Inclusive Smart Cities: IoT-Cloud Solutions for Enhanced Energy Analytics and Safety

Abdulwahab Ali Almazroi[1], Faisal S. Alsubaei[2], Nasir Ayub[3], Noor Zaman Jhanjhi[4]
College of Computing and Information Technology, at Khulais,Department of Information Technology
University of Jeddah, Jeddah, 21959, Saudi Arabia[1]
Department of Cyber Security, College of Computer Science and Engineering
University of Jeddah, Jeddah, 21959, Saudi Arabia[2]
Department of Creative Technologies, Air University Islamabad, Islamabad 44000, Pakistan[3]
School of Computer Science SCS, Taylor's University SDN BHD, Subang Jaya, Selangor 47500, Malaysia[4]

***Abstract*—Securing smart cities in the evolving Internet of Things (IoT) demands innovative security solutions that extend beyond conventional theft detection. This study introduces temporal convolutional networks and gated recurrent units (TCGR), a pioneering model tailored for the dynamic IoT-SM dataset, addressing eight distinct forms of theft. In contrast to conventional techniques, TCGR utilizes Jaya tuning (TCGRJ), ensuring improved accuracy and computational efficiency. The technique employs ResNeXt for feature extraction to extract important patterns from IoT device-generated data and Edited Nearest Neighbors for data balancing. Empirical evaluations validate TCGRJ's greater precision (96.7%) and accuracy (97.1%) in detecting theft. The model significantly aids in preventing theft-related risks and is designed for real-time Internet of Things applications in smart cities, aligning with the broader goal of creating safer spaces by reducing hazards associated with unauthorized electrical connections. TCGRJ promotes sustainable energy practices that benefit every resident, particularly those with disabilities, by discouraging theft and encouraging economical power consumption. This research underscores the crucial role of advanced theft detection technologies in developing smart cities that prioritize inclusivity, accessibility, and an enhanced quality of life for all individuals, including those with disabilities.**

***Keywords*—IoT Security; theft detection; smart cities; cloud computing; disability support**

I. Introduction

Urban areas are undergoing a paradigmatic transition towards intelligent ecosystems, propelled by the incorporation of state-of-the-art technologies that fundamentally alter conventional urban terrains [1]. The integration of cloud computing and the Internet of Things (IoT) is driving a transformative change in the way cities function by establishing smart cities. This research article investigates the complex relationship between cybersecurity, smart energy analytics, and the incorporation of cloud and IoT technologies in smart city environments. The motivation behind the development of smart cities is the necessity to address the challenges presented by increasing populations and limited resources [2].

Smart cities, which are conceptualized as environments that promote innovation through the use of data, are built upon the integration of digital technologies, citizen engagement, and data-driven decision-making. Energy management emerges as a pivotal field in which optimization, sustainability, and resilience are paramount. Central to the smart city paradigm are cloud computing and the Internet of Things, which function as neural networks that empower municipalities to comprehend, assess, and intelligently respond [1], [3]. The IoT, by means of interconnected sensors and devices, supplies smart cities with real-time data that is vital, whereas cloud computing provides the necessary infrastructure and processing capabilities to analyze the enormous datasets produced by IoT devices [3]. These technologies have a significant impact on energy management by improving bidirectional connectivity and real-time monitoring for smart meters, smart grids, and Advanced Metering Infrastructure (AMI) [4]. However, the establishment of a fully operational smart energy environment continues to present obstacles, necessitating the implementation of strong security protocols to safeguard against data management complications, cyber risks, privacy apprehensions, and the resilience of cloud-based systems.

Intelligent energy analytics faces the difficulty of effectively managing enormous quantities of data [5]. This article highlights the significance of implementing a Demand Side Management System (DSMS) in smart cities as a means to improve energy efficiency, offer inventive resolutions, and exert efficient authority over energy consumption. DSMS developments, which include load shifting, economic planning, and system optimization, improve energy management precision and efficiency through the use of machine learning algorithms such as Grey Wolf Optimization (GWO), Long Short-Term Memory (LSTM), and Recurrent Neural Network (RCNN) [6].

Energy theft is a major concern, causing damage to infrastructure and leading to global economic hardship, despite progress. Detecting electrical theft promptly improves environmental safety by reducing the risks associated with illegal connections. This effort aims to encourage the implementation of sustainable energy practices, which will result in more affordable power and benefits for all residents, including persons with disabilities. The incorporation of advanced theft detection technologies into smart city infrastructure enables faster and more precise decision-making through the use of machine learning algorithms [7]. The Energy Theft Detection and Prevention System (ETDPS) sets a new benchmark in smart cities by ensuring its efficacy even in unmonitored households, therefore revolutionizing energy theft monitoring.

Research Gap: Overcoming Challenges in Smart City Data Analytics: Although there have been notable progress in smart city technologies, there are still some technological constraints that impede the complete utilization of data analysis in smart cities. The efficient management of the growing amount of data in smart cities greatly depends on strong data security and the use of advanced energy-related information systems. Nevertheless, even with these technological breakthroughs, there is still a crucial requirement to improve the performance of smart city infrastructure in order to attain maximum levels of efficacy and efficiency. The changing dynamics of intelligent city infrastructure sometimes exceed the capacity of existing optimization tools, requiring the creation of simpler ways for assessing restrictions. In addition, adapting machine learning models to process massive volumes of data poses considerable difficulties, particularly considering that scalability is essential for successful implementation in expansive urban regions. An important problem in machine learning approaches is the adoption of a "black box" design, which makes it difficult to understand the underlying processes, especially in vital industries like power management, where accountability and openness are crucial. The reliability of input data has a substantial influence on the outcomes of machine learning models, and inherent biases can undermine both the impartiality and precision of energy statistics. In order to effectively implement and improve data analytics systems in smart cities, it is crucial to tackle these obstacles. The objective of this study is to create new and creative methods to address the technological obstacles, therefore enhancing the efficiency and dependability of smart city infrastructure.

