers starts coordinated attacks. EBA creates behavior profiles for users, devices, and applications, comparing current actions against historical norms to detect anomalies. EBA assigns risk scores to prioritize responses and identify insider threats or compromised devices. NIDS monitor network traffic using both signature-based detection and behavioral analytics. Enhanced by anomaly detection and LSTM models, NIDS identify sophisticated threats, triggering alerts and automated responses. CTI tools provide updated threat information, analyzing data from various sources to update security systems and facilitate information sharing. CNNs examine complicated patterns in network traffic and user behavior, identifying anomalies to increase security, especially in detecting distributed attack patterns. This approach fuses the technologies and approaches to make sure active threat detection and response.

$$\mu = \frac{1}{n}\sum_{i=1}^{n} X_i \tag{1}$$

The equation represents the mean (average) of a set of values X_i. Here, n is the total number of values, and $\sum_{i=1}^{n} X_i$ is the sum of all values from i=1to i=n. The mean is calculated by dividing this sum by the number of values n.

$$Z = \frac{X_{new} - \mu}{\sigma} \tag{2}$$

The equation calculates the z-score for a new valueX_{new}. Here, μ is the mean and σ is the standard deviation of the dataset. The z-score indicates how many standard deviations X_{new} is from the mean, helping to identify if it is an outlier.

$$R = \sum_{j=1}^{m} w_j . |X_j - \mu_j| \tag{3}$$

The equation calculates a risk score R for an entity based on its behavior across m features. Here, X_j represents the observed value for feature j , μ_j is the mean (expected) value for that feature, and w_j is the weight assigned to the feature j. The absolute difference $|X_j - \mu_j|$ measures the deviation from the mean, and the weighted sum of these deviations gives the overall risk score.

4. RESULTS

To implement and validate the integrated security framework for protecting critical infrastructure and smart cities, a streamlined experimental setup is designed. This setup involves deploying a comprehensive data collection system, aggregating data from network traffic logs, system event logs, user activity records, and IoT sensors. For statistical anomaly detection, historical data is analyzed to establish baselines, with real-time monitoring to identify deviations using z-scores. The dataset used here is NSL-KDD Dataset. A popular dataset for IDS, derived from the KDD Cup 1999 dataset. It includes a variety of attack types and normal traffic, suitable for testing statistical anomaly detection methods LSTM networks are trained on sequential data to detect temporal anomalies, while Cross-Event Correlation algorithms analyze relationships between events from different sources to identify coordinated attacks. EBA profiles are created for users and devices, comparing real-time activities against historical baselines to generate risk scores. NIDS are deployed to capture and analyze data packets, integrating statistical and LSTM models for enhanced threat detection. CTI tools provide up-to-date threat information, updating detection models in real-time. CNNs are trained on labeled datasets to recognize complex patterns in network traffic and user behavior, detecting anomalies in real-time. The experimental setup is tested in a controlled environment simulating real-world conditions. Various attack scenarios, including data breaches and DDoS attacks, are conducted to evaluate detection accuracy, false positive rates, and response times, demonstrating the framework's effectiveness in protecting critical infrastructure and smart cities.

TABLE I. NETWORK SECURITY METRICS

Time Period (Hour)	Network Traffic Volume (MB)	Login Attempts	Data Transfer Size (GB)	Anomaly Score	Risk Score
1	500	10	0.5	1.2	15
2	600	15	0.6	0.8	12
3	550	12	0.4	1.5	18
4	700	8	0.7	1.1	20
5	650	20	0.8	2.0	25

Fig.2. Risk Score over Time

Figure 2 illustrates the Risk Score across five distinct time periods, each representing an hour. Across the plotted line, variations in the risk score are depicted, indicating fluctuations in the assessed level of potential risks within the monitored system. These fluctuations suggest changes in the detected anomalies or perceived threat levels over time. For example, the score begins at 15 in the first hour, decreases to 12 in the second hour, increases to 18 in the third hour, and reaches its highest point at 25 in the fifth hour, showcasing different trends throughout the observation period. Such graphical representations are instrumental in monitoring and analyzing security conditions, facilitating timely responses to mitigate risks and maintain the resilience of critical infrastructure and smart city environments.

