SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

IT Governance In Complex Systems: A Computational Framework For System Control And Reliability

Satya Ranjan Das[1], Gnanakumar Ganesan[2], Alok Singh Sengar[3], Ponmurugan Panneerselvam[4], Anuradha R[5], J. Sabitha[6]

[1] Associate Professor, Department of Computer Science and Engineering, Institute of Technical Education and Research, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India. Email: satyadas@soa.ac.in, ORCID: 0009-0009-5723-9665
[2] Assistant Professor, Department of Computer Science and Engineering, Presidency University, Bangalore, Karnataka, India. Email: gnanakumar.g@presidencyuniversity.in, ORCID: 0000-0001-6499-0080
[3] Associate Professor, Department of Computer Science & Application, Vivekananda Global University, Jaipur, India. Email: alok.sengar@vgu.ac.in, ORCID: 0000-0003-1933-5786
[4] Professor & Dean – Doctoral Studies & IPR, Department of Research, Meenakshi Academy of Higher Education and Research, India. Email: ponmurugan@maher.ac.in
[5] Assistant Professor, Department of Commerce, Meenakshi College of Arts and Science, Meenakshi Academy of Higher Education and Research, India. Email: anuradhar@maher.ac.in
[6] Associate Professor, Department of Commerce, SRM Institute of Science and Technology, Ramapuram Campus, Chennai, Tamil Nadu, India. Email: sabithakausik@g.mail.com, ORCID: 0000-8642-4282

Abstract
The increasing complexity of smart city infrastructures creates significant challenges for effective Information Technology (IT) governance, system reliability, and adaptive control. Smart city environments integrate heterogeneous components, such as Internet of Things (IoT) gadgets, communication networks, and cloud-based systems, with real-time analytics, thereby creating highly dynamic and interdependent systems. Conventional governance models often lack the computational intelligence and scalability required to manage large-scale, data-intensive environments. An Intelligent Control and Reliability-based IT Governance (ICR-IT Gov) model is proposed to enhance governance efficient with operational reliability in smart city ecosystems through the integration of data-driven intelligence and adaptive control mechanisms. Data collection is performed using distributed sources such as IoT sensors, network logs, and urban service platforms. Z-Score Normalization was employed for Data preprocessing to improve data quality and consistency. Independent Component Analysis (ICA) is employed for feature extraction to identify statistically independent patterns associated with anomalies and system reliability. The Modified Equilibrium Optimizer (ModEO) is utilized for feature selection and hyperparameter optimization, while Extreme Gradient Boosting (XGBoost) performs anomaly detection and risk prediction. The proposed model is implemented using the Python programming environment with machine learning and data analytics libraries for intelligent governance analysis and model optimization. A feedback-driven control mechanism enables dynamic policy adaptation and system stabilization. Experimental results demonstrate superior governance performance, achieving 96.8% prediction accuracy, 94.2% precision, and 96.7% recall, along with improved anomaly detection efficiency in smart city environments

Keywords: Internet of Things (IoT), Information Technology (IT) governance, Communication networks, Smart city environments.

1. Introduction

Smart cities make use of different technologies to guarantee that there is efficiency in the utilization of the available resources within cities. The use of information technology increases efficiency in different aspects, such as transportation, energy, and public utilities [1]. The introduction of IoT and artificial intelligence provided a chance for different cities to become smart cities. The market for smart cities worldwide is expected to grow tremendously due to increased IoT adoption [2].The use of IoT can help smart cities enhance the urban experience through enhanced services in sectors such as transportation, health care, energy usage, unusual activities, and the environment [3]. Through the use of IT and other tools such as information analysis, automation, and communication, smart cities can effectively manage their resources for the well-being of their citizens. As urban populations continue to grow, there is a need for smart cities to have strong IT governance

[4].The idea behind smart cities is becoming of the most crucial regions of investigation in urban planning, motivated by the increasing necessity for sustainable development, effective resource utilization, and enhanced living standards in urban areas. While smart cities offer numerous advantages to homeowners and investors, it also presents significant opportunities for cyberattacks that compromise the security of consumers [5, 6]. The integration of state-of-the-art technologies in smart cities aims to enhance service delivery and address various urban challenges, including anomalies and transportation issues. The IoT performs a crucial part in ensuring data collection, connectivity, and context-based decision-making [7, 8].