Field Contributions: This work adds significantly in several important areas:

1) Incorporation into Smart Cities Framework: The TC-GRJ paradigm effectively interacts with the smart cities architecture, specifically targeting security concerns associated with IoT devices. The use of advanced theft detection technology plays a significant role in the advancement of inclusive and interconnected smart city infrastructures.
2) Processing in the Cloud: Utilizing a cloud-based data processing technique improves computational efficiency in real-time theft detection in smart cities. Every person, including those with impairments, reaps the advantages of sustainable energy practices as a direct result.
3) Collection of Data from IoT Devices: The approach employed in the formulation of the conceptual framework involves gathering data from adaptive Internet of Things (IoT) devices to identify patterns of behavior in urban environments connected to the IoT. This promotes affordable electricity expenses that benefit both the general public and those with disabilities.
4) Dynamic adaptability to security challenges: The framework's capacity to accommodate intricate security issues in smart cities is exemplified by its division of theft into eight distinct categories. This approach demonstrates accuracy and efficiency in managing the growing threats to security.

This study enhances the existing comprehension and efficacy of security protocols in connected devices through the implementation of cutting-edge techniques and the improvement of larceny detection.

The subsequent sections of the paper are organized as follows: Section 2 provides an overview of the most recent advancements in the field of literature. Additionally, in Section 3, the issue that has been identified and emphasized in the work is discussed. The proposed materials and methods utilized to address the issue are detailed in Section 4. Section 5 discusses how the identified issue is resolved by the proposed model, which is simulated using experimental results. In Section 6, the article's concluding remarks are discussed.

II. Related Work

The current research analyzes how modern technologies could benefit living in cities in various kinds of methods, including specific focus on IoT, cloud-based computing, power, information analysis, and cybersecurity.Incorporating Internet Control Message Protocol information, a pioneering study [8] demonstrates the relevance of early recognition of power theft for security when operating urban intelligent environment. The system prevents complications and threats involved in illegal activities associations through employing sensitivity assessment and neural networks for recognizing and reduce efficient criminal activity. Furthermore, to raising stability, it additionally minimizes the entire energy expenses benefiting every citizen and includes those with handicap. In study [9], a connection between cloud systems and IoT in the evolution of smart cities is completely examined, especially emphasizing on the prerequisites of constant monitoring and immediate enhancements for IoT and cloud-based integration. Future research objectives and evaluating factors may become enhanced with the guidance of this study.

In study [10], obstacles to IoT adoption in smart cities in India are examined through the utilization of a hybrid multi-criteria decision-making methodology. The research identifies and evaluates fifteen barriers impeding the extensive adoption of the Internet of Things (IoT), providing policymakers with a systematic framework to facilitate informed decision-making. The investigation of traffic prediction in smart cities using long-term and short-term memory networks is detailed in study [11]. The research is centered around enhancing traffic management and reducing congestion through the development of precise prediction models for environmentally sustainable and intelligent urban transportation systems.

A proposed security system in study [12] addresses secure communication in IoT-driven smart cities using a detection concept. Utilizing neural network-based training, the system track local and global changes in the sharing of data among IoT devices in order to detect vulnerabilities in resource access and bolster overall security. Researcher in study [13] presents a thorough examination of machine learning techniques based on the Internet of Things (IoT) in diverse domains. The article illuminates the ways in which machine learning models have been implemented in the energy management, healthcare, agriculture, vehicle wireless networks, device security, and environmental sectors.

Energy statistics and dependability are the subject of the second compilation of works, which addresses the critical issue of energy theft in smart cities. In their study, [14] presents a data-driven approach that employs the hybrid Bagged Tree method to detect Non-Technical Losses (NTLs) resulting from deceitful customer conduct. The research highlights the criticality of surmounting challenges associated with the complexity of artificial intelligence algorithms designed for the purpose of detecting larceny. The authors in study [15] emphasize the significance of pattern identification and prediction error calculation in their examination of pattern formation utilizing LSTM models. The theft detection systems, which are essential for ensuring a consistent power supply and averting blackouts, contribute to the overarching objective of establishing urban environments that are more secure, intelligent, and efficient.

The study conducted by [16] investigates novel approaches to ensuring energy reliability and presents a methodology founded on Distributed Generation (DG). Utilizing photovoltaic modules, the study recommends installing renewable distributed generation units on the properties of customers. In order to address instances of fraudulently reported overcharging, the authors suggest implementing SCADA metering point-based solutions. The investigation of hardware-driven architecture and network-based topology for monitoring energy distribution in the Neighborhood Area Network (NAN) is detailed in study [17]. As an effort to improve energy management in smart cities, the authors propose a NAN strategy that includes a central master monitor for the complete energy supply.

This study examines the significance of variable transfer learning (TLs) and the properties of non-sequential auxiliary data. This anthology explores the complex issues and creative solutions found in the fields of energy data analysis, cybersecurity, the Internet of Things (IoT), and smart cities. Researchers from throughout the world are actively promoting the advancement of smart cities. Their contributions include identifying transgressions, predicting congestion, and detecting energy theft. The many ideas and methods discussed in these publications together contribute to the continuing discussion about creating urban settings that are smarter, safer, and more efficient.

III. Problem Statement

The fusion of IoT and cloud computing in smart energy data analysis is driving secure smart city development, presenting challenges that demand focused research. The influx of data in smart city ecosystems necessitates intelligent solutions for efficient processing to optimize resources, plan cities, and inform decisions [18]. Inefficient processing poses a threat to smart city futures, hindering innovations in energy efficiency, infrastructure design, and citizen services [19]. Energy theft is a critical challenge compromising the integrity of smart city energy infrastructures. This research proposes innovative methods integrating technology, security, and energy analytics to address challenges and meet future smart city standards. Early identification of electricity theft enhances safety, reducing the risk of incidents and hazards from unauthorized power connections [20]. Preventing theft lowers power costs and ensures a reliable supply, aligning with sustainable energy practices. Cutting-edge theft detection technologies contribute to inclusive smart cities, enhancing accessibility, mobility, and living conditions, especially for individuals with disabilities.

