EFFICIENT AND SECURE SMART CITY TRANSPORT MANAGEMENT WITH THE USE OF IOT AND DEEP LEARNING

[1]K.SOMASUNDARAM , [2]Dr.K.SELVAM

[1]Research Scholar,Department of Computer Applications
Dr.M.G.R Educational and Research Institute,E-mail:tnc_somu@rediffmail.com
[2]Professor and Dean, Department of Computer Applications
Dr.M.G.R Educational and Research Institute,E-mail:selvamk@drmgrdu.ac.in

Abstract

In recent times, smart cities have become an effective approach to providing excellent services to the population by efficiently using the resources at hand. While smart cities provide several benefits, ensuring security remains a significant obstacle that has to be addressed. The incorporation of Internet of Things (IoT) applications into the smart city management system, namely in the transportation sector, has the potential to greatly improve urban mobility, efficiency, and sustainability. In this paper, developed Attention-Based Bidirectional Long Short-Term Memory (ABiLSTM) for the efficient and secure data transmission in smart cities IoT based transmission. The proposed ABiLSTM incorporates attention-based scheme integrated with the Bi-LSTM for the data IoT data processing in smart cities. To improve security the ABiLSTM model uses the Advanced weighted AES model for the IoT transportation data encryption and decryption. The encrypted and decrypted data is processed with the Bi-directional LSTM architecture for the efficient and secure data transmission in the smart cities. The implementation is performed with the consideration of real-time IoT with consideration of bus, train and traffic light data in smart cities. Simulation results demonstrated that the ABiLSTM model exhibits a superior performance in terms of encryption and decryption efficiency. Specifically, ABiLSTM achieves an average encryption time of 0.000458 seconds and an average decryption time of 0.000109 seconds. This is notably faster compared to CNN's average encryption time of 0.002888 seconds and decryption time of 0.000327 seconds, and DL's average encryption time of 0.003320 seconds and decryption time of 0.000408 seconds. With the proposed ABiLSTM average data size for encryption is measured as 444bytes which is significantly less than conventional CNN and DL methods achieving 464 and 485 respectively. Additionally, ABiLSTM achieves higher classification performance in terms of accuracy, precision, recall, and F1-Score values of 0.975, 0.950, 0.994 and 0.792 respectively.

Keywords Smart City, Internet of Things (IoT), Transportation Management, Advanced Encryption Standard (AES), Deep Learning, Data Privacy

1. Introduction

Recently, the smart City Transportation model exhibited significant performance with the integration of Internet of Things (IoT) technology. The advancement in IoT technology exhibits a significant transformation towards urban transportation with the integration of sensors, connectivity, and data analytics with consideration of various parts incorporated in the infrastructure of transportation [1]. The advancement in transportation management systems facilitates real-time information monitoring and traffic flow management with the transit of

public and fleets in vehicles to improve the efficiency of operation with reduced congestion. Also, the advancement incorporates effective traffic signals for the dynamic management of traffic with smart parking management for guidance of drivers for the space availability through integrated platforms for real-time information and predictive analytics for efficient communication [2]. With effective advancement in Smart City Transportation integrated with IoT provides advancement in autonomous vehicles and mobility. IoT provides the seamless technology for communication with vehicles between each device through effective infrastructure for traffic maintenance with appropriate safety and roads coordination. IoT data collection involved in construction of personalized and adaptive transportation to manage transit system responsiveness with modification of real-time users' modification in routes and scheduling [3]. The implementation of IoT environment with other technologies incorporates Artificial Intelligence (AI) and Big Data Analytics to improve the patterns prediction of traffic, optimization of traffic and minimized environmental factor [4].

Smart City integrated with IoT subjected to security challenges due to intricate and multifaceted network for the interconnection of devices and systems [5]. The primary factor associated with IoT environment focused on data privacy for the collection of IoT devices and process large data for the sensitive information processing, strict measures of information for the effective unauthorized access and misuse of information. The vulnerability in IoT devices subjected to risk as vast range of devices in IoT environment minimizes the processing power for the features in security those are considered as target for the attacks. Other hand, network security is considered as the critical issue where one part of breach affects the entire network. It demands for the authentication and access control scheme for the security in the infrastructure to prevent the manipulation of the entire network [7]. The update of firmware and software also challenging to prevent the vulnerability of system those updates are not handled effectively and correctly [8]. The issues in the IoT devices comprises of the interoperability for the various manufactures to overcome security concern and physical factors those are deployed in public or remote areas in smart cities those are identified as the vulnerable to security environment. Additionally, in the smart cities transportation environment compliances and regulations adds security issues in the smart cities [9].

The transportation system with IoT in smart cities provides significant performance in the large devices those are interconnected for data management [10]. The fundamental factor associated with the transportation system uses the encryption associated for the effective data transmission and storage to process sensitive information those are confidential and security for the unauthorized access. Multi-factor authentication (MFA) is considered as the critical method for the improving access control with the multiple verification for the system access environment [11]. With the conventional software and firmware critical step is addressing the vulnerabilities and security flaws for protecting devices from the threats. Intrusion Detection System (IDS) integrated with network segmentation model comprises of the data monitoring and isolation of certain threats and preventing the network for the security [12]. Additionally, with the security scheme comprises of the devices those are authorized and software those are unaltered offers robust security in physical environment for data protection to prevent tampering and theft. With implementation of industry standards and regulations security practices are utilized for the data protection in smart city data [13].

Within the smart cities IoT data deep learning technology offers advanced analysis and decision-making process in different area of the security in smart cities. The smart city environment with deep learning algorithm process the vast range of data collected from IoT devices those need to be protected and secured [14]. The deep learning mode with the examination of real-time data effectively manage the traffic in network those obtained information are obtained with traffic cameras, sensors to minimize flow of traffic and congestion with predictive based adaptive signalling. In case of factors related to public safety

deep learning improves the performance of surveillance system for the detection of anomaly for prevention of security threats [15]. In management of smart city transportation data deep learning algorithm is implemented for pattern estimation, distribution of energy and effective energy sources. The deep learning model with continuous monitoring allows personalized and responsive services in smart cities.

Smart cities implemented with deep learning model exhibits significant performance for detection of threat, identification of anomaly and predictive analytics. Through extensive analysis of data collected from IoT devices using sensors and devices comprises of deep learning algorithm for estimation of patterns or behaviours to withstand the potential threats and security breaches [16]. Smart cities use the deep learning model for the surveillance system with deep learning for image and video analysis for the estimation of activities those are suspicious and identify the faces to achieve higher accuracy for the safety. IDS integrated with deep learning estimates the network intrusion than the conventional methods to prevent threats [17]. In smart infrastructure deep learning model predict and security vulnerabilities for examination of historical data for processing of real-time data. Additionally, deep learning model in smart cities increases the authentical process in the smart cities for biometric verification for different applications such as face and fingerprints to offer authorized individual system in critical environment [18].

This paper contributed for the effective transportation system in smart cities with the uses of the proposed ABiLSTM for the smart cities. The proposed ABiLSTM model uses the attention scheme for transportation in smart cities. This paper uses real-time data like traffic light, bus, and train data in smart cities. Through the generated data attention mechanism is implemented along with the weighted AES cryptography scheme for data security and privacy. The developed weighted AES model with the attention scheme is implemented with a deep learning model for the management of the data and security. The results analysis demonstrated that the proposed ABiLSTM model exhibits superior performance than the conventional technique of Convolutional Neural Networks (CNN) and Deep Learning (DL). The performance of ABiLSTM is effective for the encryption/decryption speed and data size. The proposed ABiLSTM model achieves an encryption time of 0.000458 and a decryption time of 0.000109 seconds.

2. Literature Review

Smart city environment with IoT comprises the deep learning model in the urban environment for the cyber and physical threats. Smart cities with IoT communication incorporate more services than traditional security measures for complex and modern threats. Recently, traditional researchers showcased transformative models for deep learning in security environments. Researchers expressed that the deep learning model algorithm significantly increases anomaly detection in network monitoring for traffic management more than the traditional methods to achieve intrusion in the network. Bhowmik et al. (2022) evaluate the management of privacy in smart cities using deep learning and machine learning to evaluate the importance of sensitive data information processing. Similarly, Dogra and Kaur (2022) examined the machine learning process in IoT-based smart transportation to increase security and efficiency in smart city management. Hameed et al. (2022) developed a deep learning model with multi-classification in IoT traffic monitoring for effective traffic management in smart cities for the management of traffic and security. Bhardwaj et al. (2022) examined the deep learning-based cybersecurity model for smart cities for the vast range of applications and advancements. Li et al. (2022) discussed the contribution of big data analytics in deep learning for smart cities. The model uses the digital twin's technology for the analysis for improved predictive maintenance and security. Jiang et al. (2022) examined a deep learning model environment for smart logistics to improve operational efficiency and security. Ajay et al. (2022) designed an intelligent, eco-friendly transport management systems, in cause of

intelligent transportation deep learning model increases the security. Ullah et al. (2024) examine the intersection of IoT, machine learning, and data-centric smart environments, providing insights into how these technologies are advancing the development of secure smart cities. Prawiyogi et al. (2022) and Djenouri et al. (2023) explore applications of machine learning and federated deep learning, respectively, in improving smart city security. Additionally, Mohanta et al. (2022) address accident prediction in IoT-enabled transportation systems, while Al-Qarafi et al. (2022) investigate privacy-preserving blockchain solutions. Rashid et al. (2022) discuss adversarial training for deep learning-based cyberattack detection, and Musa et al. (2023) review challenges and recommendations for sustainable traffic management using IoT-oriented intelligent transportation systems.