Research Aim: The proposed ICR-IT Gov) model integrates the Modified Equilibrium Optimizer (ModEO) for feature selection and hyperparameter optimization, with Extreme Gradient Boosting (XGBoost) for efficient anomaly detection and risk prediction in smart city IT governance environments.

Research Organization: Section 1 provides the background of the research. Section 2 focuses on reviewing existing research. Section 3 discusses the process of gathering data, preprocessing, and future extraction, as well as the proposed model. Section 4 includes result and discussion. Section 5 presents the performance, constraints, and future work in the conclusion.

2. Related Work

An authentication mechanism that ensures the safety and confidentiality of data for smart cities using Automated Validation of Internet Security Protocols and Applications (AVISPA) was examined [9]. AVISPA is a simulation tool utilized in formal analysis for smart cities. The results demonstrate that this scheme outperforms other related schemes, but it is limited by the processing power of IoT sensors. Research [10] focused on improving smart city urban living by improving a range of services, such as logistics. An Intelligent Parcel (iParcel) method, which employs piezoresistive sensors, predicts violations such as theft and damage. It improves tracking accuracy and enables condition monitoring to make the delivery process safe. However, its implementation is contingent upon IoT and blockchain integration. The incorporation of IoT sensor networks and AI analytics improves urban resilience and facilitates sustainable smart city development using an innovative methodology. Neural Network (NN) was explored [11] for evaluating Digital Transformation (DT) in smart cities. The results obtained indicate a considerable improvement with good performance in evaluating DT in local administrations with 80% accuracy. But still, the scalability of the methodology can be affected by some regional factors. Research [12] focused on automated anomaly detection in smart city surveillance systems without human intervention. The hybrid model comprising a 2D-Convolutional Neural Network (CNN) coupled with an Echo State Network (ESN) is used for detecting anomalies in smart city environment. The effectiveness of the model is significantly improved to execute roughly 30% better than other models. The use of edge computing devices limits their scalability. An AI-based method for enhancing cybersecurity in IoT smart cities with 5G networks that use the Long Short-Term Memory (LSTM) networks was analyzed [13] to identify anomalies in terms of space and reconstruction. The experimental results indicate that the proposed hybrid method performs improved than a traditional intrusion detection system (IDS) and a pure deep learning method. Deep learning methods require considerable computational resources, which is difficult for IoT-based devices. Anomaly prediction in smart cities' IoT systems using AI systems and the Technology Acceptance Model (TAM) was discussed in [14] to improve smart city resilience against cyber threats. There is an increase in anomaly detection efficiency by 30%, and the drawback is the condition scalability of AI technologies multi various urban settings.

Investigate [15] focused on IoT Network Security as well as data privacy through the use of the Quasi-Recurrent Neural Network (Q-RNN) method to identify online dangers in the network of IoT Smart city settings. The Q-RNN method achieves 8% more accurate results with 5 % lower false-positive rate in contrast to alternative models.IoT network usage for smart cities offers an opportunity to detect patterns and abnormalities from the dataset using the Improved Bacterial Foraging Optimization Algorithm with Optimum Deep Learning (IBFO-ODLAD),[16]. Experimental results indicate the efficiency of the IBFO-ODLAD algorithm with maximum accuracy of the dataset. An IoT system for anomaly detection and decision-making transparency in smart cities using the Explainable Artificial Intelligence (XAI) was developed in [17]. The research reveals considerable advancements in the field by improving the accuracy of anomaly detection via 25%. However, certain limitations remain, such as computational limitations, scalability issues, and privacy threats. Anomaly detection for IoT-based systems to ensure the security of wireless sensor networks (WSNs) in 6G-driven smart cities by using Variational Autoencoder-Long Short-Term Memory (VAE-LSTM) networks was analyzed [18].The result

achieves the highest accuracy in detecting malicious activities in low-latency systems. An IoT-based smart city improves urban resilience and sustainability using the reliability of the AE-LSTM method was analyzed [19] to predict anomalies in smart cities.The experimental evaluations and technology address important issues in urban energy management by improving energy efficiency by up to 50%. The use of low-power IoT devices creates some problems for large-scale deployment. IoT-Secure Fusion is two stages of protection framework for smart cities using the Autoencoder (AE), Variational Autoencoder (VAE), Generative Adversarial Network (GAN), and LSTM [20], to combine knowledge from the two data sources into a unified, practical security response. This model demonstrates a 15% improvement in network data accuracy is utilized with an impressive 20% improvement if sensor data is employed alone.