IV. Materials and Methods

Our strategy, combining machine learning and advanced data mining in IoT-Cloud solutions, fortifies smart cities against energy theft and enhances cybersecurity. In simulations, 20% data is for testing and 80% for training. The following sections detail our approach, with Fig. 1 illustrating the model. Detecting electricity theft early ensures safety and benefits all, including those with disabilities. It prevents mishaps and aligns with our goal of a secure smart city ecosystem. Guarding against theft makes power more affordable and aids equitable energy use, reducing financial burdens for everyone. Identifying theft promotes sustainable energy practices, benefiting all residents, especially those with impairments. Cutting-edge technologies for theft detection advance smart city creation and enhance inclusivity. Implementing theft detection systems prevents disruptions, ensuring a steady power supply, crucial for those relying on electric-powered technology. Our strategy aligns with inclusive urban design, acknowledging the transformative impact on the well-being of individuals with disabilities. To solve this problem, we have proposed a model comprises of differnt components including the preprocessing of input data from cloud, processing of the gathered data, check imbalancing, extraction of relevant features and then perform classification based on the TCN-GRU network.

A. Dataset Collection and Preprocessing

This study used a dataset obtained from the Open Energy Data Initiative (OEDI) [21], which is acquired from the Internet of Things (IoT). The dataset provides comprehensive information on energy consumption across 16 different categories, covering a period of 12 months. In order to replicate a wide range of energy theft situations, we have incorporated eight different forms of fraudulent activities into our analytical model, hence expanding the scope of our depiction. The use of IoT architecture enables the collection of real-time data, which facilitates a comprehensive analysis of energy consumption patterns. Fig. 2 provides a visual representation of the dataset. Initial preprocessing is conducted to assure the quality of the data by resolving concerns such as differences in size, missing values, and anomalies. The unprocessed data, obtained from intelligent meters and Internet of Things (IoT) devices, offers vital observations on energy consumption trends in smart urban infrastructures. The methods are shown numerically.

$$\text{normalized\_data} = \frac{\text{raw\_data} - \text{mean}}{\text{std\_dev}} \tag{1}$$

where, the original dataset is denoted by raw_data, the dataset mean is mean, and the standard deviation is std_dev. By ensuring that characteristics with varying sizes contribute equally to the ensuing analyses, normalizing the data helps to avoid variables with greater magnitudes from predominating.

Interpolation for Handling Missing Values and Outlier Removal [22]:

$$\text{interpolated\_data} = f(\text{observed\_data}) \tag{2}$$

$$\text{Data\_filtered} = \{\text{DT\_instance}_i \mid \text{DT\_instance}_i \notin \text{outliers}\} \tag{3}$$

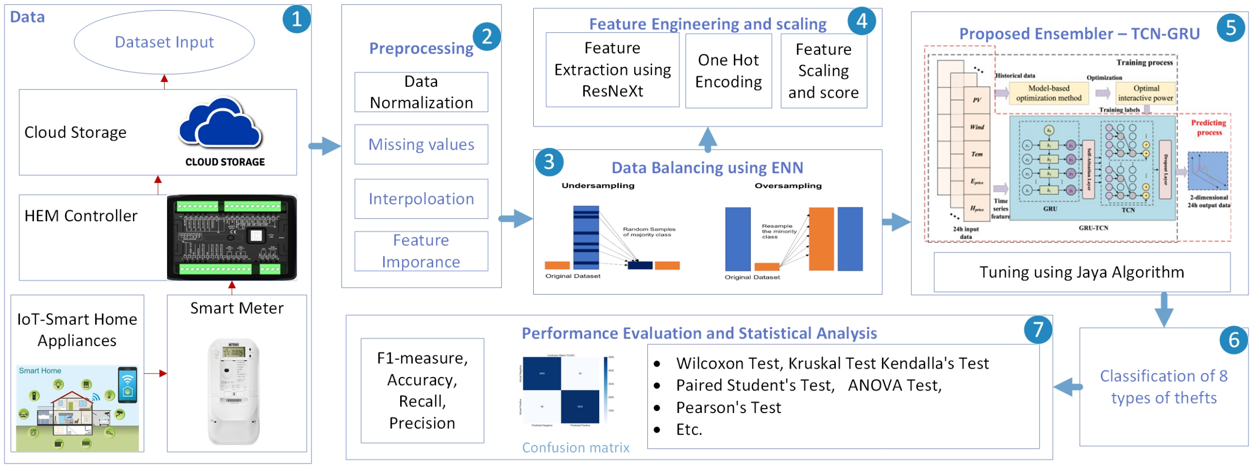

Fig. 1. Proposed system model of theft detection in IoT-SM data.

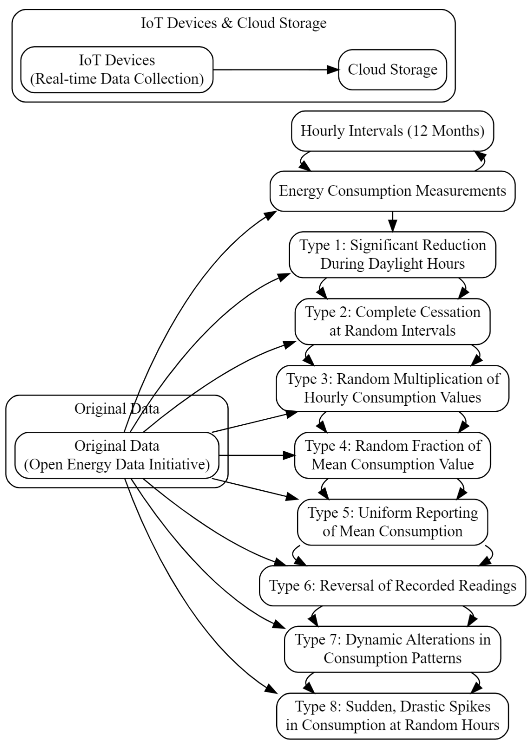

Fig. 2. Derived dataset broad overview.