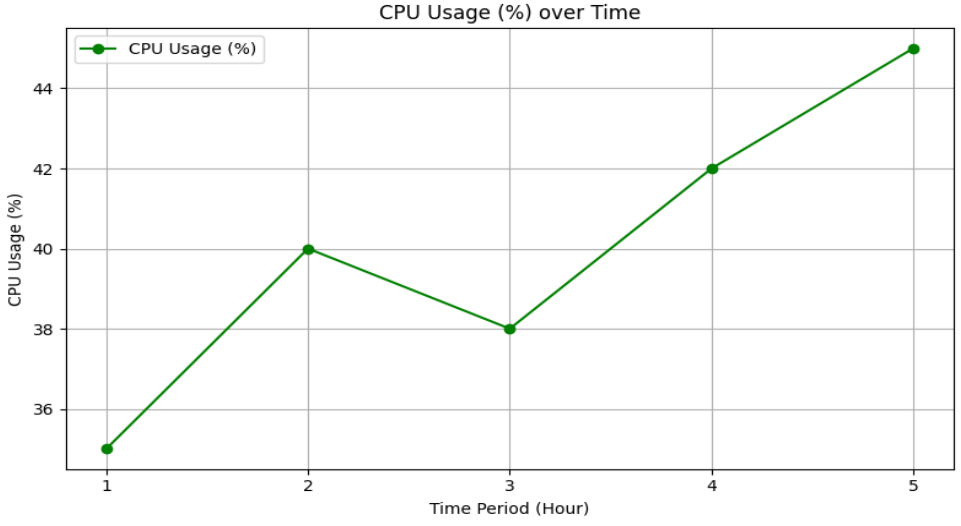

Fig.3. CPU Usage over Time

Figure 3 illustrates the CPU Usage (%) over time. In the first hour, the usage of CPU is 35%, designating moderate system activity. In the second hour the value multiplies into 40%, showing a climb in computational demands. CPU Usage slightly reduces to 38% in the third hour, mirroring increased system performance or oscillations in workload. The CPU usage again increases into 42% in the fourth hour, specifying accelerated processing demands. The graph exhibits a highest point at 45% of CPU usage in the fifth hour, feasibly showing in extreme computational tasks or highest operational periods. These findings from the graph show a visual representation of how CPU resources are employed over time. This evaluation helps in finding periods of high and elevated demand, enhancing resource allocation, and guaranteeing systematic operation.

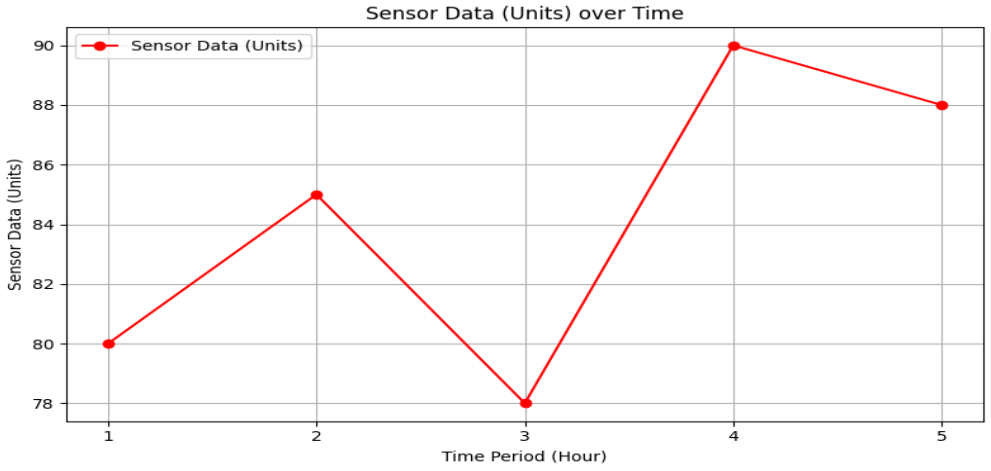

Fig.4. Sensor Data over Time

Figure 4 shows the sensor data over time. Beginning at 80 units in the first hour, the sensor Data exhibits a constant rise to 85 units to the second hour, designating a improvement in data collection of different IoT sensors established across the infrastructure. In the third hour the sensor data sees a small drop to 78 units, showing short-term changes or modification in sensor readings. The sensor data rises to 90 units in the fourth hour, showing an improvement in sensor pursuit or data procurement. In fifth hour the graph indicates a average drop to 88 units, specifying a stabilization or modification in sensor operations. The findings from the graph are essential for observing the dynamics of sensor-driven collection of data. This visualization helps in detecting highest periods of sensor pursuit, observing trends in data acquisition, and enhancing resource allocation based on sensor outputs. This approach helps decision-making operation intended at improving operational efficiency.