3. Methodology

An innovative computing method, ICR-IT Gov, the idea is for IT governance in IoT-enabled smart cities that addresses issues related to system control, reliability, and detection of anomalies. Data are sourced from different data sources, such as IoT devices, network logs, as well as urban services systems. To improve the quality of collected data, preprocessing procedures such as data normalization was used. The feature extraction method involves ICA to reduce complexity to find independent components in the signal. The proposed method combines the ModEO algorithm and XGBoost algorithm for effective anomaly detection and predictive modeling in smart cities (Figure 1).

3.1 Data Collection

The IoT-Enabled Smart City anomaly detection dataset it available on the Kaggle dataset Link: (https://www.kaggle.com/datasets/zara2099/smartcity-cybersecurity-iot-dataset). It consists of communication characteristics, energy consumption data, and security variables related to smart city IoT and edge networks. This dataset includes 19 columns with 1200 device ID's. The dataset also consists of IoT device features, communication parameters, energy consumption measures, and security variables. The proposed ICR-IT Gov model can be tested using 80% training and 20% testing data for anomaly detection and risk assessment in IoT based smart cities.

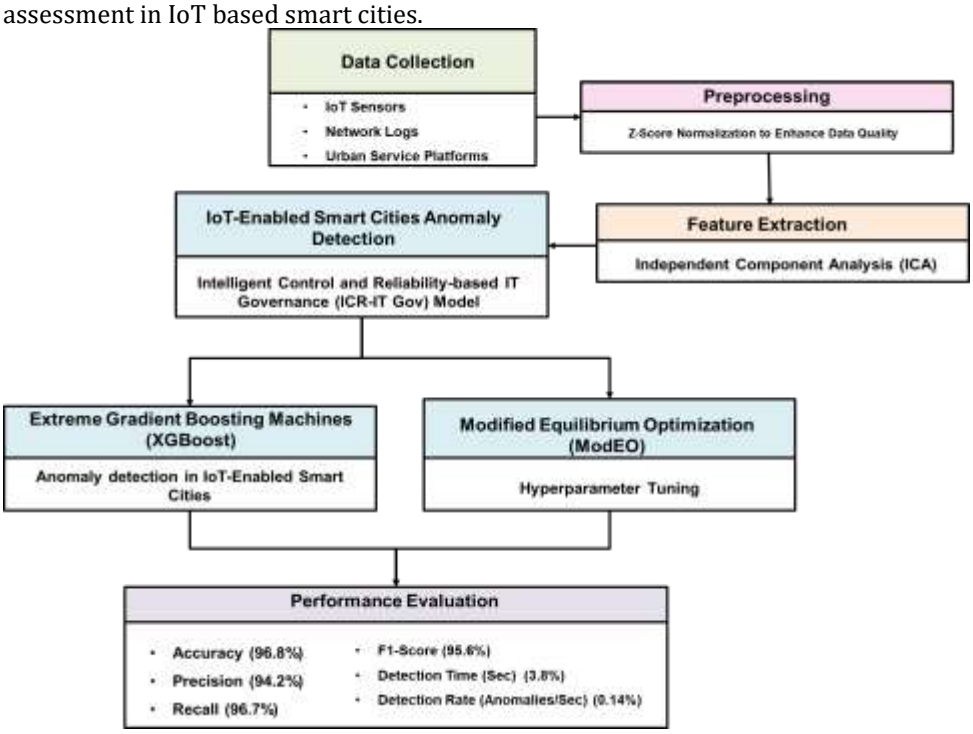

Figure 1: Methodology Workflow of IoT-Enabled Smart Cities for Anomaly Detection

3.2 Z-Score Normalization Technique for Preprocessing

In intelligent cities through IoT, enhancing the quality of data is essential to detect anomalies and perform IT governance effectively. In order to normalize various forms of data that are gathered from IoT devices, network

logs, and city service portals, the Z-score normalization technique transforms raw data into a score that is easily recognizable in Equation (1).

$$Y = \frac{W-v}{\sigma} \quad (1)$$

The standardized data used to detect outliers within IoT-Enabled smart cities is represented by Y, while a specific data point within the smart city framework can be expressed as W, where W represents the actual data point captured by IoT sensors, network traffic logs, or Urban Service Platforms. The average of the anomaly data points, represented by v, shows the central tendency of the data set and can be calculated from the values collected in the anomaly data set, σ quantifies the variability or dispersion of the anomaly data points around the mean.