Observed data, observed_data, undergo interpolation for missing values, ensuring a comprehensive dataset. DT_instance$_i$ instances have outliers removed to preserve integrity, enhancing dataset quality for valid inferences in further study.

B. Data Balancing using ENN

Addressing energy theft detection challenges in unbalanced datasets, we employ the Edited Nearest Neighbors (ENN) technique [23]. ENN adeptly navigates dataset complexities, effectively balancing irregular theft and consistent energy use patterns by pruning redundant information based on nearest neighbor concepts [23].

$$E_{\text{ENN}}(X, Y) = \{(x_i, y_i) \in X, Y \\ \mid x_i \text{ satisfies the ENN criterion}\} \tag{4}$$

Applying ENN to a dataset E_{ENN} modifies instances represented by X, with corresponding class labels Y as (x_i, y_i). ENN assesses an instance's significance based on its proximity to neighbors in the feature space. This technique balances the dataset, enabling the next machine learning model to better identify patterns associated with energy theft, enhancing accuracy and dependability in smart city settings.

C. Feature Extraction using ResNeXt

In order to analyze data from smart cities, it is essential to first do feature extraction, which involves taking the raw input information and identifying patterns and correlations. Modern Convolutional Neural Networks (CNNs) such as the ResNext architecture are used for this [24]. The following represents the feature extraction method mathematically: $\mathbf{X}_{\text{raw}}$ is the original input dataset. Its dimensions are $D \times F \times G$, where D is the number of channels and F and G are the input's width and length, respectively. ResNext's feature extraction process can be stated as follows:

$$\mathbf{X}_{\text{high-dim}} = \text{ResNext}(\mathbf{X}_{\text{raw}}; \theta_{\text{ResNext}}) \tag{5}$$

The mapping function that ResNext performs with learnable parameters θ_{ResNext} is denoted as $\text{ResNext}(\cdot)$ in this case. Hierarchical representations are captured by the high-dimensional feature tensor $\mathbf{X}_{\text{high-dim}}$, which is the output. ResNext uses a sequence of convolutional layers to extract features. The convolutional process with parameters θ_{Conv} can be represented as $\text{Conv}(\cdot)$. ResNext is hierarchical and consists of L convolutional layers followed by activation and normalization routines. The general procedure may be represented numerically as follows [24]:

$$\mathbf{Y}_l = \text{ReLU}(\text{BN}(\text{Conv}(\mathbf{Y}_{l-1}; \theta_{\text{Conv}_l}) \\ \theta_{\text{BN}_l}); \quad l = 1, 2, \ldots, L \tag{6}$$

In this case, $\mathbf{Y}_0 = \mathbf{X}_{\text{raw}}$, and the notations $\text{ReLU}(\cdot)$, $\text{BN}(\cdot)$, and $\text{Conv}(\cdot)$ stand for batch normalization, convolutional operations, and rectified linear unit activation, respectively. Concatenating the output tensors from each layer yields the final high-dimensional feature tensor $\mathbf{X}_{\text{high-dim}}$ [24]:

$$\mathbf{X}_{\text{high-dim}} = \text{Concat}(\mathbf{Y}_1, \mathbf{Y}_2, \ldots, \mathbf{Y}_L) \tag{7}$$

The resultant $\mathbf{X}_{\text{high-dim}}$ provides a rich and informative feature representation for further classification tasks, encapsulating complex spatial hierarchies and semantic representations.

D. Classification by Jaya Optimization-based TCN-GRU

The core of our proposed model lies in the fusion of Temporal Convolutional Networks (TCN) and Gated Recurrent Units (GRU), optimized through the Jaya optimization algorithm. Although TCN-GRU is highly adept at recognizing historical connections in data presented in sequence, it acts as an appropriate preference for assessing variations in electricity consumption continuously. Jaya optimization adjusts the model's assumptions for its greatest accuracy for recognizing cases of electrical theft, improving it's convergence and flexibility.

The set of inputs at time i will be expressed by A_i, though the stored state with time i is represented by B_i. The GRU equations are given by [25]:

$$C_i = \sigma(D_{AB}A_i + E_{AB}B_{i-1} + F_{AB}) \tag{8}$$

$$G_i = \sigma(D_{GB}A_i + E_{GB}B_{i-1} + F_{GB}) \tag{9}$$

$$H_i = \tanh(D_{HB}A_i + C_i \odot (E_{HB}B_{i-1}) + F_{HB}) \tag{10}$$

$$B_i = (1 - G_i) \odot H_i + G_i \odot B_{i-1} \tag{11}$$

Within each GRU problem, D_{AB}, D_{GB}, D_{HB} identify updated, reset, and candidate state hidden vectors. E_{AB}, E_{GB}, E_{HB} represent associated weight matrices. σ is the sigmoid function, and $\odot$ indicates element-wise multiplication. Collectively, these elements impact GRU dynamics and sequential input processing. The TCN component generates Y_i using:

$$Y_i = \text{softmax}(M_{HY}H_i + B_{HY}) \tag{12}$$

When Y_i is added in the classification, it signifies the model's prediction at time i. The softmax function processes H_i to determine the output. The weight matrix M_{HY} and bias term B_{HY} link the hidden state to the output, crucial for confidence and probability shaping. Jaya optimization reduces the cross-entropy loss in TCN-GRU parameter modification [26].

$$\mathcal{L} = -\sum_{k}^{N}\sum_{j}^{C} L_{k,j}\log(P_{k,j}) \tag{13}$$

In this context, C represents the total number of classes, and N signifies overall instances. Binary indicator $L_{k,j}$ discerns whether instance k corresponds to correct class j. Predicted probability $P_{k,j}$ expresses the model's estimation for k in class j. These facilitate comprehensive evaluation of TCN-GRU model's accuracy in identifying energy theft. Formulas govern iterative parameter adjustments through Jaya optimization [26].

$$M_i = M_i + N \cdot O \cdot (B_i - |A_i|) \tag{14}$$

$$A_i' = A_i + M_i \tag{15}$$

In our optimization method, symbols like M_i, N, O, and P_i are crucial. M_i represents present mobility, indicating solution change speed. Variable N controls acceleration, skillfully organizing modifications. O adds controlled randomness, injecting uncertainty. P_i guides the best solution domains. The TCN-GRU model, employing Jaya optimization, converges for accurate energy theft recognition. Fig. 3 shows TCGR-JA model.