With extensive analysis of existing literature such as those by Bhowmik et al. (2022) and Bhardwaj et al. (2022) demonstrate the application of deep learning models for privacy management and cybersecurity, there is a limited exploration of how these models can be seamlessly integrated across heterogeneous IoT devices and systems with varying security requirements. Additionally, Hameed et al. (2022) and Li et al. (2022) exhibited advancements in traffic management and digital twins, there is a lack of comprehensive research on the scalability of deep learning solutions in handling the enormous and dynamic data generated by smart city IoT networks. The literature also reveals a need for more studies on the effectiveness of federated deep learning models, as discussed by Djenouri et al. (2023), in addressing privacy and security concerns in decentralized IoT environments. Furthermore, while current research addresses specific applications such as smart transportation and logistics, there is insufficient focus on the interoperability of deep learning-based security solutions across different domains of smart cities. The integration of privacy-preserving techniques and blockchain, as explored by Al-Qarafi et al. (2022), also requires further investigation to evaluate its practical implications and effectiveness in real-world scenarios. The identification of limitations associated with the implementation of deep learning in smart cities for security needs broader analysis. Hence, this research focused on the construction of a deep learning-based efficient security scheme for the smart cities transportation with IoT connections.

The advanced level of security algorithms of distributed system, cloud system were discussed with various innovative approaches like hybrid cryptography [20], blockchain technology[21], edge computing [22] and cyber physical systems [23].

3. Proposed Attention-Based Bidirectional Long Short-Term Memory (ABiLSTM)

The proposed ABiLSTM model real-time data for the evaluation of IoT based transportation in smart cities. The proposed ABiLSTM mode uses the conventional Bidirectional Long Short-Term Memory (BiLSTM) integrated with an attention mechanism for the computation of contextual and temporal data computation Within the BiLSTM collected IoT data is processed with the transport devices in forward and backward estimation for the evaluation of dependencies. With the incorporation of the attention mechanism, significant time stamps within the modules are computed for the relevant information processing. The BiLSTM component can be expressed as in equation (1) and (2)

$$\overrightarrow{h_t} = LSTM\left(\overrightarrow{h_{t-1}}, x_t\right) \tag{1}$$

$$\overrightarrow{h_t} = LSTM\left(\overrightarrow{h_{t+1}}, x_t\right) \tag{2}$$

In equation (1) and (2) $\overrightarrow{h_{t-1}}$, and $\overrightarrow{h_{t+1}}$, denoted the LSTM forward and backward state in a hidden state and x_t represented the input data time step those represented as t. The context vector of the attention mechanism is stated as c_t those are represented in equation (3) – (5).

$$c_t = \sum_{i=1}^{T} \alpha_{t,i}, h_i \tag{3}$$

$$\alpha_{t,i} = \frac{exp(e_{t,i})}{\sum_{j=1}^{T} exp(e_{t,i})} \tag{4}$$

$$\left(e_{t,i}\right) = Score\left(h_i, S_{t-1}\right) \tag{5}$$

In equation (3) – (5) $\alpha_{t,i}$ represents the attention weights, $e_{t,i}$ is the alignment score, and $Score$ is a function determining the relevance of each hidden state h_i to the current time step. To evaluate the privacy requirement in IoT transportation in smart cities proposed ABiLSTM model uses the Advanced Encryption Standard (AES) with the weights for the data protection. The weighted AES model encrypt the IoT transportation data for the effective analysis. The AES algorithm with the weights are defined in equation (6) and (7)

$$C = WAES(P, K) \tag{6}$$

$$P = WAAES^{-1}(C, K) \tag{7}$$

In equation (6) and (7) C is the ciphertext, P is the plaintext, and K is the encryption key. The weighted AES encryption is applied to user data before it is fed into the ABiLSTM model, preventing unauthorized access and data breaches. The figure 1 illustrates the overall process involved in the proposed ABiLSTM model for the transportation data security in smart cities.

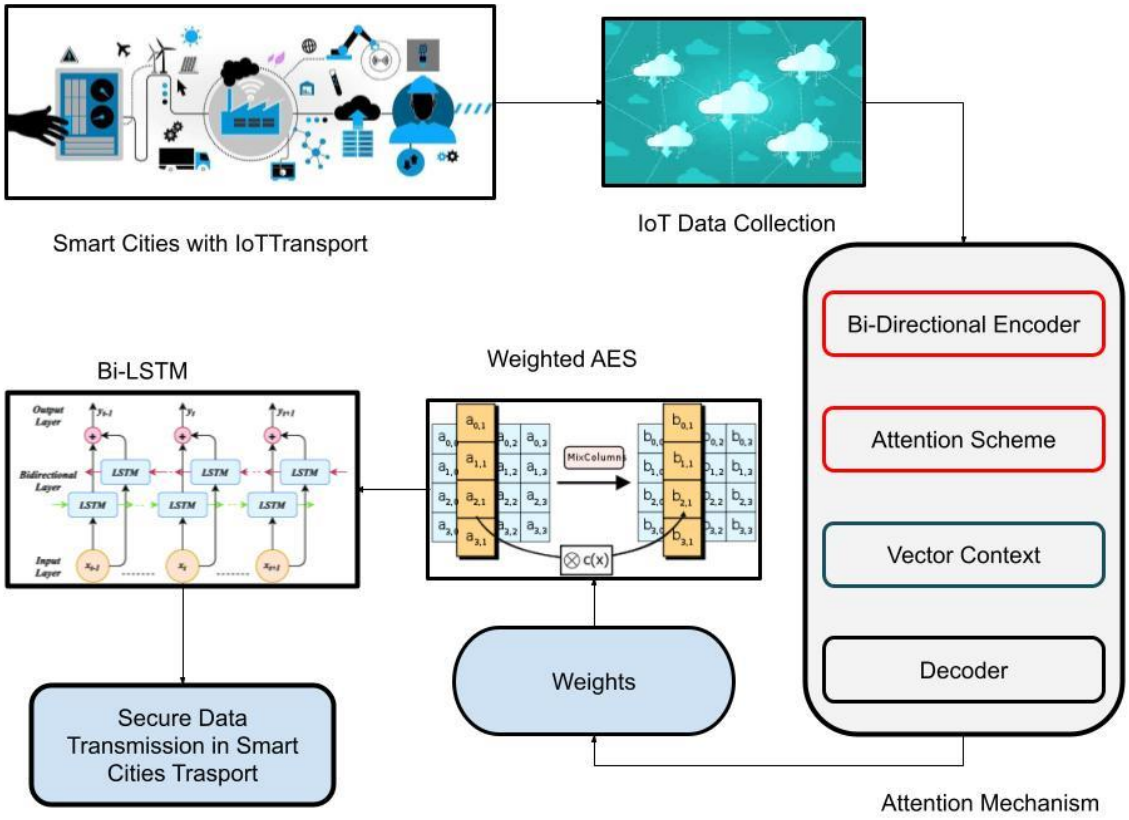

Figure 1: IoT data secure architecture for smart city transportation with ABiLSTM

The ABiLSTM model's enhanced capabilities in handling temporal and contextual information significantly improve its predictive power for traffic management in smart cities. Through bidirectional processing, the model captures dependencies in both past and future data sequences, allowing it to forecast traffic patterns and identify potential congestion points more accurately. The attention mechanism adds another layer of complexity by enabling the model to focus on critical time steps or events that have a greater impact on traffic flow, thus enhancing the decision-making process as shown in Figure 1. The integration of WAES encryption into the ABiLSTM framework ensures that the data used for predictive analytics is kept secure. AES is a symmetric key encryption algorithm known for its high level of security and efficiency. The integration of weights with AES encrypts data before it is processed by the ABiLSTM model, thus protecting it from unauthorized access or tampering. The decryption process occurs only when the data needs to be analyzed, ensuring that sensitive information

remains confidential throughout its lifecycle. The encrypted data C is input into the ABiLSTM model for analysis. During this stage, the model processes the data as usual, but the actual content remains protected.

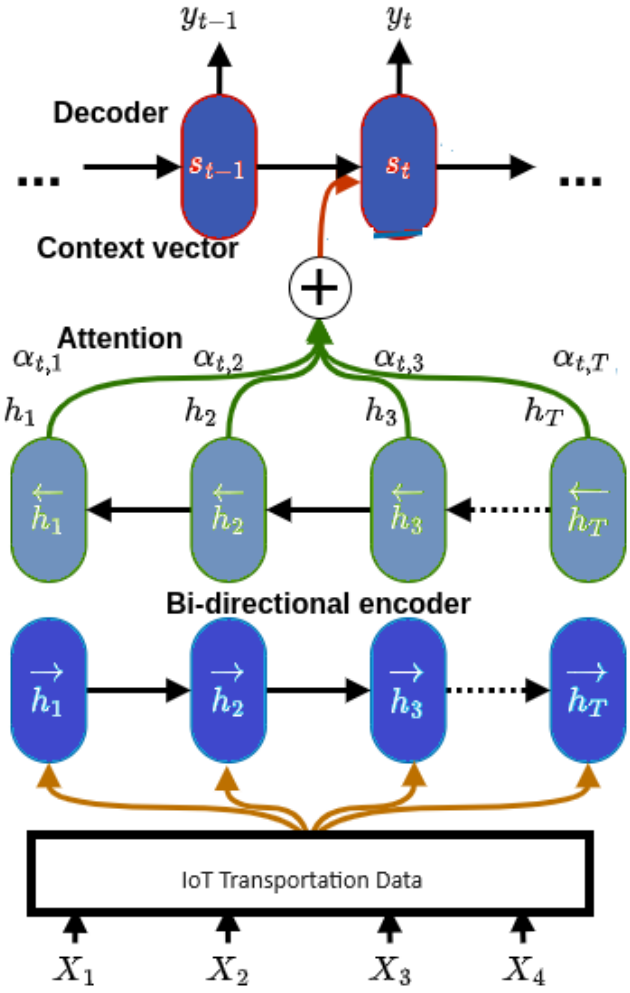

Figure 2: Attention Mechanism in ABiLSTM

The attention mechanism in IoT systems, particularly in the context of deep learning models like the ABiLSTM, is designed to enhance the model's ability to focus on important parts of the input IoT data sequence as shown in Figure 2. This is crucial for applications such as traffic prediction and anomaly detection, where certain time steps or data features are more relevant than others. For each time step t in the input sequence, the mechanism calculates an alignment score $e_{t,i}$ between the current state $S_{t-1}$and each hidden state h_i from the sequence. This score determines how well the hidden state at position iii aligns with the current state at time t stated in equation (8)

