

A Trust-Aware Modeling Framework for Jakarta Smart Transportation Open Data

Setyawan Widyarto¹, Riki², Sulaiman Said Omar Al-Hinai³, Dur Soomro⁴

¹Computer Science, Postgraduate Program, Budi Luhur University, Jakarta, Indonesia

^{2,3}Information System, Faculty of Sains and Technology, Buddhi Dharma University, Tangerang, Indonesia

³Ministry of Transport, Communications and Information Technology (MTCIT), Sultanate of Oman

⁴Department of Electrical Engineering, DHA Suffa University, Karachi, Pakistan

Received:

June 26, 2026

Revised:

July 20, 2026

Accepted:

September 2, 2026

Published:

October 24, 2026

Corresponding Author:

Author Name*:

Setyawan Widyarto

Email*:

setyawan.widyarto@budiluhur.ac.id

DOI:

10.63158/journalisi.v8i5.1785

© 2026 Journal of Information Systems and Informatics. This open access article is distributed under a (CC-BY License)



Abstract. Smart transportation open data can support urban data-quality assessment and operational-risk screening, but it does not contain verified cybersecurity labels. This study develops a preliminary trust-aware modeling dataset for Jakarta Smart Transportation Open Data using nine Satu Data Jakarta sources covering TransJakarta operations and stops, road-speed observations, ATCS and CCTV locations, busway ITS corridors, traffic violations, congestion-risk points, and modal share. The sources are harmonized into a record-level schema comprising node_id, data_type, period, location, value, trust, output, source_dataset, and raw_label. Researcher-defined, source-specific rules assign trust scores from recency, completeness, active status, speed, violation intensity, and congestion-risk status. The resulting dataset contains 2,790 records: 2,508 trusted/non-malicious and 282 anomalous/untrusted proxy records. A separate baseline-repository ANN replication is reported only as a trust-threshold pipeline-consistency check, not as Jakarta model performance. The heuristic labels require expert review, sensor and incident logs, and controlled attack simulation before cybersecurity use. The contribution is therefore dataset construction and an exploratory trust-risk modeling framework rather than validated attack detection.

Keywords: Jakarta Smart Transportation Open Data, Satu Data Jakarta, trust-aware modeling, trust scoring, anomaly detection, dataset construction

1. INTRODUCTION

Smart city development increasingly depends on integrated digital infrastructure, data interoperability, and intelligent public services. In transportation, this integration includes public transport operations, road speed monitoring, traffic control systems, CCTV, intelligent transportation systems, and citizen-facing platforms. Prior studies show that IoT-enabled smart city services improve monitoring and decision making, but they also raise new concerns around privacy, data integrity, cyber security, and trust [2], [3], [4]. Transportation is especially sensitive because incorrect or malicious data can affect routing, congestion management, public transport reliability, emergency response, and urban safety.

Smart transportation has become one of the most visible parts of Jakarta's smart city agenda. Earlier research on Jakarta smart transportation emphasized performance measurement and integrated mobility planning [5], [6], while more recent studies discussed public transportation service quality, JAKI-based smart mobility governance, and the role of commuter systems in Jakarta's mobility ecosystem [7], [8], [9], [10]. These studies provide useful urban and governance contexts, yet fewer studies explicitly combine Jakarta's open transportation data with IoT security, trust management, and machine learning.

In Jakarta, smart transportation data are produced by multiple operational entities. ATCS supports traffic-signal control and intersection management, CCTV provides visual monitoring points, TransJakarta records represent public-transport operations and service demand, road-speed observations describe traffic-state conditions, and congestion-risk or violation records indicate abnormal operational patterns. These data sources are not identical, but together they represent a city-scale transportation monitoring ecosystem that can be transformed into a trust-aware modeling structure.

Security-oriented smart transportation research has developed rapidly. Khan et al. [11] proposed a deep neural network and trust-management approach to secure smart transportation data in sustainable smart cities. Related studies have also examined DDoS detection, intrusion detection, misbehavior detection, and deep learning for IoT environments [12]–[19]. In the Internet of Vehicles domain, trust management has been used to identify unreliable or malicious nodes by combining location verification, stability,

distributed trust computation, and cooperative misbehavior detection [12]-[26]. These approaches are relevant to Jakarta because its transportation ecosystem contains many node-like entities, such as bus stops, ATCS signals, CCTV units, road corridors, and public-transport services.

In this study, a node is a modeling unit rather than one homogeneous physical device. It may represent a TransJakarta stop, CCTV point, ATCS signal, road-speed segment, ITS corridor, modal-share record, congestion-risk location, or traffic-violation area. An operational anomaly is an unusual mobility condition; a data-quality anomaly is an incomplete or inconsistent record; and an untrusted record is one whose researcher-defined score falls below 0.5. A cyberattack, by contrast, requires verified malicious activity. Because the Jakarta sources contain no verified attack logs, traffic violations and congestion-risk points are used consistently as trust-risk proxies. The current framework supports record-level data-quality and operational-risk screening, not validated cyberattack detection.

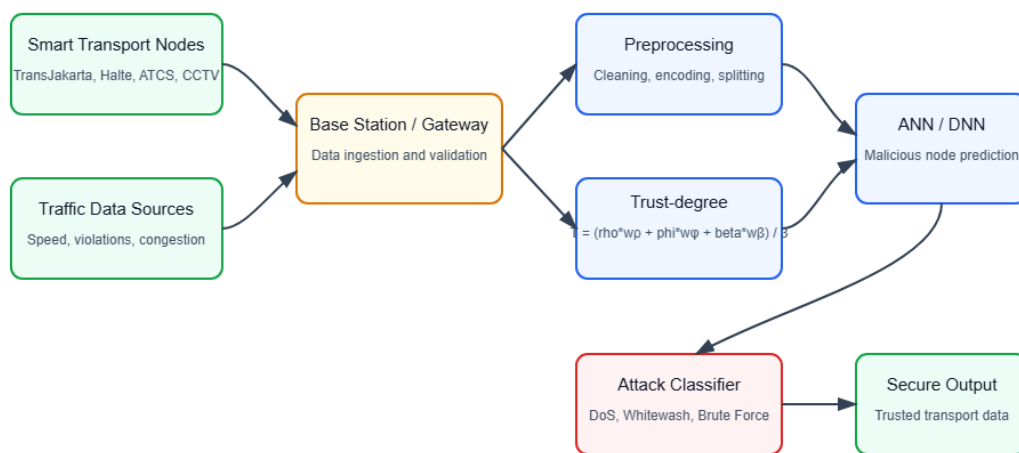
The objective is to construct a preliminary trust-aware modeling dataset and record-level trust framework for Jakarta smart transportation open data. The framework supports operational-risk monitoring and future trust-aware security analysis, but it does not yet provide validated cyberattack detection or deployed data-protection mechanisms. Many cyber-security datasets contain network-level attack labels, but they do not represent Jakarta's mobility conditions. Conversely, Jakarta's open data contains rich transportation and infrastructure information, but it does not directly include malicious-node labels. This study therefore constructs a localized modeling dataset by transforming Jakarta transportation datasets into a trust-aware format inspired by the secure smart transportation literature [11], [20], [21], [27]. The objective is not to claim that open transportation records directly prove cyber-attacks, but to prepare a transparent and reproducible dataset that can support anomaly detection, trust scoring, and later DNN experimentation. The contributions of this paper are:

Therefore, the central problem addressed in this study is how to transform heterogeneous Jakarta smart transportation open data into an auditable trust-aware modeling dataset without overstating the data as verified cyberattack evidence. The research gap lies between city-specific transportation open data, which are operationally rich but rarely

include security labels, and smart-transportation security models, which often rely on generic, simulated, or non-Jakarta datasets. Accordingly, this study aims to define transparent trust rules, generate provisional trusted and anomalous labels, and evaluate whether the resulting structure can support leakage-aware future DNN experiments for Jakarta Smart City data.

- 1) A Jakarta Smart Transportation modeling dataset based on local open data.
- 2) A trust-scoring mechanism that maps transportation records into trusted/non-malicious and anomalous/untrusted labels.
- 3) A methodological framework for future leakage-free DNN-based trust prediction using validated Jakarta labels.
- 4) Descriptive tables and figures generated from the constructed dataset.

The trust-aware Jakarta transportation data-engineering architecture is shown in Figure 1. It separates current dataset construction and exploratory record-level risk screening from the future validation and leakage-free modeling stages.



Localized Jakarta Smart City data pipeline adapted from trust-aware smart transportation architecture.

Figure 1. Trust-aware Jakarta transportation data-engineering framework

2. METHODS

2.1. Research Design

This study uses a data engineering and modeling-design approach. The framework adapts the trust-degree formulation in secure smart transportation research [11] and combines it

with IoT security and misbehavior-detection literature [11], [25]. The research pipeline consists of five stages:

- 1) Dataset selection from Satu Data Jakarta and the original article repository.
- 2) Data extraction and normalization into a unified node-based schema.
- 3) Trust-score construction using transparent heuristics.
- 4) Binary label generation for trusted/non-malicious and anomalous/untrusted records.
- 5) DNN-ready dataset preparation and descriptive analysis.

Figure 2 details how the research was conducted. First, transportation datasets were collected from official Jakarta open-data sources and the article baseline repository. Second, each source was extracted, cleaned at schema level, and normalized into a node-based structure. Third, source-specific trust rules converted operational indicators such as recency, completeness, status, speed, violation intensity, and congestion-risk status into trust scores. Fourth, the trust threshold generated provisional trusted/non-malicious and anomalous/untrusted labels. Finally, the study evaluated the resulting dataset using descriptive statistics, baseline ANN pipeline-consistency checks, threshold metrics, confusion-matrix diagnostics, and provisional Jakarta trust-risk bins.

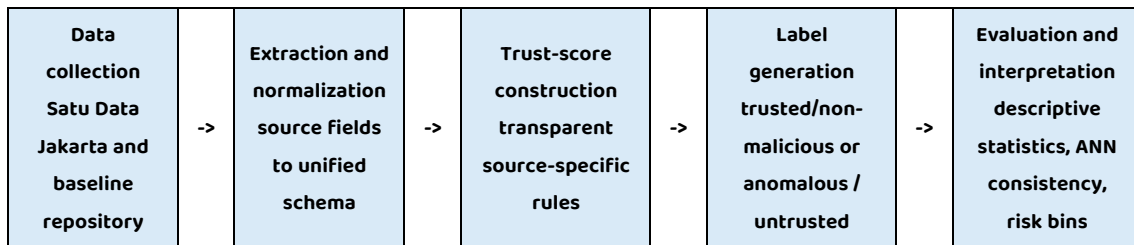


Figure 2. Research workflow from data collection to evaluation

The method follows the broader argument that smart city security requires data integrity, privacy-aware infrastructure, and trustable IoT systems [1], [2], [27]. It also follows transportation-security studies that recommend combining intelligent transportation data with cyber-security and blockchain-aware approaches [28], [29], [30].

2.2. Dataset Sources

The Jakarta dataset was constructed from nine Satu Data Jakarta sources maintained by the Provincial Government of DKI Jakarta [31]-[40]. Exact modeling snapshots are

preserved in the project archive, while Table 1 identifies the corresponding official catalog records. The separate article baseline was obtained from the Transport-Sustainable repository cited by Khan et al. [10].

Table 1. Jakarta dataset sources used in this study

No.	File and official catalog reference	Role in model	Rows
1	pelanggaran_lalu_lintas.csv [31]	traffic-violation proxy	810
2	kecepatan_jam_sibuk.csv [32]	average road speed	675
3	halte_transjakarta.csv [34]	transit-stop node	538
4	lokasi_atcs.csv [35]	traffic-signal node	419
5	lokasi_cctv_dishub.csv [36]	CCTV node	141
6	transjakarta_bus_penumpang.csv [37]	passenger/bus operation	73
7	koridor_busway_its.csv [38]	ITS corridor node	60
8	titik_rawan_kemacetan.csv [39]	congestion-risk proxy	38
9	modal_share_transportasi_publik.csv [40]	public-transport share	36
Total Jakarta modeling records			2,790

Sources: official Satu Data Jakarta portal and catalog records [31]-[40]; reproducible modeling snapshot: <https://zenodo.org/records/21712805>.