3.3Feature Extraction using Independent Component Analysis (ICA)for Anomaly Behavior

The ICA algorithm is applied to find any sort of irregularity in IoT-enabled smart cities by decomposing complex signals and identifying statistically independent features that affect the performance of the system. The ICA algorithm is based on the concept that the observed signal can be expressed as a linear summation of statistically independent components, as shown in Equation (2).

$$Y = As \quad (2)$$

The composite inputs that exist from IoT sensors and smart city facilities are denoted as Y, which consists of individual components contributing to the overall efficiency of the system. A denotes the link between multiple inputs from anomalous data and the way they combine together to create the anomalous data input. s stands for the independent source components, which are non-Gaussian, statistically independent signals that underlie the observed data and are essential for spotting anomalies in the smart city system. The complex anomaly signals using ICA can help detect any hidden anomalies are expressed in Equation (3).

$$s = WY \quad (3)$$

The unmixing matrix, denoted by W, aids in extracting the independent components from the observed anomaly data.

3.4 IoT-Enabled Smart Cities Anomaly Detection Using the Intelligent Control and Reliability-based IT Governance (ICR-IT Gov) Model

The IC-R IT-Gov model provides an improved method for detecting anomalies in IoT-powered smart cities by utilizing intelligent algorithms and adaptive controllers. The suggested method makes use of ModEo optimization for hyperparameter-tuning and feature selection, together with the XGBoost machine learning algorithm, for anomaly prediction, accurate prediction, and reliable IT governance in smart cities.

Extreme Gradient Boosting Machines (XGBoost) for anomaly prediction in IoT Based Smart Cities: XGBoost is used to predict anomalies in IoT based smart cities, with the capacity to work well within the framework of large-scale and highly data-intensive system operations. XGBoost makes use of several decision trees to reduce anomaly prediction error as depicted in Equation (4).

$$\hat{z} = \sum_{l=1}^{L} e_l(w_j)\,, e_l \in E \quad (4)$$

The output of the ensemble model, which combines the predictions of every decision tree in the IoT system, is represented by $\hat{z}$, which is the projected value for anomaly detection. $e_l(w_j)$ represents the l^{th} decision tree's forecast, where w_j is the smart city's j^{th} input data point, such as IoT sensor anomaly data, and l is the upper limit of $\Sigma_{l=1}^{L}$ summing from L to $l = 1$. $\in$ is a subset of E that represents the collection of all decision tree functions utilized in the model, including the group of trees that collaborate to lower the error in anomaly prediction. Equation (5) defines each tree recursively to reduce anomaly errors.

$$e_l(w) = x_r(w: \theta_l) \quad (5)$$

$e_l(w)$ is the function of the l^{th} tree, which predicts anomalies in the smart city system based on input anomaly data w and model parameters θ_l, and x_r is the weight of anomaly prediction.Final prediction of anomalies is obtained by adding all tree predictions, as shown in Equation (6).

$$Z = \sum_{l=1}^{L} x_r(w: \theta_l) \quad (6)$$

Z denotes the ultimate forecast of anomalies in the IoT system, which is derived by adding the forecasts from every decision tree. The loss function with both loss term and the regularizer terms that control tree complexity anomaly errors is shown in Equation (7).

$$K(\Theta) = \sum_{j=1}^{M} K\left(z_j, \hat{z_j}\right) + \sum_{l=1}^{L} \Omega(e_l) + \lambda\|\Theta_l\|2 \quad (7)$$

$K(\Theta)$ is the total loss function, which controls tree complexity to avoid overfitting in anomaly detection by combining the prediction loss and the regularization component. $K\left(z_j, \widehat{z_j}\right)$ is the loss function that quantifies the difference between the true anomaly labels z_j and the predicted anomaly values $\widehat{z_j}$. $\Omega(e_l)$ refers to the regularizer term that helps to control its complexity to avoid overfitting. The $\sum_{j=1}^{M}$and $\sum_{j=1}^{L}$symbol denotes summation, whereby addition starts from 1, which shows that addition is done starting from the first data point for the anomalies, while $M$and Lstands for the total number of data points for the anomaly. $\lambda\|\Theta_l\|2$ represents the regularization parameter that is more suited for anomaly detection in smart cities, guarantees smoother decision boundaries, and lowers anomaly detection mistakes.