$$e_{t,i} = Score(h_i, S_{t-1}) \tag{8}$$

In equation (9) $score$ is a function that computes the compatibility between $h_i$and S_{t-1}. The ABiLSTM model uses the scoring function as a dot product for the conversion in SoftMax layer in attention scheme with weights $\alpha_{t,i}$. The scores that are aligned are converted as the weights for the attention denoted as $\alpha_{t,i}$ with the normalization of weights, those are summed equal to 1 as probability values. Within ABiLSTM model attention scheme integrated with LSTM architecture for the temporal estimation for the prediction in the data sequences. Assume the IoT transport sequences of hidden states $h_1, h_2\ and\ h_3$ and corresponding alignment scores c_t, the context vector is calculated using equation (9)

$$c_t = \alpha_{t,1}h_1 + \alpha_{t,2}h_2 + \alpha_{t,3}h_3 \quad (9)$$

Through the attention model, the weights in the hidden state are computed based on the context vector based on average values in the hidden state for the higher weights values.

3.1 Secure Bidirectional Long Short-Term Memory for IoT Transportation in Smart Cities

The ABiLSTM model uses the attention model for the IoT transportation data integrated with BiLSTM combined with the Weighted AES for the data processing in forward and backward estimation. This estimates the dependencies in IoT applications for the computation of prediction and analysis of data sequences.

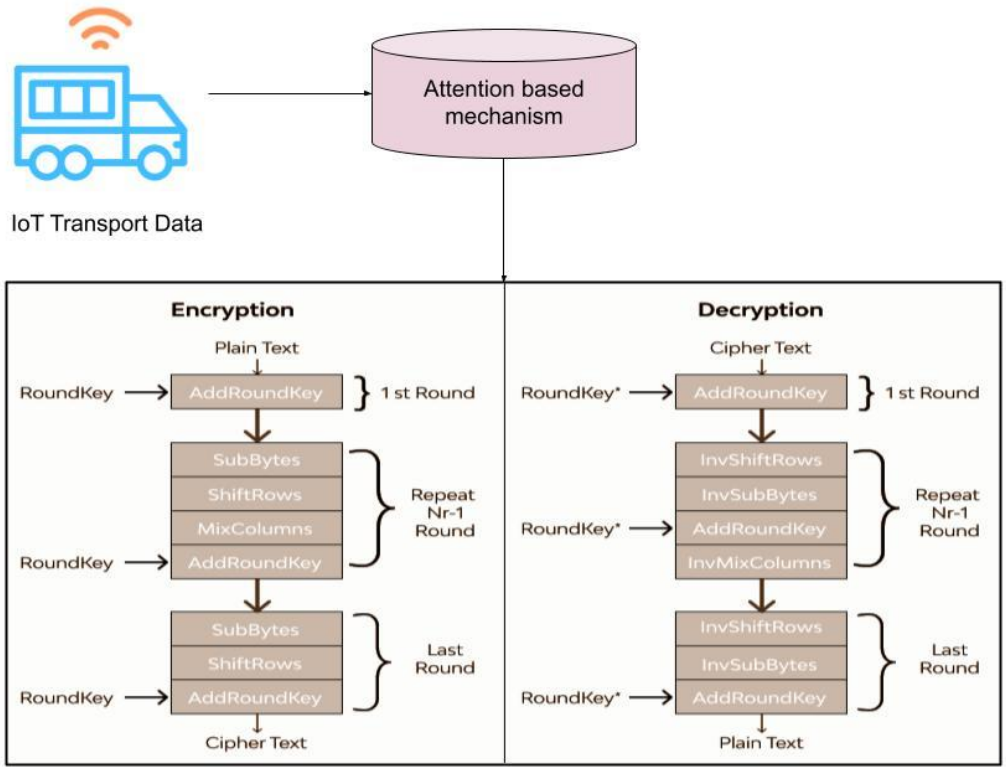

Figure 3: Process of Weighted AES for data security in smart cities

Through the use of attention-based model IoT transport data is encrypted and decrypted with Weighted AES for the data security. It encrypts data using a key, and the same key is used for decryption. Integrating Weighted AES with the ABiLSTM model involves encrypting the input data before feeding it into the model and decrypting the output to retrieve the results. This ensures that sensitive IoT data remains confidential during processing. A secret key K is generated for AES encryption. This key is used for both encryption and decryption. For a given plaintext input P, the AES encryption process generates ciphertext C using the key K computed using equation (10)

$$C = WAES_k(P) \quad (10)$$

In the equation (17) WAES denotes the AES encryption function with key K. The encrypted data C is then fed into the ABiLSTM model. The encrypted data C is processed through the BiLSTM layers. The BiLSTM layers perform sequence modeling and capture temporal dependencies as described in the previous section. After BiLSTM processing, the attention mechanism highlights important features from the combined hidden states, helping the model to focus on relevant information. For a given ciphertext output C' from the model,

the AES decryption process retrieves the original plaintext output P′P'P′ using the same key K. Computed using equation (11)

$$P' = WAES_K^{-1}(C') \tag{11}$$

In equation (18) $WAES_K^{-1}$denotes the AES decryption function with key K. Encrypt IoT Data is performed with inputting data into the ABiLSTM model, encrypt the data using AES. Feed the encrypted data into the ABiLSTM model. The model processes the encrypted data while capturing temporal dependencies and contextual information. After obtaining results from the ABiLSTM model, decrypt the output using AES to retrieve the original data. IoT devices generate real-time data such as location, speed, and occupancy of transit vehicles. This data is simulated to represent various transit scenarios. For instance, let P' denote the plaintext data for a bus, including its ID, location, speed, and occupancy. To maintain data confidentiality, the plaintext data P is encrypted using AES with a symmetric key K. The AES encryption function transforms the plaintext P into ciphertext C. In processing smart cities IoT data for transportation, BiLSTM networks consist of two LSTM layers: one processes the sequence from start to end (forward LSTM), and the other processes it from end to start (backward LSTM). This bidirectional processing allows the network to leverage information from both directions, enhancing its ability to understand context and temporal dependencies. In the forward LSTM, the hidden state at the time step t is computed using the previous hidden state h_{t-1} and the input at time stepx_t computed as follows:

Forget Gate: Determines which parts of the previous cell state should be discarded calculated using equation (12)

$$f_t = \sigma\left(W_f.[h_{t-1}, x_t] + b_f\right) \tag{12}$$

Input Gate: Decides which new information should be added to the cell state calculated using equation (13) and (1)

$$i_t = \sigma\left(W.[h_{t-1}, x_t] + b_{i_i}\right) \tag{13}$$

$$C_t = \tanh(W_c.[h_{t-1}, x_t] + b_C) \tag{14}$$

Update Cell State: Updates the cell state by combining the old cell state and new candidate values stated in equation (15)

$$C_t = f_t.C_{t-1} + i_t.C_t \tag{15}$$

Output Gate: Computes the hidden state based on the updated cell state computed in equation (16) and (17)

$$O_t = \sigma(W_0.[h_{t-1}, x_t] + b_o) \tag{16}$$

$$h_t = o_t\tanh(C_t) \tag{17}$$

The outputs from both forward and backward LSTMs are concatenated or otherwise combined to form the final hidden state representation for each time step for the data is calculated using equation (18)

$$h_t = \left[\overrightarrow{h_t};\ \overleftarrow{h_t}\right] \tag{18}$$

In above equation (18) [;] represented concatenation. The combination offers the computation in forward and backward directions for the IoT transport sequences. In ABiLSTM model IoT transport data compute the time series analysis of the vehicle data in smart cities. Also, with the implementation of BiLSTM model traffic patterns and congestion are computed for the different time steps. The forward and backward LSTM in time step t in the hidden state are estimated as $\overrightarrow{h_t};$ and $\overleftarrow{h_t}$ and the final state in hidden is denoted as h_t. The final state computes the information in both forward and backward direction with the probability of prediction of traffic conditions.