Table 1 identifies the official data sources and clarifies the role of each source in the modeling dataset; this is important because the trust framework depends on combining operational, infrastructure, and risk-related transportation records rather than a single homogeneous sensor stream. The implementation performs schema-level concatenation rather than geospatial-temporal fusion. It reads every source row, converts selected numeric strings, constructs a source-specific node_id, maps fields into the common schema, and concatenates the results. It does not explicitly remove duplicates or incomplete rows, nor merge records by time, corridor, node identity, or proximity. Table 2 reports these implemented operations so the 2,790-row snapshot can be reproduced. Future work should add auditable quality filters and geospatial-temporal integration. The baseline article dataset contains 10,000 records with four primary data types: sensor data, infrastructure data, traffic camera data, and GPS data. Its labels consist of 5,504 non-malicious records and 4,496 malicious/untrusted records.

Table 2. Preprocessing and Transformation Steps for Jakarta Smart Transportation Datasets

Source	Cleaning and normalization	node_id construction	value field
Traffic violations	Retain rows; convert jumlah to numeric; preserve labels	wilayah + enforcement type + period	violation count
Road speed	Retain rows; convert kecepatan to numeric; preserve labels	road segment + period	average peak-hour speed
TransJakarta stops	Retain rows; test whether both coordinates are present	stop name + row number	constant node indicator (1)
ATCS	Retain rows; preserve location, region, and period	ATCS row number + period	constant node indicator (1)
CCTV	Retain rows; convert jumlah; test status text for 'Aktif'	CCTV row number + period	reported unit count
Bus/passenger operations	Retain rows; convert passengers and buses to numeric	service type + period	passenger count
ITS corridors	Retain rows; preserve corridor and intersection labels	corridor + row number	constant node indicator (1)
Congestion-risk points	Retain rows; preserve location and description	row number + period	constant risk indicator (1)
Modal share	Retain rows; convert percentage to numeric	transport mode + period	reported share

Table 2 explains how heterogeneous fields were made comparable. The table shows that the transformation was intentionally transparent and reproducible, while also indicating where future work should add stronger temporal, spatial, and duplicate-record controls. The value field is a normalized source-dependent measurement. For road-speed data, value represents average speed. For passenger and bus operation records, value

represents passenger count or operational volume. For traffic-violation data, value represents violation count or intensity. For CCTV, ATCS, stops, and ITS corridor records, value may represent node availability, active status, or a binary infrastructure indicator when no continuous measurement is available. For modal-share data, value represents the reported share of public transport use. Because the meaning of value differs by data_type, the model should interpret value together with data_type rather than as a single universal physical measurement.

2.3. Unified Schema

Table 3 presents the common schema used to align all sources. This schema is the basis for later trust-score computation because it gives each record a node identity, data type, period, location, value, trust score, and output label. Every Jakarta source file was transformed into the following unified structure:

Table 3. Unified schema for the Jakarta smart transportation dataset

Field	Description
node_id	Synthetic node identifier from stop, road, ATCS, CCTV, ITS corridor, or violation record.
data_type	Standardized feature group such as average_speed, cctv_sensor_node, or traffic_violation_signal.
period	Original dataset period.
location	Road, stop, area, administrative region, or service label.
value	Main numeric measurement when available.
trust	Trust score from 0 to 1.
output	Binary label: 1 for trusted/non-malicious, 0 for anomalous/untrusted.
source_dataset	Source CSV filename.
raw_label	Additional original label from the source.

Table 4 is the operational core of the framework. It explains why certain records receive lower trust scores: low trust is assigned when the implemented rule detects older or missing periods, incomplete coordinates, inactive infrastructure status, low speed, high violation intensity, or predefined congestion-risk status.

Table 4. Complete implemented trust-score and label rules

Scope	Condition	Implemented trust rule	Output rule
Recency baseline	period missing	$T_{base} = 0.65$	threshold unless source forces label
Recency baseline	period 2024-2026	$T_{base} = 0.90$	threshold unless source forces label
Recency baseline	period 2020-2023	$T_{base} = 0.82$	threshold unless source forces label
Recency baseline	other period	$T_{base} = 0.72$	threshold unless source forces label
Bus/passenger	passengers/bus > 50,000	$T = T_{base} - 0.10$; otherwise T_{base}	$Y = 1$ if $T \geq 0.5$
Road speed	speed < 10	$T = T_{base} - 0.25$	$Y = 1$ if $T \geq 0.5$
Road speed	$10 \leq \text{speed} < 15$	$T = T_{base} - 0.15$; otherwise T_{base}	$Y = 1$ if $T \geq 0.5$
ATCS	all retained records	$T = T_{base}$	$Y = 1$
TransJakarta stop	coordinates complete / incomplete	$T = 0.92 / 0.78$	$Y = 1$
Modal share	all retained records	$T = T_{base}$	$Y = 1$
Traffic violation	count > 500	$T = 0.35$	$Y = 0$
Traffic violation	$100 < \text{count} \leq 500$	$T = 0.48$	$Y = 0$
Traffic violation	count ≤ 100 or missing	$T = T_{base} - 0.10$	$Y = 1$ if $T \geq 0.5$
Congestion-risk point	all retained records	$T = 0.45$	$Y = 0$
CCTV	status contains 'Aktif' / otherwise	$T = 0.88 / 0.55$	$Y = 1$ if $T \geq 0.5$
ITS corridor	all retained records	$T = T_{base}$	$Y = 1$

2.4. Implemented Heuristic Trust Computation

Trust-management studies use behavior, performance, interaction history, and consistency to estimate reliability [19], [25]. Equations (1)-(4) summarize the reference concepts; Equation (5) and Table 4 specify the distinct source-specific rules actually implemented for Jakarta. Following the reference article, experience, performance, and behavior are defined as shown in Equation (1) to (4):

$$\rho_n = \frac{\text{Number of Interactions}}{\text{Total Number of Possible Interaction}} \quad (1)$$

$$\phi_n = \frac{\text{Number of Successful Interactions}}{\text{Total Number of Interactions}} \quad (2)$$

$$\beta_n = \frac{\text{Number of Positive Interactions}}{\text{Total Number of Interactions}} \quad (3)$$

In the reference model, trust degree is expressed as the weighted combination in Equation (4):

$$\text{Trust-degree}_n = \frac{\rho_n \omega_p + \phi_n \omega_\phi + \beta_n \omega_\beta}{3} \quad (4)$$

In Equations (1)-(4), ρ_n is experience (observed interactions divided by possible interactions), ϕ_n is performance (successful interactions divided by observed interactions), β_n is behavior (positive interactions divided by observed interactions), and ω_p , ω_ϕ , and ω_β are the corresponding reference-model weights. Direct interaction logs are unavailable for Jakarta; consequently, Equation (5) defines the implemented source-specific rule function h rather than claiming unimplemented component weights.

$$T_n = h_{s(n)}(P_n, Q_n, V_n, S_n), \quad 0 \leq T_n \leq 1 \quad (5)$$

In Equation (5), T_n is the trust score for record n ; $s(n)$ identifies its source; P_n is period/recency; Q_n is completeness; V_n is the source-specific numeric value; and S_n is node status. The function h is fully specified in Table 4. The rules were researcher assumptions informed by the trust-management literature, not optimized weights or expert-validated ground truth.