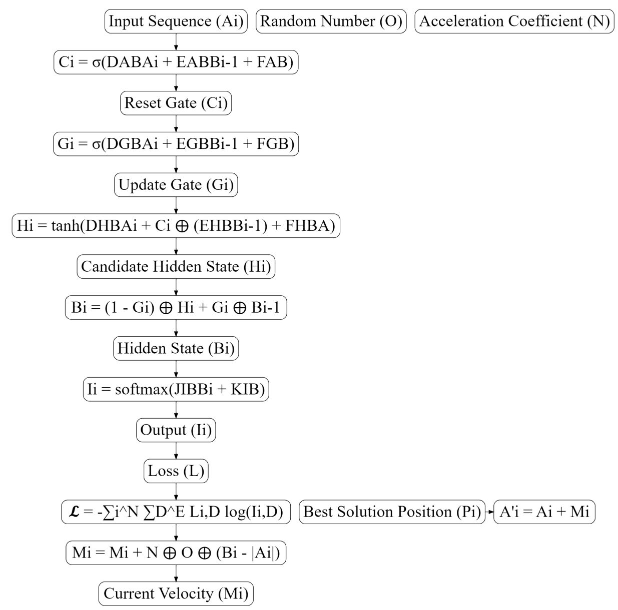

Fig. 3. TCGR-JA Model.

E. Significance of Statistical Analysis and Results Validation

Utilizing critical metrics including log loss, ROC-AUC, MCC, and PR-AUC, the efficacy of our method in averting energy theft in smart cities is meticulously evaluated [27], [28]. ROC-AUC and PR-AUC assess the predictive capability of the framework across various thresholds, whereas metrics such as MCC offer comprehensive insights into classification performance through the integration of specificity and sensitivity. In situations where probabilistic predictions are prevalent, the progressive increase in log loss indicates the precision of stochastic approximations. In order to substantiate the claims made, we utilize Pearson correlation tests to identify linear relationships, ANOVA tests to examine group variance, and Student's t-tests to identify pairwise comparisons. Our model endeavors to decrease energy theft and set a standard for cybersecure urban infrastructures by placing immense importance on these validation measures and performing comprehensive comparisons with prior related research. In order to make a significant contribution to the advancement of smart city technologies, we aim to empirically validate the model's dependability in real-world scenarios.

V. Simulation and Results

This section outlines our use of TensorFlow's powerful GPU in Google Colab to enhance ETDPS efficiency. Testing the architecture involved cloud-stored IoT datasets. Detailed results follow in subsequent sections. The initial exploratory data analysis (EDA) involves scrutinizing feature distribution, using visual aids to uncover trends. Though complex, this process equips decision-makers with deep insights, facilitating informed decisions despite model-building challenges.

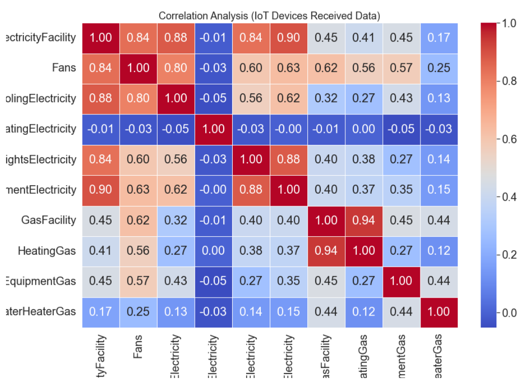

Fig. 4. Correlation analysis of the data received from IoT devices.

Quantitative dataset characteristics are depicted in Fig. 4, emphasizing patterns in IoT device data. The correlation research systematically uncovers connections, displayed on the heatmap. Ranging from -1 to 1, values indicate no link (0), opposing alliance (-1), or a perfect connection (1). Warmer tones denote more complex associations, enhancing the understanding of relationships.

Fig. 5 provides a clear visual depiction of the attribute distribution of the dataset, with each histogram corresponding to a different feature and providing a numerical value frequency. These histograms reveal the wide range of dataset features, providing a complicated view. In addition to being visually attractive, they serve as perceptive guides by highlighting anomalies and deviations that reveal important subtleties in the data. A brief summary of feature importance based on the Random Forest method is shown in Fig. 5, which also shows the effect of each variable on the prediction of theft. Greater impact is shown by taller bars that stick out. Shorter bars, however, have less of an impact. In order to effectively mitigate energy theft in smart city infrastructures, decision-makers may concentrate on key aspects by using this detailed analysis to inform resource allocation and intervention tactics.