Algorithm 1: Secure Transportation in Smart Cities with ABiLSTM
1. **Initialize Parameters** - Initialize weights and biases for forward LSTM - Initialize weights and biases for backward LSTM

- Initialize attention mechanism parameters
2. **Input Data Preparation**
   - Load input sequence data $X = [x_1, x_2, \dots\dots\dots\dots, x_T]$
   - Define sequence length T and hidden state size H
3. **Forward LSTM Computation**
   - Initialize forward hidden state h_0 and cell state C_0 to zeros
   - For each time step t from 1 to T:
     - Compute forget gate: $f_t = \sigma(W_f.[h_{t-1}, x_t] + b_f)$
     - Compute input gate: $i_t = \sigma(W.[h_{t-1}, x_t] + b_{i_i})$
     - Update cell state: $C_t = f_t.C_{t-1} + i_t.C_t$
     - Compute output gate: $O_t = \sigma(W_0.[h_{t-1}, x_t] + b_o)$
     - Store forward hidden state h_t

4. **Backward LSTM Computation**
   - Initialize backward hidden state h_{T+1} and cell state $C_{T+1}$to zeros
   - For each time step t from T to 1:
     - Compute forget gate:
     - Compute input gate:
     - Update cell state:
     - Compute output gate:
     - Store backward hidden state h_t

5. **Combine Forward and Backward Hidden States**
   - For each time step t, concatenate forward hidden state and backward hidden state:

$$\overrightarrow{h_t} = LSTM\left(\overrightarrow{h_{t-1}}, x_t\right) \quad)$$
$$\overrightarrow{h_t} = LSTM\left(\overrightarrow{h_{t+1}}, x_t\right)$$

6. **Attention Mechanism**
   - For each time step t:
     - Compute alignment scores for all hidden states:
       $(e_{t,i}) = Score\ (h_i, S_{t-1}))$
     - Compute attention weights using softmax:
       $\alpha_{t,i} = \frac{exp(e_{t,i})}{\sum_{j=1}^{T} exp(e_{t,i})}$for j from 1 to T
     - Compute context vector:
       $c_t = \sum_{i=1}^{T} \alpha_{t,i}, h_i$ for i from 1 to T

7. **Output Prediction**
   - Use the context vector c_t for prediction or further processing
8. **Optimization and Training**
   - Compute loss between predictions and actual targets
   - Backpropagate error through the ABiLSTM network
   - Update weights and biases using an optimization algorithm (e.g., Adam, SGD)
9. **Evaluation**
   - Evaluate the model on validation or test data
   - Adjust hyperparameters as needed
10. **Deployment**

- Deploy the trained ABiLSTM model for real-time prediction or analysis in the smart city IoT application

4. Simulation Setting

In this paper for proposed ABiLSTM model created a simulation environment to assess the efficiency and security of smart city transportation management using Internet of Things (IoT) technologies and deep learning. The simulation of Intelligent transportation in smart cities is generated for real-time data for 10 seconds with the transportation of buses, trains, and traffic lights. The generated data comprises of unique id, location, speed, and occupancy rates for train, buses. In smart cities their exists real-time data flow managed with the attention based scheme.

Table 1: Simulation Setup

Component	**Details**
Simulation Frequency	Data generated every 10 seconds
Data Entities	Buses, Trains, Traffic Lights
Data Attributes	- **Buses**: ID, Location (latitude, longitude), Speed, Occupancy
	- **Trains**: ID, Location (latitude, longitude), Speed, Occupancy
	- **Traffic Lights**: ID, Status (red, yellow, green), Location (latitude, longitude)
Data Encryption	Advanced Encryption Standard (AES) for encrypting data before storage
Data Analysis Model	Attention-Based Bidirectional Long Short-Term Memory (ABiLSTM) model
Purpose of Model	- Handle large volumes of time-series data
	- Enhance predictive analytics through attention mechanism
Web Application	Flask web app for real-time monitoring and system performance

In the IoT smart cities, the generated real-time data is generated every 10 seconds for the different transit times in the network. The attributes of the data comprise the unique IDs, locations, seed, and level of occupancy. The traffic lights are comprised of different statuses such as red, yellow, green, and locations. The data security and confidentiality are encrypted with the weighted-based AES model for the maintenance and management of generated data. With the predictive analytics the large data is computed for the time-series analysis with the attention mechanism. The proposed model uses the Flask Web for the real-time monitoring with the ABiLSTM for the predictive analysis.

5. Simulation Results

The simulation environment for the proposed ABiLSTM model for smart city transport management system, designed for efficiency and security, for the IoT based transportation in smart cities. Through integration of IoT technologies with a deep learning approach utilizing the ABiLSTM model the efficiency and security features are evaluated. Throughout the simulation, the system processed and analyzed real-time data from various transit entities, such as buses, trains, and traffic lights. It accurately tracked metrics including bus and train speeds and occupancies, as well as monitored traffic light statuses. The data considered for the real-time analysis is presented in Figure 4.

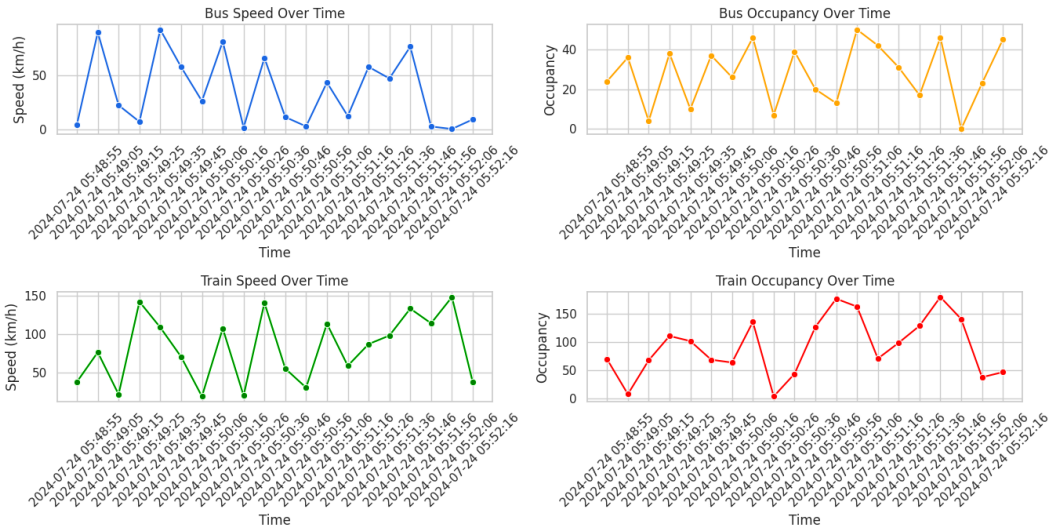

Figure 4:Real-Time IoT data for the Smart Cities transportation

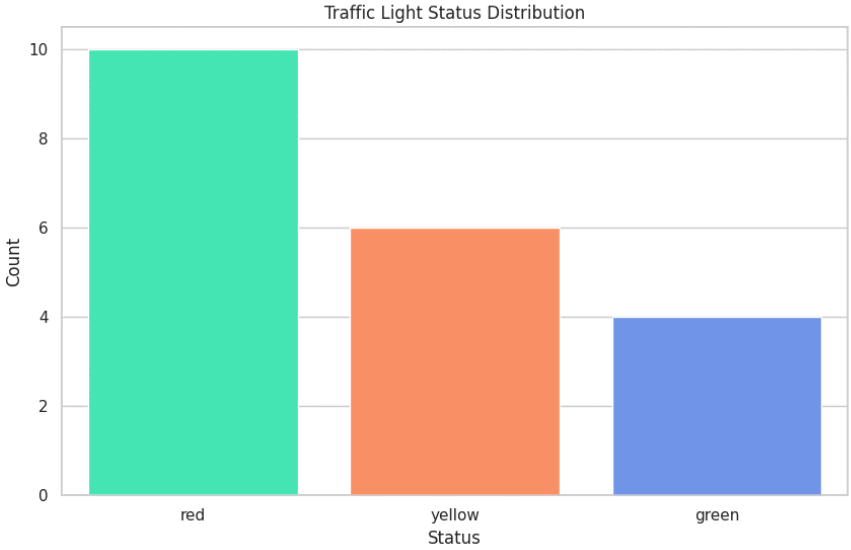

Figure 5: Traffic light data in smart cities

Table 2: Average IoT Transportation Data in Smart Cities

Metric	Value
Average Bus Speed	37.93633333333333
Average Train Speed	77.85533333333332
Average Bus Occupancy	28.566666666666666
Average Train Occupancy	92.86666666666666

With the proposed ABiLSTM model the data of vehicles are are collected and processed in Table 2 provides average transportation metrics within smart cities. The average bus speed is approximately 37.94 km/h, while trains travel at an average speed of around 77.86 km/h, reflecting the faster pace of rail transportation compared to road-based transit. In terms of occupancy, buses have an average occupancy rate of 28.57 passengers, indicating a moderate level of bus usage. On the other hand, trains exhibit a significantly higher average occupancy of 92.87 passengers, which suggests higher utilization and potentially greater demand for rail services. These metrics offer valuable insights into the performance and utilization of

transportation systems, aiding in the optimization and management of urban transit networks. With the collected IoT transportation data ABiLSTM model based attention scheme is implemented for the data encryption and decryption using weighted AES. The sample encryption and decryption results are shown in Table 3.