The transformation script applies the exact base values, overrides, penalties, thresholds, and forced labels reported in Table 4. The binary label use Equation (6).

$$Y_n = \begin{cases} 1, & T_n \geq 0.5 \\ 0, & T_n < 0.5 \end{cases} \quad (6)$$

Here Y_n is a researcher-generated record-level trust label: $Y_n = 1$ denotes trusted/non-malicious and $Y_n = 0$ denotes anomalous/untrusted. It is not legally or operationally verified cyberattack evidence.

Implemented Source-Specific Trust-Score Procedure use Algorithm 1 as follow:

- 1) Read all records from the nine Jakarta source files without an explicit row-filtering step.
- 2) Convert selected numeric fields and construct node_id using the source-specific keys in Table 2.
- 3) Assign T_{base} from period: 0.90 for 2024-2026, 0.82 for 2020-2023, 0.72 for other periods, or 0.65 when missing.
- 4) Apply the source-specific completeness, coordinate, or active-status rule in Table 4.
- 5) Apply the exact speed, passenger-load, violation-count, or congestion-risk override/penalty in Table 4.
- 6) Store T to two decimal places and assign Y using the implemented threshold or source-specific forced label.
- 7) Export node_id, data_type, period, location, value, trust, output, source_dataset, and raw_label.

2.5. Future Leakage-Free DNN Formulation and Baseline Pipeline Check

A future Jakarta DNN should use raw or transformed predictors such as encoded data_type, source_dataset, grouped location, period, and normalized value, with output as the target. Encoding and scaling must be fitted only on training data. Because output is generated directly from the trust threshold, trust must be excluded from the predictor set to prevent label leakage and circular prediction. The reported baseline-repository replication is separate: it deliberately uses Trust as its sole input only to verify that the published trust-output pipeline is internally

consistent, not to estimate Jakarta performance. A future leakage-free DNN can be formulated as follows:

Equation (7) is a common architecture of a Deep Neural Network (DNN) with three layers (two hidden layers and one output layer):

$$\hat{y} = \sigma(W_3 F(W_2 F(W_1 X + b_1) + b_2) + b_3) \quad (7)$$

where X is the leakage-free feature vector; W_1 , W_2 , and W_3 are layer-weight matrices; b_1 , b_2 , and b_3 are bias vectors; f is the hidden-layer activation; z_n is the output logit; σ is the sigmoid function; and Y_n is the binary prediction defined by Equation (8). Equation (9) groups only sub-threshold values into provisional trust-risk bins; these bins are not attack labels. This formulation consists of DNN-based IoT intrusion and DDoS detection approaches [11], [17] and with misbehavior-detection frameworks in Internet of Vehicles research [19], [20], [41]. The sigmoid output is interpreted as:

$$\hat{Y}_n = \begin{cases} 1, & \sigma(z_n) \geq 0.5 \\ 0, & \sigma(z_n) < 0.5 \end{cases} \quad (8)$$

$$\text{Attack Type} = \begin{cases} \text{DoS}, & T < 0.1 \\ \text{Whitewash}, & 0.1 \leq T < 0.3 \\ \text{Brute Force}, & 0.3 \leq T \leq 0.4 \\ \text{Operational Anomaly}, & 0.4 < T < 0.5 \end{cases} \quad (9)$$

Future Leakage-Free DNN Procedure for Jakarta Records use Algorithm 2 as follows:

- 1) Input encoded data_type, source_dataset, grouped location, period, and normalized value; exclude trust.
- 2) Split records before fitting encoders or scalers; remove or impute missing values using training data only.
- 3) Use a stratified 70/30 split with a declared fixed seed for future Jakarta experiments.
- 4) Train and tune the ANN/DNN only on the training partition; use cross-validation where feasible.
- 5) Predict record-level trust status using the prespecified 0.5 decision threshold.

- 6) Report precision, recall, F1, ROC-AUC, PR-AUC, balanced accuracy, and a confusion matrix on held-out data.

Provisional Trust-Risk Binning from Trust Values use Algorithm 3 as follows:

- 1) Input the computed or predicted trust value T .
- 2) If $T < 0.1$, assign the critical trust-risk bin.
- 3) If $0.1 \leq T < 0.3$, assign the very-high trust-risk bin.
- 4) If $0.3 \leq T \leq 0.4$, assign the high trust-risk bin.
- 5) If $0.4 < T < 0.5$, assign the moderate trust-risk bin.
- 6) If $T \geq 0.5$, assign trusted/non-malicious status rather than a risk bin.

Because the Jakarta label is heuristically generated, this paper reports descriptive dataset results rather than claiming final classification accuracy. A future model-training experiment should validate labels using expert annotation, real incident logs, or controlled attack simulation. Although the study uses open data, transportation infrastructure data can have governance and security implications. The framework should avoid exposing sensitive operational vulnerabilities, should not identify specific infrastructure as compromised without validation, and should be used only for aggregate research, planning, and risk-screening purposes. Any deployment for cyber-security monitoring should involve the relevant data owners, transportation authorities, Jakarta Smart City stakeholders, and security experts.

3. RESULTS AND DISCUSSION

3.1. Dataset Composition

The Jakarta modeling dataset contains 2,790 records. Table 5 reports record counts and trust-score statistics by data type. Table 5 shows why the dataset should be interpreted as an operational-risk screening dataset: some data types have uniformly high trust values, while traffic-violation and average-speed records contain wider variation and therefore contribute more to the trust-risk signal. The largest component is traffic violation signal data, followed by average-speed data and TransJakarta stop nodes. This composition indicates that the constructed dataset combines operational behavior, traffic performance, and infrastructure-node information.