Hyperparameter Tuning with Modified Equilibrium Optimization (ModEO): In this research, the ModEO method is used for hyperparameter tuning it increase the precision of XGBoost in detecting anomalies. The concept of ModEO is a trade-off between exploration and exploitation when searching for the optimum solution, which becomes necessary to dealing with large-scale data in smart cities. As seen in the equilibrium pool model, the decrease of the equilibrium pool makes sure that at the beginning, exploration is the focus of search, while anomaly exploitation is prioritized later on. This procedure is mathematically expressed in Equation (8).

$$w_s = \{\overrightarrow{w_1^s}, \overrightarrow{w_2^s}, \overrightarrow{w_3^s}, \dots, \overrightarrow{w_l^s}, \overrightarrow{w_n^s}\} \quad (8)$$

w_s stands for the equilibrium pool, which is essential for anomaly prediction in IoT based smart cities as well as the selected potential solutions, such as hyperparameters or feature subsets, for anomaly optimization.$\overrightarrow{w_1^s}, \overrightarrow{w_2^s}, \overrightarrow{w_3^s}, \dots, \overrightarrow{w_l^s}$,represent each of the potential solutions for hyperparameter sets in the equilibrium pool during the anomaly investigation stage, and the anomaly population is denoted by $\overrightarrow{w_n^s}$, updating the equilibrium pool process expressed in Equation (9).

$$i = [\mu \times M \times \left(1 - \tfrac{l}{L}\right)] \quad (9)$$

To prioritize anomaly exploitation, i represents the number of candidates in the equilibrium pool at a particular iteration, which dynamically reduces with time. In hyperparameter tuning, μ represents the parameter that balances exploration and anomaly exploitation by regulating the initial number of particles in the equilibrium pool, and M is the total population of the optimization process.L is the total number of iterations of anomaly optimization (Equation 10).

$$\overrightarrow{w_n^s} = \frac{\overrightarrow{w_1^s} + \overrightarrow{w_2^s} + \overrightarrow{w_3^s} + \dots + \overrightarrow{w_l^s}}{l} \quad (10)$$

The updated anomaly population in IoT-enabled smart cities, denoted by $\overrightarrow{w_n^s}$and$\overrightarrow{w_1^s}, \overrightarrow{w_2^s}, \overrightarrow{w_3^s}, \dots, \overrightarrow{w_l^s}$, represents each of the potential solutions for hyperparameter sets in the equilibrium pool during the updated anomaly investigation stage.l represents the number of candidates in the equilibrium pool at an updated iteration for anomaly optimization.

Hyperparameter of proposed ICR-IT Gov: The optimized hyperparameters in the ICR-IT Gov model for governance of IT systems in IoT-based smart cities include the following values are the ModEO algorithm uses parameters such as the number of particles (N_p) = 30 and T_max = 100 is the maximum number of iterations, and exploration coefficient (A_coef) = 0.1-2.0 for exploration. The exploitation coefficient (β) is estimated within the limits of 0.2-0.9. Local search improvement, generation rate (G) = 1.0, to be used as well. As for the XGBoost, the algorithm used for anomaly classification in the ICR-IT Gov model uses a learning rate (η) = 0.001-0.30, the maximum depth of trees (D_max) = 3-15, and the number of estimators (N_est) = 50-500. There are also other hyperparameters, which include subsample ratio (S_sub) and regularization (α, λ).

4. Result and discussion

ICR-IT Gov model is highly effective in anomaly detection with the assistance of IoT based smart cities. Experiments carried out on the model revealed greatly improved anomaly prediction of F1-Score, recall, accuracy, precision, detection time (seconds), and detection rate (anomalies/seconds), which lowered system failures and increased governance efficiency, when compared with other models. The model adaptive control component enabled the framework to modify policies dynamically, which improved system stability and reliability within smart cities.

Experimental Setup: The ICR-IT Gov architecture for IoT-powered smart cities is evaluated using high-performance hardware and software to support efficient anomaly detection and IT governance management.

The system employs an Intel Core i9 or AMD Ryzen 9 processor, 32 GB DDR5 RAM, 1 TB NVMe SSD, and NVIDIA RTX 4080/4090 GPU with CUDA 12.0. The software environment includes Windows 11 Pro or Ubuntu 22.04 LTS, Python 3.11, Scikit-learn, XGBoost 2.0, TensorFlow, and PyTorch.

Exploratory Analysis: Figure 2(a) represents the correlation variables that are used for IoT security purposes and network operation, to detect anomaly dependencies and emphasize which variables are significant impacts on security threats and system operation. Figure 2(b) depicts the power consumption density of the nodes according to hardware, to make a comparison between the efficiency and consistency of the nodes. Figure 2(c) represents the probabilities of attack occurrence based on the probabilities of each type of anomaly attack, to classify normal behavior from abnormal behavior for prioritized security actions.