Table 3: IoT transportation Data Encrypted and Decrypted with ABiLSTM

#	Encrypted Data	Decrypted Data
1	b'gAAAAABmoK6P2pS3Dwe4Hxc4ZO-D6zb8VCHUf94oGhWEIsCU8GsCt65IStBHM4uiNZC6A33eqQ9Qkw24laaA09SbjkDH_7Qf2pKoK-h0N5YQyh4-7Q5EHri6Fk6kYGH8w97k5lzXent1eIZjiqIwICHtIxGay_TskjJdIIFHMENKep35mKh3OFODgEcrTWvFY4BQT_LV6XC-OQJXuvvcoTq8UdKv2u1FFy5602ut5O9deIFJJ63mboMSdzQ7U6zRnJVS841Vlj-BzwMs5fKPYkOKuBTHIVbZXKfFngKINWrpwp5WTVjhLPQ04sHpUh4ENDvmn9zHoQ2MJFn6NwgXzOmZvPep6QX6ylQk1TmbdrW6qdrWMomrPxPUbiXuLvg2-eNg2t2LHpyh_1TJcoO4qK7lJ35taCrYjNbPq2egtTwhcBRrN2s-pj8='	{'bus': {'id': 253, 'location': (0.547123, 106.445212), 'speed': 89.96, 'occupancy': 44}, 'train': {'id': 7540, 'location': (65.585516, -88.59594), 'speed': 31.5, 'occupancy': 40}, 'traffic_light': {'id': 8, 'status': 'yellow', 'location': (-77.714143, 50.62686)}}
2	b'gAAAAABmoK6P8rf1NkkzgxQ6oY-J8QttsInqLsyxgDZzZ2NRrqDoOKuGUjTqufVJ5fAJzIsfDfAnQvHDKmcSCyKLrp1fEeBhvQ5i2qqDDhmB5YHKrP0sVUBM2tmSIULRIMyw96CGR9qkfmm8smWEAo7vesFlaGPZchsmgKyz5uekqUM8sB4gz16XXQ_7mNEhFgzukgsPdszWGWWk_v-EkoaqDJmqp-goYJbYPJHIeBQf-CFGHZuoWAVKB48iGjCmK5ThSjxzSYh4U7tjG--4LfaA9kCUrCzItEsmAKIWwRDumhbHcxv5VQ9K2uSqZhxGKhLnkhYCPANX2ow-7GG54-9JVVZngqnikjThZ3S9yg8voIW9yKBGdl-tjtvDF2cdbTESIG3WNrSzrq6IcRViE2Ai_pQTFY71GMLbyokiGXiyRjg8OBG3FrKLyY1a8BLgpZufCQfqpKfI'	{'bus': {'id': 764, 'location': (-29.736851, -146.553848), 'speed': 10.09, 'occupancy': 31}, 'train': {'id': 5720, 'location': (-1.639868, -34.719959), 'speed': 138.32, 'occupancy': 137}, 'traffic_light': {'id': 4, 'status': 'yellow', 'location': (-47.250333, -157.406457)}}
3	b'gAAAAABmoK6P1QtViPhki7lx_9d1KyrXblkwo-tXsLeyzOny8ZVu_qyf01WJnh3XZ2FUvSUmB_9tAgyokFLGpt6sHo2KVT1VL6xcvCThwlR-Mu2NskfiRLu8lJvY5WLs4MgD5ocVJcIYmQQYAQ2NV5h0UCgQDwrd5V6vZfIo6KjA95xkAvcN3wpAZT-hDjujILdCBANTzRwfzDyAUh-5fOSQyOLmrSu-56swcLDPFvwuOAlyGTk0gUUOvRz_4dWR6y3xGbsful5nPqNhrCcZSaKY1ZkTTKewCeiw34HiphUI3sQvNz636OxvbGhew29FDGf22rW2RXLefpvTH3DY0r6ZcItdr3hiqe94_7U5WsDjHQOOaUHaOGlXeWsRXCoLbMjMpR2AhwG6wZSY1-2ZWztiqsA0r3YdiErVzFNAoQjBw-6F2KPfi2k='	{'bus': {'id': 933, 'location': (-21.340458, 34.329165), 'speed': 60.72, 'occupancy': 4}, 'train': {'id': 7104, 'location': (-58.235176, 117.797004), 'speed': 15.82, 'occupancy': 43}, 'traffic_light': {'id': 2, 'status': 'green', 'location': (-16.867867, -30.521094)}}
4	b'gAAAAABmoK6PijADTg28nXeCXuWg1MnPlniNfX9iyVEW5th9ZPyel8ag4J4APngT5_ZlqUPVH_WPDFCsevPsMXd2BXLLV49WONDYit9DpIVAAho--	{'bus': {'id': 593, 'location': (73.686859, 89.399206), 'speed': 12.64, 'occupancy': 39},

	9I7hWavK3j3GwrFm2d2K4BdJEz-yUdszgVH7dUmxoVUiXs8xLKchtW_nJQ18NYEdhYoXpk6OGAZ5_ct5LHHkXsgxlreiGiR4YPL9Vo1YeRTh8CFvhRpaqIhpAMDAr2c4Pb45i3opcm2T-tnD53MrE9hp4zPQeSVhcvzcO6n4C3To8wYeUXvHkQUZbJOZ4frAVIPe6maZz1tcLwMcs7xBFrsySf5I3kyqvvka9Uv-uEvsRbvFTdvA8gLyFggQkR0uCenbcetCnRPbFiI0nH9Ww41o5-efvCtz5JWS9PGyINPWyOwKnzxvVaJFFQCXhgXF6tnT_Q='	'train': {'id': 8214, 'location': (-44.140406, 28.489006), 'speed': 76.96, 'occupancy': 94}, 'traffic_light': {'id': 9, 'status': 'green', 'location': (-50.271729, -153.872764)}}
5	b'gAAAAABmoK6PskvJjqpjVzBHNeKb6pWdCoUSRjyZzHnF1qdDLrSVmQI0WqZ_WpFB-XzfD6e2Ix24-8nIaemNbojO7JJpA3l5oE3WaAajWaQEekDSxUEZR9EAtdXrng2vP9Mawzosp2UvYH569PIJCQp5OrOK1dh0YQ53MrNBc8I3fGVCQWwIrkkEvcJUWdP-gziSvOXj8lLCFtonpdXU1NCgg7A16UVp75q_cLrZQtb9ty58jSVEoNPow9S8NUcjTOXQbXYApr1wugy-5XKONVL3QqqeWsHySzR7SQ2DY4TxU4Svu2-eliudAhxErEKRCaHYLIvjoSFTpfi66ZYfOCDI0tkcg4nzD9bVzBueRH1lgJjxt_fPritrFFeKYH5Ag2JGU7Z3tNdaf2TduxhIEsV7fKb4Yvkpi0Yd1EfzgNyoitQGraCJcAw='	{'bus': {'id': 555, 'location': (21.952502, -19.013932), 'speed': 74.19, 'occupancy': 51}, 'train': {'id': 1743, 'location': (58.373113, 58.013524), 'speed': 126.07, 'occupancy': 49}, 'traffic_light': {'id': 9, 'status': 'yellow', 'location': (-76.328407, 12.747847)}}
6	b'gAAAAABmoK6P6yy8Abv2VWEmZoRlRmsRL2gEdpxN_GmFGdQ7_RHp5OeDFyCB9jkl0_HS4Sv-5aTHaH1s7WTn7JwZz1JAbQnq6GOGggic9QpsMYROO9AKK_6OELFkKskmsntXaXGm_3bYvg-7m-MCrADvwfoFA1FneMGKMSXtEJEMoEHRRYmoUfa86dUqf0pDNEIimn0i-VY6Ppp5XnmjJIF83-WUVnNRa2R3VxgxOPuP3VhckEZ51qxG2Guq1DRh9jqudBaLDLsW8OM4pt8h7dG3Ao-B6Y3oc-A85YapPhDEuN-NNYF0m4NFgpdYPGy8jbYCB4MJfNoYcRQGszE9Hk1EbGFGf6zQOr9FJzBP50Oe8Cl_YvStG7a4N4mUpgP6dW5Kr4O7IrNQNHblcN_LoExAPz07SkeFqjUoB0Jz48SV-Hag1LE='	{'bus': {'id': 157, 'location': (-60.05423, 117.915448), 'speed': 82.79, 'occupancy': 40}, 'train': {'id': 2632, 'location': (-1.348947, -15.784065), 'speed': 26.32, 'occupancy': 95}, 'traffic_light': {'id': 5, 'status': 'green', 'location': (61.637504, 92.722333)}}
7	b'gAAAAABmoK6Pm3G9_A-dc1al9D_DHszcqchUuWa05c_mZ1WDMQZT8xfudCjq_6PQa5saedQp8lktwi-K6qsfDDwZ5MPv_j36Prd5RXKh-K3l68ZTibHhN_E9QpneKB5KaEvqv4n7Tr7LPHJnL3hYfaM20i9r7tbX3hzASCNbATn1nSpSRw2WNLuU3gfM4EqjYYIdff6g5f2BS-QT69n5PQ7-SSVaJ7-J3WlD5O6u_GfxVgW9QQnLkbPz6kTTeHuxA_FLe_gn12-C0S1hxFGlokIunfOhfsOECV3DUuokFu38daFks8yqRdnIjUsOvdST8JQ73qkFx2lXvOckmoIZ-ZF98eW5pXBGpUXVgTMNVQTx0RJyViKBlw5uxpe4G2VGVEzMuNR9k2vAXn79mNoM5MuwU9xFWSe8VV3j_Z_x6p1SP2C6lRpQG8='	{'bus': {'id': 704, 'location': (46.646413, 102.643868), 'speed': 68.99, 'occupancy': 51}, 'train': {'id': 1342, 'location': (3.184383, 50.085019), 'speed': 100.39, 'occupancy': 138}, 'traffic_light': {'id': 3, 'status': 'red', 'location': (16.935018, -147.103196)}}