Table 5. Distribution and trust-score statistics by data type

Data type	Count	Mean T	Min	Max	Y=0
traffic_violation_signal	810	0.698	0.35	0.80	244
average_speed	675	0.882	0.65	0.90	0
transit_stop_node	538	0.920	0.92	0.92	0
traffic_signal_node	419	0.868	0.82	0.90	0
cctv_sensor_node	141	0.793	0.55	0.88	0
passenger_count	73	0.885	0.72	0.90	0
its_corridor_node	60	0.720	0.72	0.72	0
congestion_risk_location	38	0.450	0.45	0.45	38
public_transport_share	36	0.873	0.82	0.90	0
Total	2,790	-	0.35	0.92	282

3.2. Trust Label Distribution

The generated labels consist of 2,508 trusted/non-malicious records and 282 anomalous/untrusted records. Table 6 indicates that anomalous/untrusted records form a minority class. This imbalance explains why accuracy alone would be insufficient for later predictive modeling and why anomaly-sensitive measures are required. The class distribution is imbalanced, which is common in anomaly detection and intrusion detection problems. For future model training, this imbalance should be addressed using stratified splitting, class weighting, focal loss, resampling, or anomaly-sensitive metrics.

Table 6. Trust label distribution

Output label	Interpretation	Count	Percentage
1	trusted / non-malicious	2,508	89.9%
0	anomalous / untrusted	282	10.1%
	Total	2,790	100.0%

Warning: these percentages describe consistency with the researcher-defined trust threshold; they are not Jakarta attack-detection performance

3.3. Source Dataset Contribution

Table 7 explains the origin of the anomalous/untrusted labels. The concentration of Y=0 records in traffic violations and congestion-risk points occurs because the current rules

treat high violation intensity and predefined congestion risk as the clearest available open-data proxies for operational risk. Low-trust examples clarify the rule behavior. A Jakarta Barat traffic-violation record with value 1,140 is assigned $T=0.35$ and $Y=0$ because the count exceeds 500; records with counts from 101 to 500 receive $T=0.48$ and $Y=0$; and every congestion-risk point receives $T=0.45$ and $Y=0$. These are deterministic proxy labels, not verified incidents. Table 7 also shows that all 282 anomalous/untrusted labels come from only two sources, revealing limited anomaly coverage. The source contribution shows that the dataset is not dominated only by static infrastructure records. It combines mobility performance, public transport, traffic violations, and smart transportation infrastructure.

Table 7. Source contribution and anomalous/untrusted distribution

Source dataset	Records	Y=0	Y=0 rate
pelanggaran_lalu_lintas.csv	810	244	30.1%
kecepatan_jam_sibuk.csv	675	0	0.0%
halte_transjakarta.csv	538	0	0.0%
lokasi_atcs.csv	419	0	0.0%
lokasi_cctv_dishub.csv	141	0	0.0%
transjakarta_bus_penumpang.csv	73	0	0.0%
koridor_busway_its.csv	60	0	0.0%
titik_rawan_kemacetan.csv	38	38	100.0%
modal_share_transportasi_publik.csv	36	0	0.0%
Total	2,790	282	10.1%

3.4. Baseline-Repository ANN Pipeline-Consistency Check

The reference article reports approximately 90.31% ANN/DNN accuracy for malicious/non-malicious prediction. The present study separately replicates the public baseline repository using Trust as input and Output as target. The 10,000 rows are split deterministically by row index: indices with $i \bmod 10$ in 0-6 form the 70% training set, and indices with $i \bmod 10$ in 7-9 form the 30% test set. No pseudorandom generator is used; therefore, this implementation has no random seed. This baseline-only procedure must not be interpreted as a Jakarta experiment. It is important to interpret this result carefully: in the baseline dataset, Output is directly consistent with the trust threshold, meaning

that the ANN replication functions as a data-consistency and model-pipeline check rather than an independent cyber-attack validation experiment.

The ANN result obtained from the baseline trust-output dataset is reported only as a pipeline-consistency check. Because the output label is directly consistent with the trust threshold, the model can learn the trust-label relationship with near-perfect performance. This result should not be interpreted as empirical evidence of cyberattack-detection performance in Jakarta Smart City. In addition, using trust as an input to predict output creates label leakage when output is generated directly from trust. Future Jakarta model training should exclude the direct trust score from the predictor set, use raw and transformed transportation features, apply stratified splitting, and report precision, recall, F1-score, ROC-AUC, PR-AUC, balanced accuracy, and confusion matrix under the same experimental setting for all compared models. Figure 3 should be read as a baseline pipeline diagnostic. The high accuracy occurs because the public baseline target is directly consistent with the trust threshold, so the figure demonstrates implementation consistency rather than independent Jakarta cyberattack detection.

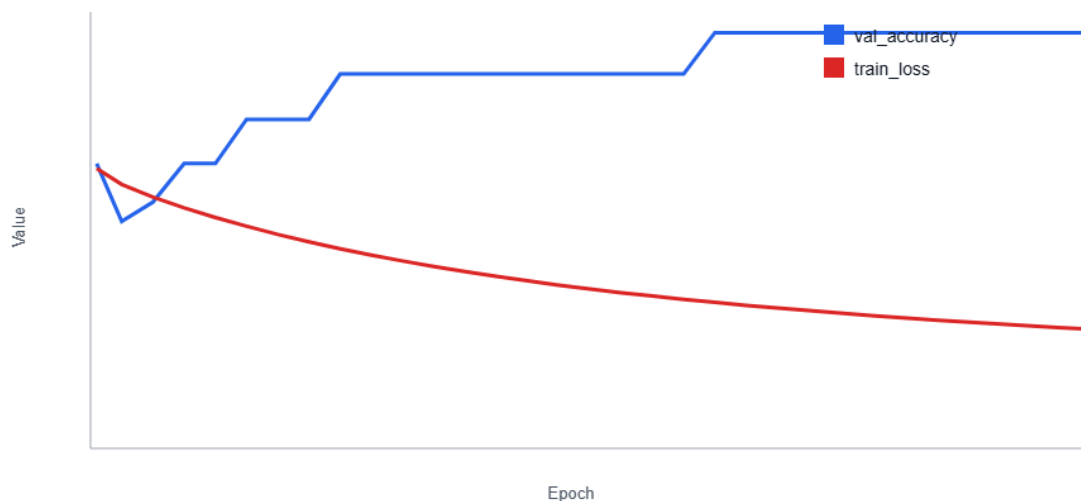


Figure 3. Baseline-repository ANN training and validation accuracy

3.5. Baseline-Repository ANN Training and Validation Loss

The training and validation loss curves describe the ability of the proposed ANN/DNN pipeline to learn the trust-output relationship. In the baseline replication, loss decreases across epochs, indicating convergence. Because the

public baseline label is threshold-consistent with trust, the curve should be interpreted as a pipeline validation result rather than final field deployment performance. Figure 4 complements the accuracy curve by showing convergence of the baseline ANN pipeline. The decreasing loss supports the interpretation that the model learned the threshold relationship, not that it discovered new field-validated attack behavior.