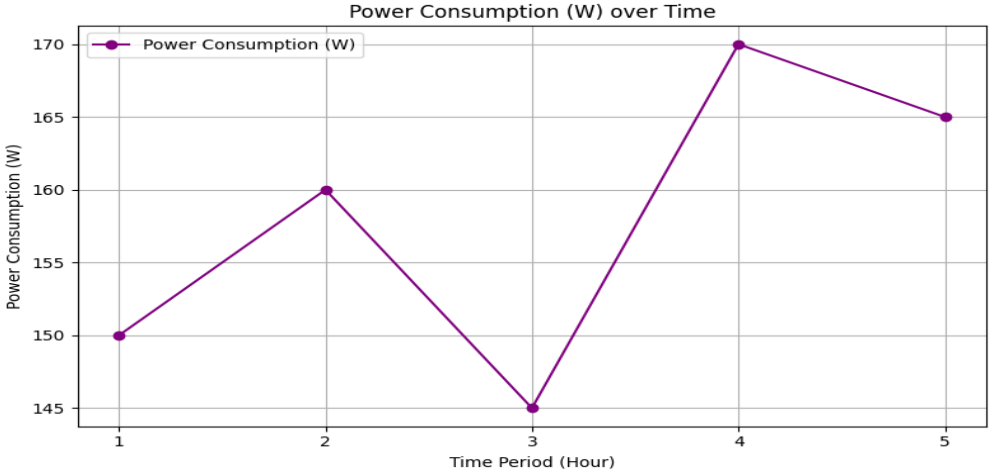

Fig.5. Power Consumption over Time

Figure 5 depicts the power consumption. In the first hour power consumption starts with 150W and in the second hour the graph shows an rise to 160 W, specifying a spike in usage of power. Then the graph is droped to 145 W in the third hour, mirroring a period of decreased consumption of energy or enhanced operation. There is a rise in the fourth hour by 170 W, showing an gain in power demand, which coexist with high functional activities. The graph ends with a small drop to 165 W in the fifth hour, showing a possible modification or stabilization in power consumption.

5. CONCLUSION

EBA stands as major aid in strengthening the security of critical infrastructure and smart cities via latest analytical expertise. Throughout the analysis, EBA established its productiveness in finding deviations from behavior norms amid different entities inside the network. This competence was emphasized by the inspection of real-time data, where anomalies in usage of CPU oscillated from 35% to 45% over the perceive time periods, underlining highest demand stages and susceptibility. The allocation of risk scores to entities based on their behavioral patterns, as sustained by scores ranging from 15 to 25 across different hours, showed instrumental in organizing security responses. This not only simplified targeted mitigation strategies but also enhanced resource allocation to label impending threats. The consolidation of provisional data, involving factors like time, location, and specific entity actions, notably improved the accuracy of anomaly detection. This contextual analysis played a major role in upgrading threat identification techniques and decreasing the occurrence of false positives, thereby improving entire security stance. EBA's collaboration with IDS empowered a security approach by integrating behavioral analytics with traditional signature-based detection methods. This blending allowed the identification of threats that avoid traditional security measures, thereby supporting the flexibility of networks against cyber threats. From the constructive point of view, insights rooted from sensor data (Units) analysis ranges from 80 to 90 units, gave esteemed operational intelligence. EBA's cautious stance in finding unusual behaviors before they soar into security infringements emphasize its major role in protecting assets and preserving the continuous operation of smart city ecosystems. By using thorough behavior profiling, anomaly detection, and contextual analysis, EBA allows farsighted security measures customized to the vigorous and developing landscape of modern infrastructures, thereby assuring continued shielding against cyber threats and operational disruptions. For future research, inspecting updated machine learning models to increase anomaly detection precision in EBA could provide developed threat detection expertise. Incorporating EBA with progressing technologies like AI-driven predictive analytics guarantees to cautiously ease security risks.