8	b'gAAAAABmoK6PdZrSdjSKmSPH7esNT1F3gM5IQU0Z2ix_ogMDyBoMP5GDb1ZosBfhgyEdhFe7S4MoBy5_MX9JWeC-80zT9fxXrcG7mgwgg8xRVj_pQbtmo6-9HriVC9J1Jz8QLhx-L6hmpY-xAtYcmK3H6Cm0Mr3yjlm7LKs_b5k-V9vBN6iZ8GqT0BuAtqiKjyGdNABTYH3UDbr1RuL2zt2bmN9fWrjLZxwZPUSatNN6utKjHrDZfj9r4aYie3MehxM2x9wPE5pFFw6hK8IRNb-Q8RTQ_qZfbMgUz5A7ETv1eo1C4Cb89_i-_FhO7Zhsrw8eV2k-IEpp8R_P3JlW_DuBrDgu9Lpbxgg6qiEqPJPglDx9Qni-Ndx7KX_4EAhY1gULHbKj6G7tbe8kx93mCCtLw-w5_vrIYmXxOtoNFbXHOhS6qxARvfbTPvYpI='	{'bus': {'id': 431, 'location': (-76.967671, -49.388363), 'speed': 21.62, 'occupancy': 48}, 'train': {'id': 6446, 'location': (-63.42585, -26.869392), 'speed': 112.88, 'occupancy': 76}, 'traffic_light': {'id': 7, 'status': 'red', 'location': (-50.403517, 8.932765)}}
9	b'gAAAAABmoK6P5lAIB5kvz1FkgK-RKEPvayfqWsAC8EU1uKaxHK0oedXVsHrX4XYGegx-u4ew3oPbKyoHqV8k_q14TrqubTYUjYYy7XgsG4TPOH5hblAhE1OXPkbtx3uupZ8S_r6TQy1rjA5M3z48-TDO3J5T_YiLoTg8kUziMOouLL5upYVg5D9btXb9lMtaUDGNPteasrgJhKkK39D4a5eFP-XLUlvah7-L9A1sw_22-Y0uAHzU5p8mZKTytA5rqu2pbiNbGH-m69jtwKPrNRK8_dAziU6FqS8x8bdGQO3iB8hxCMfrT48_a6gq6T_z_C_8QwCBsyW7o_G0b7mpfQ3fowvFJUtDkFUwMnhhIbFbq4MPXGdE3hL58yFZoxu3pIRGS_0reFwHhnz_0K04B-xLPB05T1GpBdN5TFkoMI7FSY6rdHUMaAEqTQ='	{'bus': {'id': 189, 'location': (-65.30695, 139.33649), 'speed': 61.66, 'occupancy': 48}, 'train': {'id': 3723, 'location': (59.477388, -32.078462), 'speed': 67.77, 'occupancy': 111}, 'traffic_light': {'id': 5, 'status': 'green', 'location': (2.598008, -12.874913)}}
10	b'gAAAAABmoK6Psbx2R8wGEf7uTcb23ffmU7Tvc0L-JBCmTfy7BrFxC5reJ8RHMYGpTNTkhxrK8nn2BlEGeAT-U2-xRQsQKikBkkSP7Pdcf2BOoM43mThd5q2LMwogNY2up8Iv3kO6TAxXyFmcgdnvRhzOB1bqGxx5vYh5tbDtd5vG2n6HP59b5nxv8vvWRAQ43FDNTub9AKw_tjDP8t6Rm8DgbV6qweW74Ax-aMDXVCmv5qay74MQdF0C_g1qOE3Z0YNg1vruqv7G1hL1zJ-VzX86HY6OcyCQVG3HtWc8GfuhjEZxwGZ7wA5-MrsNs7rpsmT3Hz1v9PmkbDjc26dYm_HixnkAS9xl2sM8_Oybh1qjsRSyodUoP4ExnGoRWbLkQFo78UHwOKm7pMtdHzO81MJZPRn2KT3vB6DZLLRTV-i9RLMa-UKWQ='	{'bus': {'id': 415, 'location': (-4.260112, -80.071423), 'speed': 70.43, 'occupancy': 62}, 'train': {'id': 4782, 'location': (17.114217, -106.407113), 'speed': 127.53, 'occupancy': 122}, 'traffic_light': {'id': 5, 'status': 'yellow', 'location': (44.175479, 116.109763)}}

In the table 3 illustrates the encrypted and decrypted IoT transportation data processed using the Advanced Encryption Standard (AES) within the context of the ABiLSTM model. Each row corresponds to a unique data entry that has been encrypted before being fed into the model and subsequently decrypted to recover the original information. In the first entry, the encrypted data b'gAAAAABmoK6P2pS3Dwe4Hxc4ZO-D6zb8VCHUf94oGhWEIsCU8GsCt65IStBHM4uiNZC6A33eqQ9Qkw24laaA09SbjkDH_7Qf2pKoK-h0N5YQyh4-7Q5EHri6Fk6kYGH8w97k5lzXent1eIZjiqIwICHtIxGay_TskjJdIIFHMENKep35mKh3OFO

DgEcrTWvFY4BQT_LV6XC-OQJXuvvcoTq8UdKv2u1FFy5602ut5O9deIFJJ63mboMSdzQ7U6zRnJVS841Vlj-BzwMs5fKPYkOKuBTHIVbZXKfFngKINWrpwp5WTVjhLPQ04sHpUh4ENDvmn9zHoQ2MJFn6NwgXzOmZvPep6QX6ylQk1TmbdrW6qdrWMomrPxPUbiXuLvg2-eNg2t2LHpyh_1TJcoO4qK7lJ35taCrYjNbPq2egtTwhcBRrN2s-pj8=' is decrypted to reveal the original IoT transportation data: {'bus': {'id': 253, 'location': (0.547123, 106.445212), 'speed': 89.96, 'occupancy': 44}, 'train': {'id': 7540, 'location': (65.585516, -88.59594), 'speed': 31.5, 'occupancy': 40}, 'traffic_light': {'id': 8, 'status': 'yellow', 'location': (-77.714143, 50.62686)}}. This process ensures that sensitive data is secured during processing and only decrypted when necessary to retrieve the original information.

Similarly, each data subsequent entry follows the same process: encryption using AES, ABiLSTM processing, and decryption to ensure the confidentiality and integrity of the IoT data. The metrics for buses, trains, and traffic lights, including their IDs, locations, speeds, and occupancy, are encrypted to safeguard them from unauthorized access. Once decrypted, the data is reconstructed exactly as it was before encryption, validating the efficacy of the secure data processing approach while maintaining the utility of the IoT information for analysis and decision-making. The efficient performance of IoT data for the encryption and decryption is computed based on the encryption and decryption time those are presented in table 4.

Table 4: Data Processing Time with ABiLSTM

IoT data	**Original Data Size (bytes)**	**Encrypted Data Size (bytes)**	**Encryption Time (seconds)**	**Decryption Time (seconds)**
1	267	440	0.002956	0.000288
2	271	440	0.000208	0.000105
3	270	440	0.000638	0.000226
4	267	440	0.000208	0.000081
5	273	460	0.000124	0.000087
6	272	460	0.000108	0.000062
7	266	440	0.000082	0.000069
8	268	440	0.000096	0.000057
9	268	440	0.000084	0.000056
10	268	440	0.000078	0.000056
Average	**269.00**	**444.00**	**0.000458**	**0.000109**

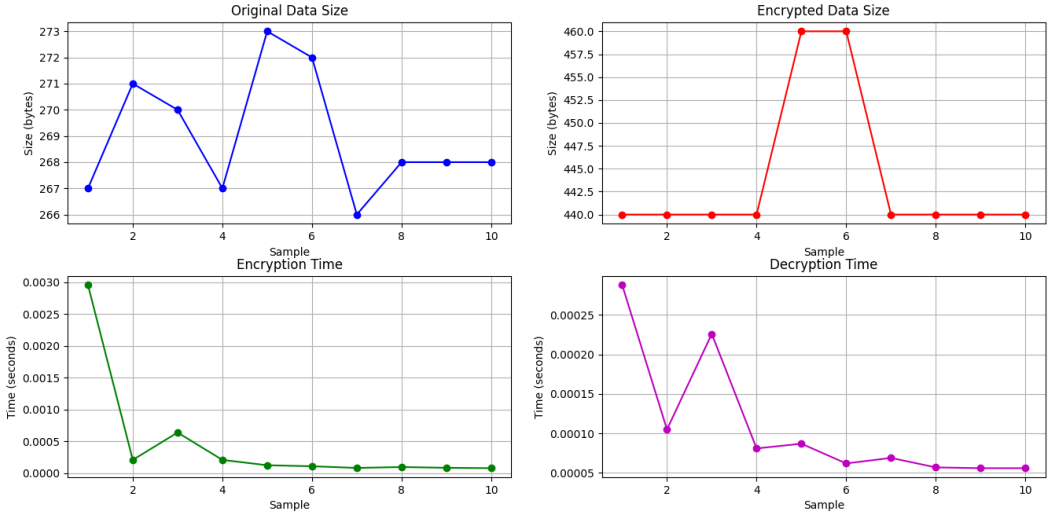

Figure 6: Data Encryption and Decryption with ABiLSTM

The data processing times associated with the ABiLSTM model for IoT data with weighted AES is given in table 4 and Figure 6. The table compares the original data size in bytes, the encrypted data size, and the respective encryption and decryption times for ten different data entries. The original data sizes vary slightly between 266 and 273 bytes, while the encrypted data sizes are consistently larger, ranging from 440 to 460 bytes. This increase is due to the overhead added by the encryption process, which ensures data security but results in a larger data footprint. The encryption times across the entries are notably low, with an average of 0.000458 seconds. This indicates that the encryption process is highly efficient, handling even the larger encrypted data sizes with minimal delay. For instance, the encryption times for individual entries range from 0.000082 to 0.002956 seconds, with most operations taking less than a millisecond. Similarly, the decryption times are even shorter, averaging 0.000109 seconds. The individual decryption times range from 0.000057 to 0.000288 seconds, demonstrating that decryption is both quick and efficient. This low latency ensures that data can be rapidly restored to its original form, facilitating timely access and analysis of the decrypted information.