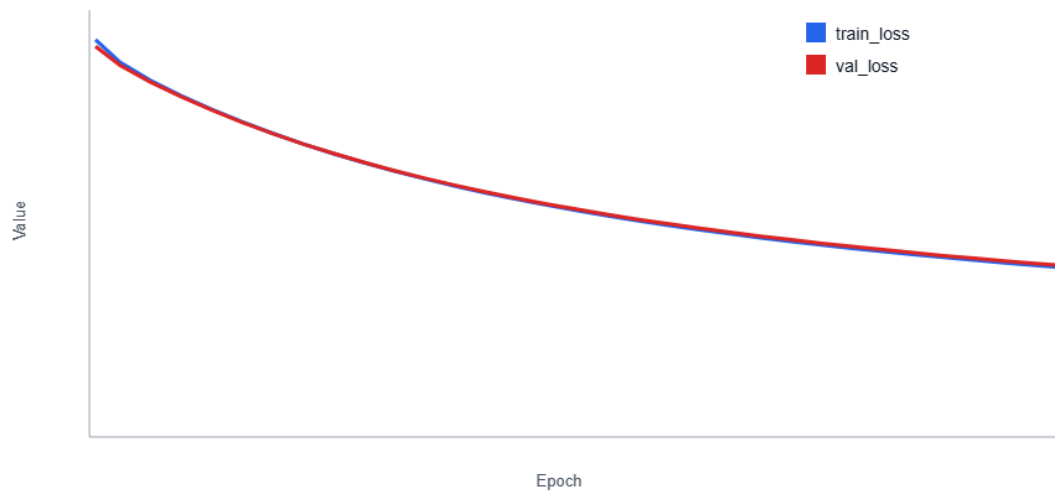


Figure 4. Baseline-repository ANN training and validation loss

3.6. Baseline Trust-Threshold Consistency Metrics

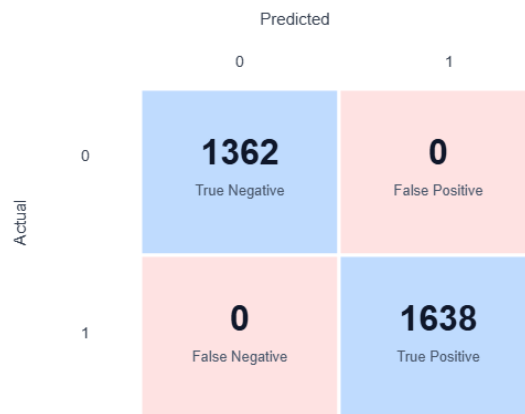
Table 8 reports perfect threshold-consistency metrics because the baseline output follows the same trust threshold used as input. The table is therefore retained only to document leakage risk and to justify the need for leakage-free evaluation in future experiments. Perfect values occur because Output is derived from the same trust threshold supplied to the baseline ANN. They measure pipeline consistency and label leakage, not independent attack detection or Jakarta generalization. The result differs from the 90.31% reported by Khan et al. [10] because the local replication uses the available public repository data, where the target label is threshold-consistent with the trust value. Therefore, the result should not be overstated as field-level attack-detection performance. It confirms that the implemented ANN pipeline correctly learns the trust-label relationship.

Table 8. Baseline-repository trust-threshold consistency metrics

Class	Precision	Recall	F1-score
0 anomalous/untrusted	1.00	1.00	1.00
1 trusted/non-malicious	1.00	1.00	1.00
accuracy	-	-	1.00

3.7. Baseline-Repository Trust-Threshold Consistency Confusion Matrix

The test split contains 3,000 baseline records. The confusion matrix shows 1,362 true negatives, 1,638 true positives, and no false predictions under the trust-threshold replication setting. Figure 5 visualizes the same threshold-consistency result as a confusion matrix. The absence of false predictions is expected under this replication setting and should not be generalized to Jakarta deployment.

**Figure 5.** Baseline-repository trust-threshold consistency confusion matrix.

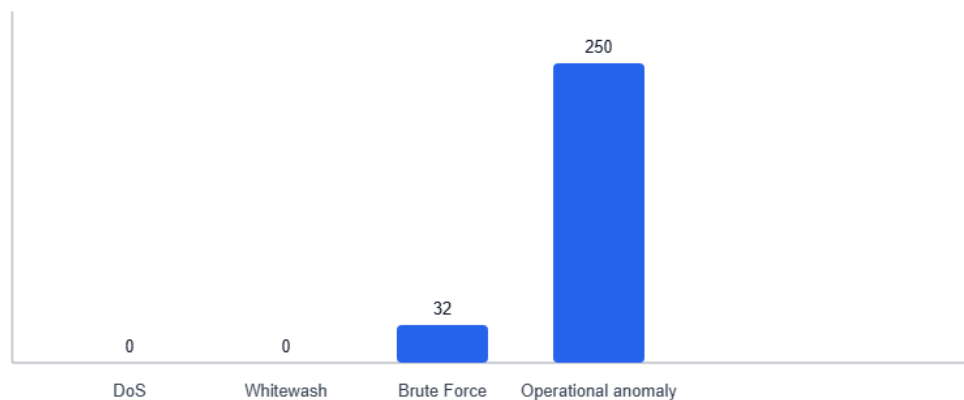
3.8. Trust-Risk Bins of Anomalous Jakarta Records

For Jakarta data, the provisional binning places 32 records in the high trust-risk range and 250 in the moderate range. No record falls below 0.3. This absence demonstrates that the heuristic rules do not cover the full risk continuum and cannot support an attack taxonomy. Table 9 groups the Jakarta anomalous/untrusted records by risk intensity. The absence of critical and very-high bins shows that the current heuristic rules identify moderate and high operational-risk proxies but do not yet represent a full cyberattack taxonomy.