Fig. 6 depicts a comparison of confusion matrices between our proposed model and existing methods. Our novel approach excels in theft detection accuracy with faster execution times, crucial for real-world responsiveness. Efficient cloud-based processing is a key feature, streamlining data acquisition from

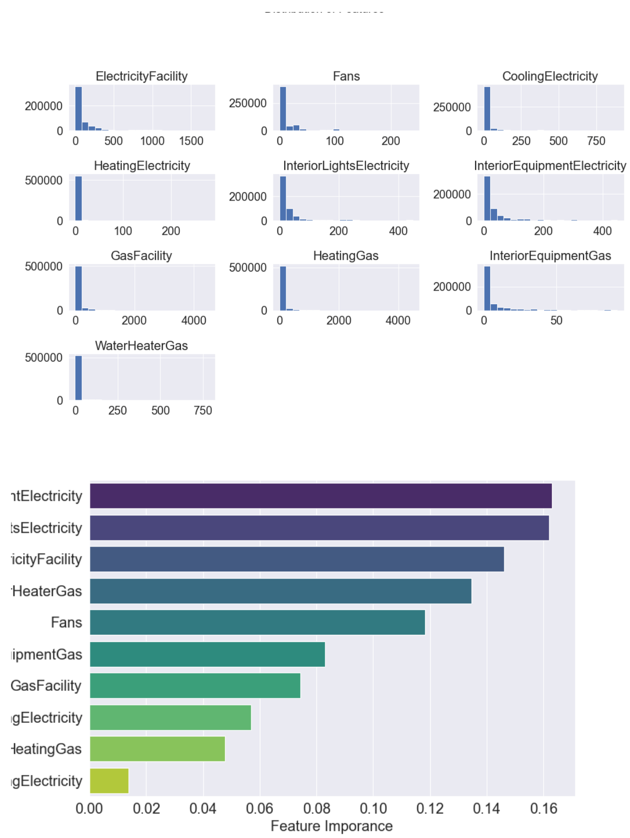

Fig. 5. Distribution of features and their importance calculated.

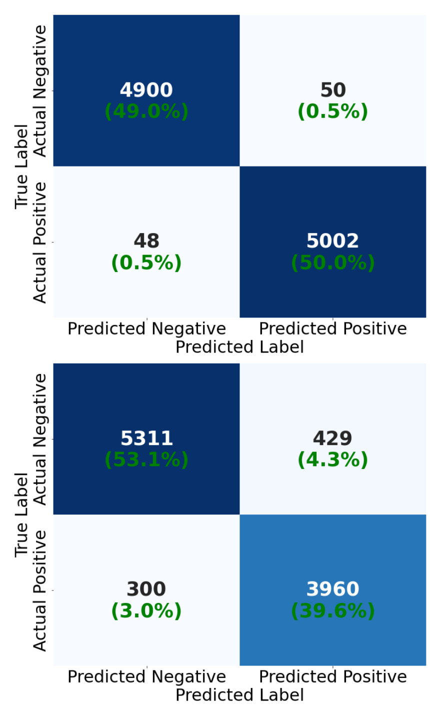

Fig. 6. Confusion matrix of the proposed model and BERT method used in literature.

IoT devices and reducing overall processing time for quicker

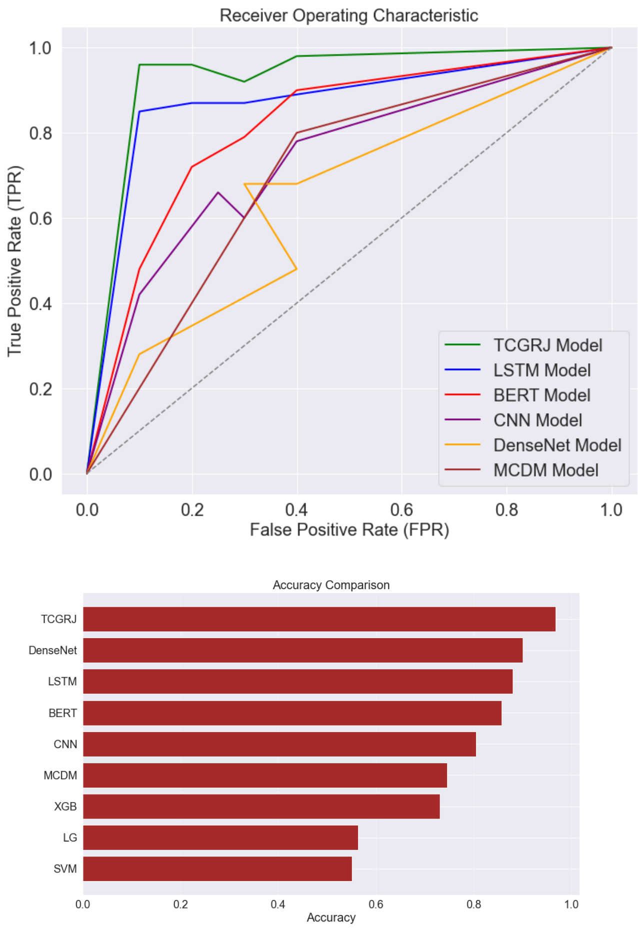

Fig. 7. ROC Curve and accuracy of the proposed VS Existing models on IoT-SM data.

theft identification.

The ROC curve with the highest AUC in Fig. 7 shows that the TCGRJ Model excels at distinguishing theft from normal situations. Using the IoT-SM dataset, Fig. 7 presents the accuracy values of numerous methods used in energy theft detection. Higher scores indicate better performance. Accuracy measures how well each technique detects instances of harmful behavior. Our proposed model TCGRJ performs in terms of accuracy.

Table I evaluates the TCGRJ model, highlighting its impressive 98.0% accuracy. This breakthrough positions TCGRJ as a highly effective approach for detecting theft activities in the IoT-based SM dataset, outperforming established models in multiple metrics.

Table II displays the average statistical analysis findings for theft detection techniques for the IOT-SM dataset. The proposed strategy, TCGRJ, performs better than current approaches on a number of statistical measures. With a Pearson correlation of 0.86, a Spearman correlation of 0.32, and a Kendall correlation of 0.89, TCGRJ performs better than its competitors. Moreover, TCGRJ demonstrates a strong correlation with a Chi-Squared test score of 18.4. These results validate the robust and dependable identification of stolen data on IoT devices by the proposed strategy.