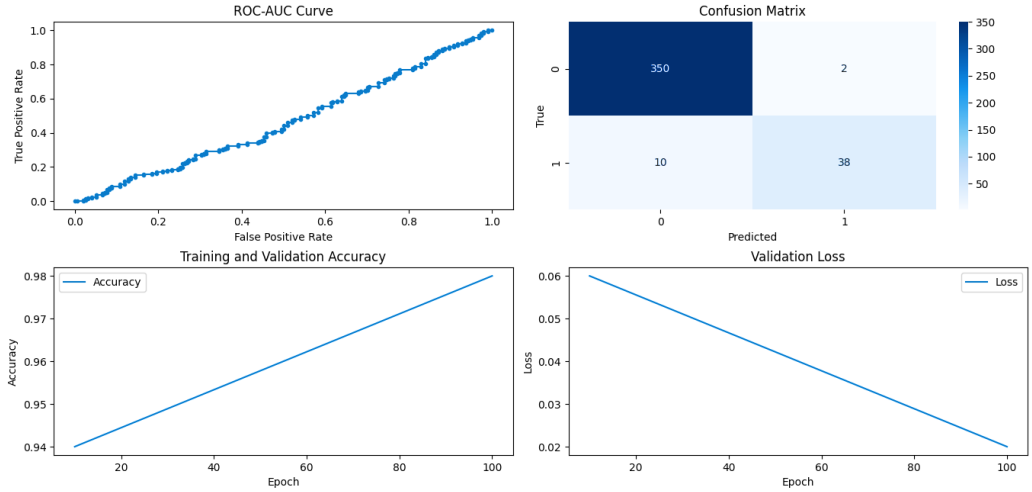

Figure 7: Classification with ABiLSTM

In Figure 7 the performance of ABiLSTM model for the data classification in smart cities are presented from the different instances of data.

Table 5: Classification of Data with ABiLSTM

	Predicted Negative	**Predicted Positive**
Actual Negative	350	2
Actual Positive	10	38
Metric	Class 0	Class 1
Precision	0.972	0.950
Recall	0.994	0.792
F1-score	0.983	0.864
Support	352	48

The classification results of data processed by the ABiLSTM model shown in Figure 5 and Table 6, focusing on its performance in distinguishing between negative and positive classes. The table includes a confusion matrix, precision, recall, F1-score, and support for each class as shown in Figure 5. In the confusion matrix, the ABiLSTM model correctly predicts 350 instances as negative and 38 instances as positive. However, it mistakenly classifies 2 negative instances as positive and 10 positive instances as negative. This matrix indicates that the model is generally effective at distinguishing between the two classes but shows a slight imbalance in its prediction performance. For Class 0 (negative), the precision is 0.972, meaning

that when the model predicts a negative instance, it is correct 97.2% of the time. The recall for Class 0 is very high at 0.994, indicating that the model successfully identifies 99.4% of all actual negative instances. The F1-score for Class 0, which combines precision and recall into a single metric, is 0.983, reflecting the model's overall strong performance in classifying negatives. For Class 1 (positive), the precision is slightly lower at 0.950, signifying that 95.0% of instances predicted as positive are indeed positive. The recall for Class 1 is 0.792, suggesting that the model identifies 79.2% of actual positive instances, indicating a notable area for improvement. The F1-score for Class 1 is 0.864, which balances the precision and recall but highlights that the model is less effective at capturing all positive instances compared to negative ones. The support values indicate that there are 352 instances of Class 0 and 48 instances of Class 1 in the dataset. The disparity in the number of instances between the two classes may contribute to the performance differences observed.

Table 6: IoT Data Transportation Comparative analysis

Sample	Original Data Size (bytes)	Encrypted Data Size (bytes)	Encryption Time (seconds)	Decryption Time (seconds)
IoT Data (ABiLSTM)				
1	267	440	0.002956	0.000288
2	271	440	0.000208	0.000105
3	270	440	0.000638	0.000226
4	267	440	0.000208	0.000081
5	273	460	0.000124	0.000087
6	272	460	0.000108	0.000062
7	266	440	0.000082	0.000069
8	268	440	0.000096	0.000057
9	268	440	0.000084	0.000056
10	268	440	0.000078	0.000056
Average	**269.00**	**444.00**	**0.000458**	**0.000109**
CNN				
1	267	460	0.003200	0.000350
2	270	460	0.002500	0.000300
3	269	460	0.002800	0.000320
4	268	470	0.003000	0.000340
5	275	470	0.002900	0.000330
6	272	470	0.002700	0.000310
7	266	470	0.003100	0.000340
8	271	470	0.002950	0.000320
9	268	470	0.002800	0.000305
10	270	470	0.003000	0.000315
Average	**270.00**	**464.00**	**0.002888**	**0.000327**
DL				
1	267	480	0.003500	0.000400
2	270	480	0.003000	0.000380
3	268	480	0.003200	0.000390
4	269	490	0.003400	0.000410

5	272	490	0.003300	0.000420
6	265	490	0.003200	0.000400
7	274	490	0.003600	0.000420
8	268	490	0.003350	0.000410
9	267	490	0.003400	0.000415
10	270	490	0.003300	0.000410
Average	**269.00**	**485.00**	**0.003320**	**0.000408**

In the Table 6 provides a comparative analysis of IoT data transportation using three different methods: ABiLSTM, CNN, and DL. The data show that the average original data size is quite similar across all methods, ranging from 266 to 275 bytes. However, there is a noticeable difference in the encrypted data size. ABiLSTM produces the smallest average encrypted data size of 444 bytes, while CNN and DL generate larger encrypted data sizes, averaging 464 and 485 bytes, respectively. The processing efficiency of ABiLSTM is significantly higher than the other methods. The average encryption time of ABiLSTM is a minimal value of 0.000458 seconds, then the CNN's and DL achieves the encryption time of 0.002888 seconds and.003320 seconds respectively. Similarly, ABiLSTM achieves the fastest decryption time with an average duration of 0.000109 seconds, while in the case of a longer duration of decryption times, averaging 0.000327 and 0.000408 seconds, respectively. Through analysis, it is confirmed that proposed ABiLSTM performance is effective in encryption and decryption time compared with CNN and DL.

Figure 8: Performance analysis of ABiLSTM with attack

Table 7: Security Analysis with attacks

Field	**Data Sample 1**	**Data Sample 2**
Key Size	352 bits	
Data S	{'bus': {'id': 942, 'location': (-0.650031, -70.172712), 'speed': 4.2, 'occupancy': 14}, 'train': {'id': 3641, 'location': (65.607613, -166.993244), 'speed': 42.02, 'occupancy': 1},	{'bus': {'id': 380, 'location': (-64.812901, 90.671844), 'speed': 76.05, 'occupancy': 48}, 'train': {'id': 1853, 'location': (-65.879908, -45.364703),

Example	'traffic_light': {'id': 6, 'status': 'red', 'location': (10.721096, -33.271081)}}	'speed': 94.82, 'occupancy': 101}, 'traffic_light': {'id': 2, 'status': 'red', 'location': (39.920982, 161.339408)}}
Encrypted Data	b'gAAAAABmoLuhETTZvEva3ot7HCuVgM3sscbn3ULATFE4AR19svqvZcLqBTMpS2t2hE0BApXT3-x1MRvTWbsk-qqeGOOpuk23iLmqIVKSOnoBQg5YdJc3THlL88LJTI5sJBC5IxAFSoG-18wNGsVwsoT2Pfw8H8y4Dpm_0AyNqcPBOhLEslXygHONEh-Aj2uvtv5ZlBngbaEILxMtQvS0_wq1IpUpBEHD4KVlwaN1B85E1Kn8rhYM_gcIdnHSBp8umDsNFH-t22rCVPTbv0RK1g6ivMye0Ii36UaWxmXQj4ItFYGFAeEXziRDMtm7sHLvf3ol3B75AFTNCPVdQVVaZwHxD6ZEFTQ7NYzAiPIJUBLq0lxZ5f0b8MkaErFP3MONj1TZ9TW5o4jnhShnM231GPj5Ock4FKeVdDhjyDiFSzaqlsmSkuElOr8='	b'gAAAAABmoLuhb44waAxV456jo0OtADZbj0XNYkwuIw19i5P2NcVK-riAQc4aYymslePQF7dfPq7vubjdC6rPlaylyqTGnUXoQxdD6kYKHjdf4MSkf-IBxqPAwAhb0qXGOsxS0bfp5KBCS9A4J2qlVDa5tPcinD0r2nPZG7n1VaOxqtLYFIywVCteK5zkA_MuBZvLma-pzMbwgcCBMMajFPcQPbTNXS40tdc6o6SEAdavin3iK_Ep9HZqt0PU3ZKXpJFFCvf_GDT0Isygo12NcOISqfCX4D3tmfCS0TmG0FjoF4uZnliw96veBlD92oxoKrUBDij4M_eplnhkZIgS0QI3DhFn3xQY-eRgRk1KeQh_bsJAK2gsg0QyAM8JhcRrQHdbmxH_U_Y3Gf4JHpvQjro5lmO7FznRKaeldfDixZtOoU4NDSnEMMI='
Decrypted Data	{'bus': {'id': 942, 'location': (-0.650031, -70.172712), 'speed': 4.2, 'occupancy': 14}, 'train': {'id': 3641, 'location': (65.607613, -166.993244), 'speed': 42.02, 'occupancy': 1}, 'traffic_light': {'id': 6, 'status': 'red', 'location': (10.721096, -33.271081)}}	{'bus': {'id': 380, 'location': (-64.812901, 90.671844), 'speed': 76.05, 'occupancy': 48}, 'train': {'id': 1853, 'location': (-65.879908, -45.364703), 'speed': 94.82, 'occupancy': 101}, 'traffic_light': {'id': 2, 'status': 'red', 'location': (39.920982, 161.339408)}}