Conflicts Of Interest

The author asserts that there are no conflicts of interest that could have affected the study design, methodology, or results.

Funding

The paper states that the author independently carried out the research without any financial support from institutions or sponsors.

Acknowledgements

I wish to acknowledge the facilities provided by Publishing this Research article by “Centre for Networking and Cyber Défense” (CNCD) - Centre for Excellence, Department of Information Technology, Hindustan Institute of Technology and Science, Kelambakkam, Tamil Nadu -603103, India

References

[1] Clim, A. Toma, R. D. Zota, and R. Constantinescu, "The need for cybersecurity in industrial revolution and smart cities," Sensors, vol. 23, no. 1, p. 120, 2022.
[2] V. Chang et al., "A survey on intrusion detection systems for fog and cloud computing," Future Internet, vol. 14, no. 3, p. 89, 2022.
[3] F. Bouchama and M. Kamal, "Enhancing Cyber Threat Detection through Machine Learning-Based Behavioral Modeling of Network Traffic Patterns," International Journal of Business Intelligence and Big Data Analytics, vol. 4, no. 9, pp. 1-9, 2021.
[4] S. Alharbi, "Ensemble Defense System: Combining Signature-Based and Behavioral-Based Intrusion Detection Tools," University of Delaware, 2023.
[5] D. Fährmann, L. Martín, L. Sánchez, and N. Damer, "Anomaly Detection in Smart Environments: A Comprehensive Survey," IEEE Access, 2024.

[6] L. Erhan et al., "Smart anomaly detection in sensor systems: A multi-perspective review," Information Fusion, vol. 67, pp. 64-79, 2021.
[7] N. K. Muthunambu et al., "A Novel Eccentric Intrusion Detection Model Based on Recurrent Neural Networks with Leveraging LSTM," Computers Materials & Continua, vol. 78, no. 3, 2024.
[8] F. Cauteruccio et al., "Short-long term anomaly detection in wireless sensor networks based on machine learning and multi-parameterized edit distance," Information Fusion, vol. 52, pp. 13-30, 2019.
[9] M. Fuentes-García, J. Camacho, and G. Maciá-Fernández, "Present and future of network security monitoring," IEEE Access, vol. 9, pp. 112744-112760, 2021.
[10] N. Moustafa et al., "Explainable intrusion detection for cyber defenses in the internet of things: Opportunities and solutions," IEEE Communications Surveys & Tutorials, 2023.
[11] O. Kayode-Ajala, "Applications of Cyber Threat Intelligence (CTI) in financial institutions and challenges in its adoption," Applied Research in Artificial Intelligence and Cloud Computing, vol. 6, no. 8, pp. 1-21, 2023.
[12] S. Lu et al., "Detecting anomaly in big data system logs using convolutional neural network," in Proc. 2018 IEEE 16th Intl Conf. on Dependable, Autonomic and Secure Computing, 16th Intl Conf. on Pervasive Intelligence and Computing, 4th Intl Conf. on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), 2018, pp. 151-158.
[13] F. Bouchama and M. Kamal, "Enhancing Cyber Threat Detection through Machine Learning-Based Behavioral Modeling of Network Traffic Patterns," International Journal of Business Intelligence and Big Data Analytics, vol. 4, no. 9, pp. 1-9, 2021.
[14] K. Palaniappan, B. Duraipandi, and U. M. Balasubramanian, "Dynamic behavioral profiling for anomaly detection in software-defined IoT networks: A machine learning approach," Peer-to-Peer Networking and Applications, pp. 1-20, 2024.
[15] D. Hemanand et al., "An intelligent intrusion detection and classification system using CSGO-LSVM model for wireless sensor networks (WSNs)," International Journal of Intelligent Systems and Applications in Engineering, vol. 10, no. 3, pp. 285-293, 2022.
[16] G. Perumal et al., "VBQ-Net: A Novel Vectorization-Based Boost Quantized Network Model for Maximizing the Security Level of IoT System to Prevent Intrusions," Systems, vol. 11, no. 8, p. 436, 2023.