TABLE I. PERFORMANCE EVALUATION RESULTS OF PROPOSED AND EXISTING METHOD ON IOT-BASED SMART METER DATA

Techniques	ROC	AUC	F1-Score	Precision	Log Loss	Accuracy	MCC	Recall
MCDM [10]	0.69	0.76	0.65	0.50	1.06	0.75	0.31	0.92
SVM [29]	0.70	0.77	0.65	0.50	0.99	0.55	0.31	0.92
LG [29]	0.71	0.79	0.66	0.51	0.98	0.56	0.31	0.93
XGB [29]	0.69	0.76	0.65	0.50	1.06	0.73	0.31	0.92
DenseNet [30]	0.91	0.96	0.91	0.86	0.21	0.90	0.85	0.90
CNN [20]	0.56	0.62	0.55	0.55	1.62	0.81	0.31	0.55
LSTM [31]	0.89	0.95	0.89	0.84	0.27	0.88	0.83	0.88
BERT [32]	0.92	0.97	0.91	0.87	0.20	0.90	0.85	0.91
TCGRJ	0.98	0.99	0.98	0.97	0.06	0.97	0.98	0.98

TABLE II. AVERAGE STATISTICAL ANALYSIS OF PROPOSED AND EXISTING MODELS

Techniques	Mann Whitney	Kruskal	ANOVA	Paired Student's	Student's	Chi-Squared	Kendall's
MCDM [10]	185.69	18.29	7.89	2.49	3.09	21.39	0.91
SVM [29]	109.99	10.79	4.79	1.59	1.99	13.19	0.64
LG [29]	120.59	11.79	5.29	1.79	2.29	14.99	0.66
XGB [29]	99.19	9.69	4.29	1.49	1.89	12.39	0.61
DenseNet [30]	142.79	13.89	6.09	1.99	2.59	17.29	0.73
CNN [20]	94.69	9.29	4.09	1.39	1.79	11.79	0.60
LSTM [31]	114.29	11.19	4.99	1.69	2.19	14.19	0.65
BERT [32]	191.89	18.79	8.19	2.69	3.29	22.69	0.92
TCGRJ	152.29	14.99	6.49	2.19	2.79	18.49	0.87

VI. CONCLUSION AND FUTURE WORK

With a primary focus on the IOT-SM dataset, our study advances intrusion detection in IoT systems. The TCGRJ model, a novel TCN-GRU architecture employing Jaya Optimization, holds promise for enhancing IoT security. Departing from the conventional approach of treating theft as a singular issue, we introduce a comprehensive categorization scheme distinguishing eight theft forms. This detailed method improves threat comprehension and fortifies the TCGRJ model's discriminatory capacity. Tailoring our ETDP to diverse theft forms overcomes the limitations of generic security solutions, making TCGRJ an effective defense against potential vulnerabilities. Our research contributes to malware detection in IoT environments, impacting privacy considerations. Preventing electricity fraud promotes safety, reduces hazards, and lowers costs, particularly beneficial for individuals with disabilities. Future work involves refining the TCGRJ model, exploring optimization opportunities, and ensuring broader applicability, scalability, and industry collaboration for comprehensive IoT security solutions.

Acknowledgment

The work was funded by the University of Jeddah, Jeddah, Saudi Arabia, under grant number (UJ-21-ICI-3). The authors, therefore, acknowledge with thanks the University of Jeddah for technical and financial support.

References

[1] N. K. Narang, *Sustainable Digital Transformation of Urban Landscape Through Disruptive Technologies and Standards*, *Building on Smart Cities Skills and Competences: Human factors affecting smart cities development*, pp. 95–122, 2022, Springer.

[2] S. E. Bibri, J. Krogstie, A. Kaboli, A. Alahi, *Smarter eco-cities and their leading-edge artificial intelligence of things solutions for environmental sustainability: A comprehensive systematic review*, *Environmental Science and Ecotechnology*, vol. 19, pp. 100330, 2024, Elsevier.

[3] W. Abu-Ulbeh, M. Altalhi, L. Abualigah, A. A. Almazroi, P. Sumari, A. H. Gandomi, *Cyberstalking victimization model using criminological theory: A systematic literature review, taxonomies, applications, tools, and validations*, *Electronics*, vol. 10, no. 14, pp. 1670, 2021, MDPI.

[4] A. Ziadeh, L. Abualigah, M. A. Elaziz, C. B. Şahin, A. A. Almazroi, M. Omari, *Augmented grasshopper optimization algorithm by differential evolution: A power scheduling application in smart homes*, *Multimedia Tools and Applications*, vol. 80, pp. 31569–31597, 2021, Springer.

[5] S. Aslam, N. Ayub, U. Farooq, M. J. Alvi, F. R. Albogamy, G. Rukh, S. I. Haider, A. T. Azar, R. Bukhsh, *Towards electric price and load forecasting using cnn-based ensembler in smart grid*, *Sustainability*, vol. 13, no. 22, pp. 12653, 2021, MDPI.

[6] A. A. Almazroi, C. A. Ul Hassan, *Nature-inspired solutions for energy sustainability using novel optimization methods*, *Plos one*, vol. 18, no. 11, pp. e0288490, 2023, Public Library of Science San Francisco, CA USA.

[7] A. A. Almazroi, M. Liaqat, R. L. Ali, A. Gani, *SLMAS: A Secure and Light Weight Mutual Authentication Scheme for the Smart Wheelchair*, *Applied Sciences*, vol. 13, no. 11, pp. 6564, 2023, MDPI.

[8] L. Westraadt, A. Calitz, *A modelling framework for integrated smart city planning and management*, *Sustainable Cities and Society*, vol. 63, pp. 102444, 2020, Elsevier.

[9] A. A. Almazroi, N. Ayub, *A novel method CNN-LSTM ensembler based on Black Widow and Blue Monkey Optimizer for electricity theft detection*, *IEEE Access*, vol. 9, pp. 141154–141166, 2021, IEEE.

[10] M. Sharma, S. Joshi, D. Kannan, K. Govindan, R. Singh, H. C. Purohit, *An Overview of Model-Driven and Data-Driven Forecasting Methods for Smart Transportation*, in *Data Analytics and Computational Intelligence: Novel Models, Algorithms and Applications*, pp. 159–183, 2023, Springer.