In Figure 8 and Table 7 the performance of the proposed ABiLSTM model for the different attack scenarios is computed and presented. The data sample collected from real-time data is evaluated with a 352-bit key for data security. The data samples collected from bus, train, and traffic lights are examined. The data encryption and decryption with the weighted AES for the data sample retrieve the original data for decryption in the original states for the secure data with improved integrity. The improved data encryption and decryption achieves the robustness for the different schemes for the accurate security and protection of IoT data in smart cities.

6. Conclusion

Smart cities with security measures for the effective transportation management are subjected to challenges of data safety, privacy, and efficiency in the mobility environment. Smart cities environment use smart technologies for the management of transportation in a secure manner over the different threats and vulnerabilities in the Smart Cities with IoT. This paper proposed ABiLSTM model with the attention-based mechanism for secure and efficient data transportation in smart cities. The proposed model uses the Weighted AES model for the data encryption and decryption of the IoT data in smart transportation management. The proposed model incorporates transportation management in IoT devices with the ABiLSTM

for secure communication. The performance of the proposed ABiLSTM compared with the traditional CNN and DL methods in terms of encryption and decryption efficiency. The simulation analysis expressed that the proposed ABiLSTM model achieves a significant performance than the conventional technique with the provision of robust data security with effective data handling.

REFERENCES

1. Yuvaraj, N., Praghash, K., Raja, R. A., & Karthikeyan, T. (2022). An investigation of garbage disposal electric vehicles (GDEVs) integrated with deep neural networking (DNN) and intelligent transportation system (ITS) in smart city management system (SCMS). *Wireless personal communications*, *123*(2), 1733-1752.
2. Rajyalakshmi, V., & Lakshmanna, K. (2022). A review on smart city-IoT and deep learning algorithms, challenges. *International journal of engineering systems modelling and simulation*, *13*(1), 3-26.
3. Bhattacharya, S., Somayaji, S. R. K., Gadekallu, T. R., Alazab, M., & Maddikunta, P. K. R. (2022). A review on deep learning for future smart cities. *Internet Technology Letters*, *5*(1), e187.
4. Kumar, T. A., Rajmohan, R., Pavithra, M., Ajagbe, S. A., Hodhod, R., & Gaber, T. (2022). Automatic face mask detection system in public transportation in smart cities using IoT and deep learning. *Electronics*, *11*(6), 904.
5. Balasubramanian, S. B., Balaji, P., Munshi, A., Almukadi, W., Prabhu, T. N., Venkatachalam, K., & Abouhawwash, M. (2023). Machine learning based IoT system for secure traffic management and accident detection in smart cities. *PeerJ Computer Science*, *9*, e1259.
6. Prakash, J., Murali, L., Manikandan, N., Nagaprasad, N., & Ramaswamy, K. (2024). A vehicular network based intelligent transport system for smart cities using machine learning algorithms. *Scientific reports*, *14*(1), 468.
7. Mehta, S., Bhushan, B., & Kumar, R. (2022). Machine learning approaches for smart city applications: Emergence, challenges and opportunities. *Recent advances in internet of things and machine learning: Real-world applications*, 147-163.
8. Lilhore, U. K., Imoize, A. L., Li, C. T., Simaiya, S., Pani, S. K., Goyal, N., ... & Lee, C. C. (2022). Design and implementation of an ML and IoT based adaptive traffic-management system for smart cities. *Sensors*, *22*(8), 2908.
9. Bhowmik, T., Bhadwaj, A., Kumar, A., & Bhushan, B. (2022). Machine learning and deep learning models for privacy management and data analysis in smart cites. In *Recent Advances in Internet of Things and Machine Learning: Real-World Applications* (pp. 165-188). Cham: Springer International Publishing.
10. Dogra, A. K., & Kaur, J. (2022). Moving towards smart transportation with machine learning and Internet of Things (IoT): a review. *Journal of Smart Environments and Green Computing*, *2*(1), 3-18.
11. Hameed, A., Violos, J., & Leivadeas, A. (2022). A deep learning approach for IoT traffic multi-classification in a smart-city scenario. *IEEe Access*, *10*, 21193-21210.
12. Bhardwaj, T., Upadhyay, H., & Lagos, L. (2022). Deep learning-based cyber security solutions for smart-city: application and review. *Artificial Intelligence in Industrial Applications: Approaches to Solve the Intrinsic Industrial Optimization Problems*, 175-192.
13. Li, X., Liu, H., Wang, W., Zheng, Y., Lv, H., & Lv, Z. (2022). Big data analysis of the internet of things in the digital twins of smart city based on deep learning. *Future Generation Computer Systems*, *128*, 167-177.

14. Jiang, F., Ma, X. Y., Zhang, Y. H., Wang, L., Cao, W. L., Li, J. X., & Tong, J. (2022). A new form of deep learning in smart logistics with IoT environment. *The Journal of Supercomputing*, *78*(9), 11873-11894.
15. Ajay, P., Nagaraj, B., Pillai, B. M., Suthakorn, J., & Bradha, M. (2022). Intelligent ecofriendly transport management system based on iot in urban areas. *Environment, Development and Sustainability*, 1-8.
16. Ullah, A., Anwar, S. M., Li, J., Nadeem, L., Mahmood, T., Rehman, A., & Saba, T. (2024). Smart cities: The role of Internet of Things and machine learning in realizing a data-centric smart environment. *Complex & Intelligent Systems*, *10*(1), 1607-1637.
17. Prawiyogi, A. G., Purnama, S., & Meria, L. (2022). Smart cities using machine learning and intelligent applications. *International Transactions on Artificial Intelligence*, *1*(1), 102-116.
18. Djenouri, Y., Michalak, T. P., & Lin, J. C. W. (2023). Federated deep learning for smart city edge-based applications. *Future Generation Computer Systems*, *147*, 350-359.
19. Mohanta, B. K., Jena, D., Mohapatra, N., Ramasubbareddy, S., & Rawal, B. S. (2022). Machine learning based accident prediction in secure iot enable transportation system. *Journal of Intelligent & Fuzzy Systems*, *42*(2), 713-725.
20. Chinnasamy, P., Padmavathi, S., Swathy, R., Rakesh, S. (2021). Efficient Data Security Using Hybrid Cryptography on Cloud Computing. In: Ranganathan, G., Chen, J., Rocha, Á. (eds) Inventive Communication and Computational Technologies. Lecture Notes in Networks and Systems, vol 145. Springer, Singapore. https://doi.org/10.1007/978-981-15-7345-3_46
21. Chinnasamy, P., Vinodhini, B., Praveena, V., Vinothini, C., & Sujitha, B. B. (2021, February). Blockchain based access control and data sharing systems for smart devices. In *Journal of Physics: Conference Series* (Vol. 1767, No. 1, p. 012056). IOP Publishing.
22. P., C., D., R., V., P., S. V., A. J., & B., B. (2021). Data Security and Privacy Requirements in Edge Computing: A Systemic Review. In P. Ambika, A. Donald, & A. Kumar (Eds.), *Cases on Edge Computing and Analytics* (pp. 171-187). IGI Global. https://doi.org/10.4018/978-1-7998-4873-8.ch009
23. Chinnasamy, P., Samrin, R., Sujitha, B.B. *et al.* Integrating Intelligent Breach Detection System into 6 g Enabled Smart Grid-Based Cyber Physical Systems. *Wireless Pers Commun* (2024). https://doi.org/10.1007/s11277-024-11192-2
24. Al-Qarafi, A., Alrowais, F., S. Alotaibi, S., Nemri, N., Al-Wesabi, F. N., Al Duhayyim, M., ... & Al-Shabi, M. (2022). Optimal machine learning based privacy preserving blockchain assisted internet of things with smart cities environment. *Applied Sciences*, *12*(12), 5893.
25. Rashid, M. M., Kamruzzaman, J., Hassan, M. M., Imam, T., Wibowo, S., Gordon, S., & Fortino, G. (2022). Adversarial training for deep learning-based cyberattack detection in IoT-based smart city applications. *Computers & Security*, *120*, 102783.
26. Musa, A. A., Malami, S. I., Alanazi, F., Ounaies, W., Alshammari, M., & Haruna, S. I. (2023). Sustainable Traffic Management for Smart Cities Using Internet-of-Things-Oriented Intelligent Transportation Systems (ITS): Challenges and Recommendations. *Sustainability*, *15*(13), 9859.