Table 9. Provisional trust-risk bins for anomalous/untrusted Jakarta records

Trust range	Provisional trust-risk bin	Count
$T < 0.1$	Critical	0
$0.1 \leq T < 0.3$	Very high	0
$0.3 \leq T \leq 0.4$	High	32
$0.4 < T < 0.5$	Moderate	250
Total $Y=0$		282

Figure 6 makes the Table 9 pattern visible by showing that most anomalous Jakarta records fall into the moderate-risk bin. This distribution explains why the present dataset is more suitable for early screening and framework design than for final attack-severity classification.

**Figure 6.** Distribution of provisional trust-risk bins

3.9. Non-Experimental Literature Benchmark Context

Table 10 preserves the numerical context reported in the source article, but it is not a direct model comparison. Only the trust-aware ANN pipeline was replicated here; Random Forest, Naive Bayes, and SVM were not rerun on the same split, features, or preprocessing. Consequently, their values must not be used to rank models in this study [10]. Table 10 is included only as literature context. Because the non-ANN values were not rerun under the same features, split, and preprocessing, the table should not be used to claim model superiority.

Table 10. Non-experimental benchmark context (not a direct comparison)

Entry	Accuracy	Provenance / comparability
Trust-aware ANN pipeline	100.00%	Replicated threshold-consistency check; leakage present
Random Forest	85.00%	Source-article benchmark; not rerun here
Naive Bayes	82.00%	Source-article benchmark; not rerun here
SVM	80.00%	Source-article benchmark; not rerun here

3.10. Comparison with Article Baseline Dataset

Table 11 explains the methodological difference between the two datasets. The Jakarta dataset provides local open-data relevance, while the article baseline provides a more balanced trust-label structure for methodological comparison. The article baseline has a more balanced malicious/non-malicious distribution, while the Jakarta dataset is more operational and context-rich but less attack-balanced. Therefore, the article baseline is useful for model pretraining or methodological comparison, while the Jakarta dataset is useful for localization and contextual validation.

Table 11. Jakarta dataset and article-baseline comparison

	Records	Label 1	Label 0	Main role
Jakarta smart transportation dataset	2,790	2,508	282	Local smart-city context
Article transport-sustainable dataset	10,000	5,504	4,496	Baseline trust/malicious-node structure

3.11. Discussion

The results show that Jakarta's open transportation data can be transformed into a trust-aware smart transportation modeling dataset. This is important because most IoT security datasets are not city-specific, while most open city datasets do not contain direct cyber-security labels. The proposed transformation links these two needs: it uses real Jakarta

records for local relevance and applies trust-management logic from secure smart transportation and Internet of Vehicles research [10], [19], [25].

The main reason this transformation is useful is that Jakarta transportation open data already contain indirect signals of reliability and operational risk. Recency indicates whether a record reflects current infrastructure conditions, completeness indicates whether the record can be operationally interpreted, infrastructure status indicates whether a node is active, speed reflects traffic-state abnormality, and violation intensity reflects behavioral pressure on the transportation system. These variables do not prove cyberattacks, but they explain why trust scoring can serve as a first layer of data-quality and risk prioritization.

The results also explain why the anomalous/untrusted class is concentrated in only a few sources. Open datasets such as CCTV, ATCS, stops, and ITS corridors mainly describe infrastructure presence or status, so they provide limited evidence for abnormal behavior under the present rules. In contrast, traffic-violation and congestion-risk datasets directly encode undesirable operational conditions; therefore, they naturally generate more low-trust labels. This source dependence is a strength for transparency but a limitation for generalization.

The dominance of traffic-violation and average-speed records makes the dataset useful for data engineering and exploratory operational-risk screening, not validated intrusion detection. Moreover, Table 7 shows that only traffic violations and predefined congestion-risk points generate $Y=0$; the remaining seven sources generate none. This concentration is a consequence of the heuristic design and limits both coverage and generalization. The records must not be interpreted as direct cyberattacks [1], [2], [27], [29]. From a modeling perspective, the class imbalance in the Jakarta dataset needs careful treatment. DNN-based intrusion detection studies often face imbalanced distributions because attacks or anomalies are rarer than normal events [12], [18]. If this dataset is used for supervised learning, model evaluation should include precision, recall, F1-score, ROC-AUC, and confusion matrix. Accuracy alone can be misleading when the trusted class dominates.

This finding explains why future DNN evaluation must avoid using the final trust score as a direct predictor when the output label is derived from the same score. If trust is used

both to generate the label and to predict the label, the model can achieve very high performance by learning the rule itself. A stronger evaluation should instead use raw or independently transformed transportation features, expert-validated labels, and the same train-test split for all compared algorithms.

The trust score also needs future validation. In the present dataset, trust is calculated from transparent rules: recency, completeness, active status, speed condition, violation intensity, and congestion-risk status. This is appropriate for an initial localized framework, but future work should improve the trust score using expert judgment from transportation agencies, real incident reports, sensor uptime logs, or controlled malicious-node simulation. Trust-aware cooperative detection studies in connected vehicles show that behavior history, consistency, and distributed verification can improve misbehavior detection [20], [22], [24], [41].

Moving from heuristic labels to validated labels requires several stages. First, transportation and IoT-security experts should review the trust-score rules and label assignments. Second, sensor uptime logs, incident reports, and operational disruption records should be integrated to validate whether low-trust records correspond to real data-quality or operational problems. Third, controlled attack simulation can be used to generate verified cyberattack labels. Finally, leakage-free machine-learning models should be evaluated with cross-validation and tested against real-time operational data.

A Jakarta-specific contribution of this study is the integration of multiple urban transportation entities as nodes. ATCS and CCTV represent sensor/control nodes, TransJakarta stops and busway ITS corridors represent mobility infrastructure, average-speed records represent traffic state, while traffic violations and congestion-risk points represent abnormal operational conditions. This mapping supports the design of a smart city security model that is not limited to packet-level cyber logs, but also includes urban operational context. Such integration aligns with smart mobility and smart transportation studies in Jakarta [4], [9].

Real-time ATCS and CCTV integration would change the framework from static dataset construction to dynamic trust monitoring by adding event time, uptime, cross-source confirmation, and persistent-risk alerts. Such a transition requires data-owner approval,

secure access controls, expert-validated labels, incident linkage, and operational testing; without them, the framework is not cybersecurity-ready. Thus, the practical implication is that the proposed framework should be positioned as a trust-aware data-engineering foundation. It helps identify which records or sources deserve closer inspection, but it must be connected to incident logs, sensor uptime records, agency validation, and controlled simulations before it can support operational cybersecurity decisions.