[11] S. Mrad, R. Mraihi, *A review of IoT application in a smart traffic management system*, in *2019 5th International Conference on Advances in Electrical Engineering (ICAEE)*, pp. 280–285, 2019, IEEE.

[12] N. Ayub, U. Ali, K. Mustafa, S. M. Mohsin, S. Aslam, *Predictive Data Analytics for Electricity Fraud Detection Using Tuned CNN Ensembler in Smart Grid*, *Forecasting*, vol. 4, no. 4, pp. 936–948, 2022, MDPI.

[13] S. Mishra, A. K. Tyagi, *The role of machine learning techniques in internet of things-based cloud applications*, in *Artificial intelligence-based internet of things systems*, pp. 105–135, 2022, Springer.

[14] A. Althobaiti, A. Jindal, A. K. Marnerides, U. Roedig, *Energy theft in smart grids: a survey on data-driven attack strategies and detection methods*, *IEEE Access*, vol. 9, pp. 159291–159312, 2021, IEEE.

[15] M. Irfan, N. Ayub, F. Althobiani, Z. Ali, M. Idrees, S. Ullah, S. Rahman, A. S. Alwadie, S. M. Ghonaim, *Energy theft identification using AdaBoost Ensembler in the Smart Grids*, *CMC-Computers, Materials & Continua*, vol. 1, no. 72, pp. 2141–2158, 2022.

[16] V. B. F. da Costa, B. D. Bonatto, *Cutting-edge public policy proposal to maximize the long-term benefits of distributed energy resources*, *Renewable Energy*, vol. 203, pp. 357–372, 2023, Elsevier.

[17] Y. Wu, H.-N. Dai, H. Wang, Z. Xiong, S. Guo, *A survey of intelligent network slicing management for industrial IoT: Integrated approaches for smart transportation, smart energy, and smart factory*, *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 1175–1211, 2022, IEEE.

[18] P. Pandiyan, S. Saravanan, K. Usha, R. Kannadasan, M. H. Alsharif, M.-K. Kim, *Technological advancements toward smart energy management in smart cities*, *Energy Reports*, vol. 10, pp. 648–677, 2023, Elsevier.

[19] P. Mishra, G. Singh, *Energy management systems in sustainable smart cities based on the Internet of energy: A technical review*, *Energies*, vol. 16, no. 19, pp. 6903, 2023, MDPI.

[20] Z. Muhammad, Z. Anwar, B. Saleem, J. Shahid, *Emerging cybersecurity and privacy threats to electric vehicles and their impact on human and environmental sustainability*, *Energies*, vol. 16, no. 3, pp. 1113, 2023, MDPI.

[21] Z. Salah, M. Alaeddine, M. Qaisar, S. Krichen, A. Haija, *Theft detection in smart grid environment*, *Mendeley Data*, vol. 1, 2022.

[22] M. N. Noor, A. S. Yahaya, N. A. Ramli, A. M. Mustafa Al Bakri, *Filling missing data using interpolation methods: Study on the effect of fitting distribution*, *Key Engineering Materials*, vol. 594, pp. 889–895, 2014, Trans Tech Publ.

[23] F. Yang, K. Wang, L. Sun, M. Zhai, J. Song, H. Wang, *A hybrid sampling algorithm combining synthetic minority over-sampling technique and edited nearest neighbor for missed abortion diagnosis*, *BMC Medical Informatics and Decision Making*, vol. 22, no. 1, pp. 344, 2022, Springer.

[24] S. Dou, Y. Liu, Y. Du, Z. Wang, X. Jia, *Research on Feature Extraction and Diagnosis Method of Gearbox Vibration Signal Based on VMD and ResNeXt*, *International Journal of Computational Intelligence Systems*, vol. 16, no. 1, pp. 119, 2023, Springer.

[25] C. Lea, M. D. Flynn, R. Vidal, A. Reiter, G. D. Hager, *Temporal convolutional networks for action segmentation and detection*, in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 156–165, 2017.

[26] E. H. Houssein, A. G. Gad, Y. M. Wazery, *Jaya algorithm and applications: A comprehensive review*, in *Metaheuristics and Optimization in Computer and Electrical Engineering*, pp. 3–24, 2021, Springer.

[27] M. Hossin, Md. N. Sulaiman, *A review on evaluation metrics for data classification evaluations*, *International Journal of Data Mining & Knowledge Management Process*, vol. 5, no. 2, pp. 1, 2015, Academy & Industry Research Collaboration Center (AIRCC).

[28] A. J. Bowers, X. Zhou, *Receiver operating characteristic (ROC) area under the curve (AUC): A diagnostic measure for evaluating the accuracy of predictors of education outcomes*, *Journal of Education for Students Placed at Risk (JESPAR)*, vol. 24, no. 1, pp. 20–46, 2019, Taylor & Francis.

[29] R. Xia, Y. Gao, Y. Zhu, D. Gu, J. Wang, *An efficient method combined data-driven for detecting electricity theft with stacking structure based on grey relation analysis*, *Energies*, vol. 15, no. 19, pp. 7423, 2022, MDPI.

[30] A. Naeem, Z. Aslam, T. Al Shloul, A. Naz, M. I. Nadeem, M. H. Al-Adhaileh, Y. Y. Ghadi, H. G. Mohamed, *A Novel Combined DenseNet and Gated Recurrent Unit Approach to Detect Energy Thefts in Smart Grids*, *IEEE Access*, 2023, IEEE.

[31] P. Pamir, N. Javaid, S. Javaid, M. Asif, M. U. Javed, A. S. Yahaya, S. Aslam, *Synthetic theft attacks and long short term memory-based preprocessing for electricity theft detection using gated recurrent unit*, *Energies*, vol. 15, no. 8, pp. 2778, 2022, MDPI.

[32] J. Shi, Y. Gao, D. Gu, Y. Li, K. Chen, *A novel approach to detect electricity theft based on conv-attentional Transformer Neural Network*, *International Journal of Electrical Power & Energy Systems*, vol. 145, pp. 108642, 2023, Elsevier.