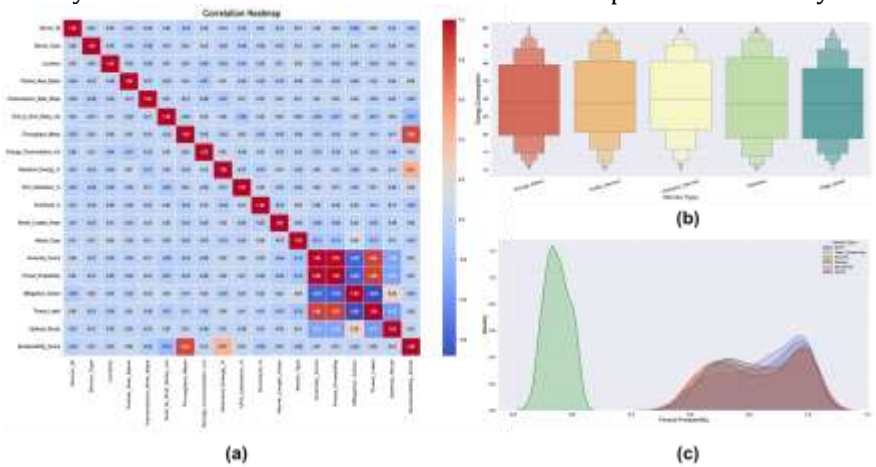

Figure 2: Exploratory Analysis of (a) Anomaly Detection Dependency, (b) Energy Consumption by Device Type, and (c) Anomaly Probability Density for IoT-Enabled Smart Cities

Evaluation Metrics: Accuracy metric provides a measure of anomaly predictions and helps determine the efficient of anomaly prediction in the model. The Precision of the model gives information about the proportion of actual positives to all number of positive anomalies, thus ensuring that there is no occurrence of any false anomaly positives. The Recall gives an assessment of the capability of detecting anomalies by the model. F1-Score determines the balance between the precision of positive anomalies and the recall of the capability of detecting anomalies. The specificity provides a measure of the system's anomaly behavior and the detection Time (Seconds) refers the time it takes for the anomaly detection system for handling data and identifies anomalies. In smart cities, the detection rate (Anomalies/Seconds) measures the capability of the system to identify anomalies using IoT data every second; emphasizing the process's effectiveness in handling vast data volumes while ensuring high sensitivity to anomalies.

Performance Evaluation: Table 1 and Figure 3(a &b) shows a comparative performance evaluation of the proposed ICR-IT Gov model for existing anomaly detection models, including AE, VAE, GAN, and LSTM methods adopted from existing studies [20]. The proposed model produces the best results with an accuracy of 96.8%, precision of 94.2%, recall of 96.7%, and f1-measure of 95.6%, which show a high level of reliability and effectiveness for the process of anomaly detection. Moreover, it also takes less detection time by 3.8 seconds, which shows the computational efficiency of the framework compared to other traditional methods. The stable detection rate is 0.14 anomalies per second, showing that the model has the potential to make highly accurate predictions without making many mistakes.

Table 1: Comparison Analysis of Existing and Proposed Methods

Methods	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Detection Time (Seconds)	Detection Rate (Anomalies/Seconds)
AE [20]	89.0	87.5	88.2	87.8	4.5	0.18
VAE [20]	88.5	87.2	89.1	88.1	4.8	0.17
GAN [20]	93.6	92.9	94.2	93.5	5.1	0.20

LSTM [20]	90.7	89.1	91.3	90.2	5.0	0.19
ICR-IT Gov [Proposed]	96.8	94.2	96.7	95.6	3.8	0.14

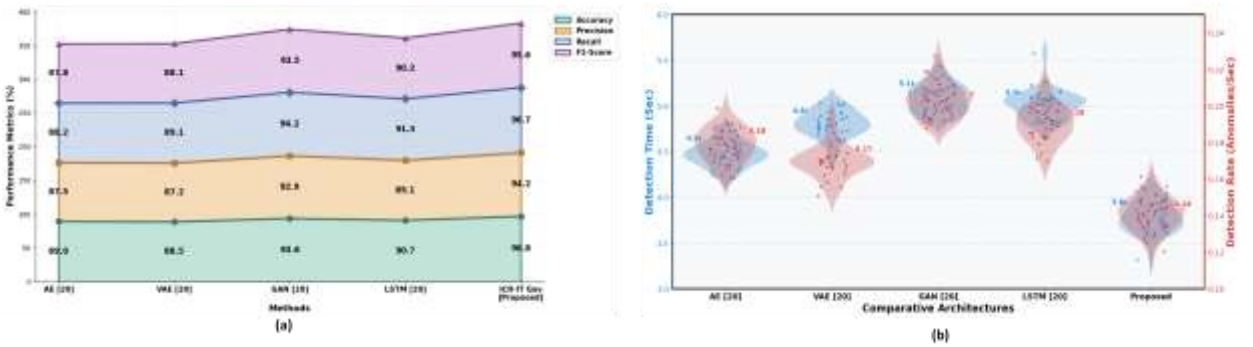

Figure 3: Performance Evaluation of Current and Suggested Techniques (a) F1 score values, Accuracy, Precision, Recall, and (b) Detection time and Detection Rate

Discussion: As a result, the suggested ICR-IT Gov model offers a highly sophisticated computation mechanism for IT governance within IoT-based smart cities, intending to increase efficiency, robustness, and ability to detect anomalies in the system. On the other hand, the AE [20] mechanism is not efficient enough in capturing complex data patterns, whereas the VAE [20] technique fails to capture interdependent data within IoT data sets. Likewise, the GAN [20] technique only concentrates on data synthesis and ignores IT governance and anomaly management processes.The LSTM [20] model also struggles in effectively handling the sequential nature of IoT data and demands greater computational power in large heterogeneous settings. In order to tackle these problems, the introduced ICR-IT Gov model leverages intelligent data analysis and adaptive control techniques to offer effective processing of IoT data. The application of the ModEO technique ensures better feature selection and tuning of hyperparameters, which leads to improved precision and stability. Furthermore, the anomaly detection algorithm based on the XGBoost algorithm ensures that abnormal behaviors are detected without unnecessary false alarms.

5. Conclusion

The suggested ICR-IT Gov model is a governance structure based on intelligence in the smart city environment that is constantly changing. This model makes use of various sources of information, such as IoT sensor data, network log information, and city utilities information, to enhance control over the system, ensure operational stability, and optimize the efficiency of governance. Data preprocessing steps such as normalization, are used to make sure that the quality of input data is high. Moreover, ICA is used for extracting features that have a substantial impact on system performance. The findings from the experiments indicate that the model developed shows marked improvement in its anomaly detection capability, with accuracies reaching 96.8%, precision levels at 94.2%, a recall rate of 96.7%, and an F1-score of 95.6%. The model also shows a detection time of 3.8 seconds and a detection rate of 0.14 anomalies per second. These findings validate the efficiency of the proposed model for improving IT governance, resilience, and security management in smart cities powered by IoT technology.Limitations include scalability issues, reliance on high-quality IoT data from the real world, and simulations. The future direction involves addressing adaptive real-time learning, distributed computing, explainable AI, and improved cybersecurity.

References

1. Alam, T., Gupta, R., Ahamed, N.N., Ullah, A. and Almaghthwi, A., 2024. Towards sustainable IoT-based smart mobility systems in smart cities. GeoJournal, 89(6), p.235. https://doi.org/10.1007/s10708-024-11227-y
2. Waqar, A., Barakat, T.A., Almujibah, H.R., Alshehri, A.M., Alyami, H. and Alajmi, M., 2025. Analytical approach to smart and sustainable city development with IoT. Scientific Reports, 15(1), p.23617. https://doi.org/10.1038/s41598-025-08861-y

3. Belli, L., Cilfone, A., Davoli, L., Ferrari, G., Adorni, P., Di Nocera, F., Dall'Olio, A., Pellegrini, C., Mordacci, M. and Bertolotti, E., 2020. IoT-enabled smart sustainable cities: Challenges and approaches. Smart Cities, 3(3), pp.1039-1071. https://doi.org/10.1007/978-3-031-39446-1_2
4. Wang, X., Yue, X., Tariq, N. and Sajid, A., 2025. Hybrid AI-and blockchain-powered secure internet hospital communication and anomaly detection in smart cities. Processes, 13(5), p.1466. https://doi.org/10.3390/pr13051466
5. Mohsen, B.M., 2024. AI-driven optimization of urban logistics in smart cities: Integrating autonomous vehicles and IoT for efficient delivery systems. Sustainability, 16(24), p.11265. https://doi.org/10.3390/su162411265
6. Shankar, A. and Maple, C., 2023. Securing the Internet of Things-enabled smart city infrastructure using a hybrid framework. Computer Communications, 205, pp.127-135. https://doi.org/10.1016/j.comcom.2023.04.008
7. Mutambik, I., 2025. Sustainable IoT-enabled parking management: A multiagent simulation framework for smart urban mobility. Sustainability, 17(14), p.6382. https://doi.org/10.3390/su17146382
8. Khalil, U., Malik, O.A., Hong, O.W. and Uddin, M., 2023. Leveraging a novel NFT-enabled blockchain architecture for the authentication of IoT assets in smart cities. Scientific Reports, 13(1), p.19785. https://doi.org/10.1038/s41598-023-45212-1
9. Kim, C., Son, S. and Park, Y., 2025. A privacy-preserving authentication scheme using PUF and biometrics for IoT-enabled smart cities. Electronics, 14(10), p.1953.https://doi.org/10.3390/electronics14101953
10. Balfaqih, M., Balfagih, Z., Lytras, M.D., Alfawaz, K.M., Alshdadi, A.A. and Alsolami, E., 2023. A blockchain-enabled IoT logistics system for efficient tracking and management of high-price shipments: A resilient, scalable and sustainable approach to smart cities. Sustainability, 15(18), p.13971.https://doi.org/10.3390/su151813971
11. Lloret, Á., Peral, J., Ferrández, A., Auladell, M. and Muñoz, R., 2025. A data-driven framework for digital transformation in smart cities: integrating AI, dashboards, and IoT readiness. Sensors, 25(16), p.5179.https://doi.org/10.3390/s25165179
12. Islam, M., Dukyil, A.S., Alyahya, S. and Habib, S., 2023. An IoT enable anomaly detection system for smart city surveillance. Sensors, 23(4), p.2358. https://doi.org/10.3390/s23042358
13. Reis, M.J., 2025. AI-driven anomaly detection for securing IoT devices in 5G-enabled smart cities. Electronics, 14(12), p.2492. https://doi.org/10.3390/electronics14122492
14. Zeng, H., Yunis, M., Khalil, A. and Mirza, N., 2024. Towards a conceptual framework for AI-driven anomaly detection in smart city IoT networks for enhanced cybersecurity. Journal of Innovation & Knowledge, 9(4), p.100601. https://doi.org/10.1016/j.jik.2024.100601
15. Priyadarshini, I., 2024. Anomaly detection of IoT cyberattacks in smart cities using federated learning and split learning. Big Data and Cognitive Computing, 8(3), p.21. https://doi.org/10.3390/bdcc8030021
16. Khayyat, M.M., 2023. Improved bacterial foraging optimization with deep learning based anomaly detection in smart cities. alexandria engineering journal, 75, pp.407-417. https://doi.org/10.1016/j.aej.2023.05.082
17. Khan, F.M., Zeb, A., Rahman, T., Al-Khasawneh, M.A., Daradkeh, Y.I., Siddiqui, I.F., Bashir, A.K. and Ullah, I., 2026. XAI-driven Data Mining for Self-defending IoT Systems: Enhancing Cybersecurity Transparency in the Age of Smart Cities. Cognitive Computation, 18(1), p.16. https://doi.org/10.1007/s12559-026-10559-w
18. Khan, W., Usama, M., Khan, M.S., Saidani, O., Al Hamadi, H., Alnazzawi, N., Alshehri, M.S. and Ahmad, J., 2025. Enhancing security in 6g-enabled wireless sensor networks for smart cities: a multi-deep learning intrusion detection approach. Frontiers in Sustainable Cities, 7, p.1580006. https://doi.org/10.3389/frsc.2025.1580006
19. Papaioannou, C., Dimara, A., Papaioannou, A., Tzitzios, I., Anagnostopoulos, C.N. and Krinidis, S., 2025. Hierarchical resources management system for internet of things-enabled smart cities. Sensors, 25(3), p.616. https://doi.org/10.3390/s25030616
20. Lilhore, U.K., Simaiya, S., Rahoof, P.P., Alroobaea, R., Baqasah, A.M., Alsafyani, M., Alhazmi, A. and Tekeste, L.G., 2025. Advanced threat detection for smart cities through IoT sensor and network data integration with IoT-securefusion. EURASIP Journal on Wireless Communications and Networking.https://doi.org/10.1186/s13638-025-02554-w