4. CONCLUSION

This study developed a preliminary trust-aware dataset-construction and modeling framework for Jakarta smart transportation open data. Nine heterogeneous sources were harmonized into 2,790 record-level observations: 2,508 trusted/non-malicious and 282 anomalous/untrusted proxy records. The contribution is a transparent data-engineering pipeline and reproducible heuristic labeling design, not a deployed cybersecurity solution or validated Jakarta attack detector. The labels are researcher-defined and have not been validated by experts, real incident logs, sensor-uptime logs, or controlled attacks. No leakage-free DNN has been trained and evaluated on the Jakarta data, and the trust-risk bins are not verified attack categories. The perfect baseline-repository metrics reflect threshold consistency and label leakage only. Future work should combine expert annotation, controlled attack simulation, real ATCS/CCTV uptime and incident logs, stratified leakage-free training, cross-validation, comparable model baselines, and operational testing. These steps are prerequisites for moving from static exploratory screening to defensible real-time trust monitoring.

ACKNOWLEDGMENT

The authors acknowledge the institutional and collaborative support of Budi Luhur University, Buddhi Dharma University, the Ministry of Transport, Communications and Information Technology of Oman, and DHA Suffa University.

REFERENCES

- [1] M. H. Panahi Rizi and S. A. Hosseini Seno, "A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city," *Internet Things*, vol. 20, Art. no. 100584, Nov. 2022, doi: 10.1016/j.iot.2022.100584.
- [2] E. Kenneally, "Intelligent data security and privacy for smart cities," *IEEE Internet Things Mag.*, vol. 2, no. 3, pp. 7–9, Sep. 2019, doi: 10.1109/MIOT.2019.8950958.
- [3] S. Akhlaghi, M. B. Menhaj, and B. Masoumi, "A survey of the smart city data security and privacy-preserving approaches in the Internet of Things," in *Proc. 10th Int. Conf. Artif. Intell. Robot. (QICAR)*, Feb. 2024, pp. 379–385, doi: 10.1109/QICAR61538.2024.10496658.
- [4] R. Sari, F. Anindra, R. Kosala, B. Ranti, and S. H. Supangkat, "Model development of smart transportation using the performance measurement of smart city result with IT balance scorecard and IPA matrix: Jakarta case," in *Proc. Int. Conf. Inf. Syst. Technol.*, 2019, pp. 199–205, doi: 10.5220/0009907901990205.
- [5] A. Apriansyah, V. A. Nora, and A. Saufi, "Smart mobility concept for determining an integrated transportation network in Jakarta," in *Proc. Int. Conf. ICT Smart Soc. (ICISS)*, Sep. 2024, pp. 1–6, doi: 10.1109/ICISS62896.2024.10751138.
- [6] M. Owais, J. Sumabrata, and N. Yusuf, "Gender-based service quality evaluation of multimodal public transportation in DKI Jakarta," *Smart City*, vol. 4, no. 2, 2024, doi: 10.56940/sc.v4.i2.3.
- [7] M. A. Athaya and R. A. Sembiring, "Analisis tata kelola smart mobility di Jakarta melalui aplikasi Jakarta Kini (JAKI) oleh Jakarta Smart City tahun 2024," *J. Gov. Policy*, vol. 5, no. 1, pp. 134–145, Apr. 2025, doi: 10.21776/ub.jgp.2025.005.01.8.
- [8] D. B. Bellastuti and R. Fathurrahman, "Application of smart mobility in the DKI Jakarta transportation system with KRL commuter line transportation mode," *Asian J. Soc. Humanit.*, vol. 2, no. 3, pp. 535–542, Dec. 2023, doi: 10.59888/ajosh.v2i03.155.
- [9] D. Zubaida and S. Megawati, "Implementasi aplikasi Jakarta Kini (JAKI) dalam mewujudkan smart city di Unit Pelaksana Teknis Jakarta Smart City," *Publika*, vol. 11, no. 3, pp. 2231–2242, Jun. 2023, doi: 10.26740/publika.v11n3.p2231-2242.
- [10] S. Khan, S. Khan, A. Sulaiman, M. S. Al Reshan, H. Alshahrani, and A. Shaikh, "Deep neural network and trust management approach to secure smart transportation data in sustainable smart cities," *ICT Express*, vol. 10, no. 5, pp. 1059–1065, Oct. 2024, doi: 10.1016/j.icte.2024.08.006.

- [11] K. Kharoubi, S. Cherbal, and M. Akkal, "Machine learning and deep learning for enhanced DDoS detection in IoT-based intrusion detection system," in *Proc. 1st Int. Conf. Innov. Intell. Inf. Technol. (IC3IT)*, Dec. 2024, pp. 1–6, doi: 10.1109/IC3IT63743.2024.10869417.
- [12] S. Hizal, U. Cavusoglu, and D. Akgun, "A novel deep learning-based intrusion detection system for IoT DDoS security," *Internet Things*, vol. 28, Art. no. 101336, Dec. 2024, doi: 10.1016/j.iot.2024.101336.
- [13] A. S. Dina, A. B. Siddique, and D. Manivannan, "A deep learning approach for intrusion detection in Internet of Things using focal loss function," *Internet Things*, vol. 22, Art. no. 100699, Jul. 2023, doi: 10.1016/j.iot.2023.100699.
- [14] V. Ravi, T. D. Pham, and M. Alazab, "Deep learning-based network intrusion detection system for Internet of Medical Things," *IEEE Internet Things Mag.*, vol. 6, no. 2, pp. 50–54, Jun. 2023, doi: 10.1109/IOTM.001.2300021.
- [15] D. Agostinello, A. Genovese, and V. Piuri, "Anomaly-based intrusion detection system for DDoS attack with deep learning techniques," in *Proc. 20th Int. Conf. Secur. Cryptogr.*, 2023, pp. 267–275, doi: 10.5220/0012146100003555.
- [16] G. Chukwukelu, A. Essien, A. Salami, and E. Utuk, "Comparative analysis of machine learning techniques for DDoS intrusion detection in IoT environments," in *Proc. 21st Int. Conf. Smart Bus. Technol.*, 2024, pp. 19–27, doi: 10.5220/0012765200003764.
- [17] A. Hattak, F. Martinelli, F. Mercaldo, and A. Santone, "Leveraging deep learning for intrusion detection in IoT through visualized network data," in *Proc. 21st Int. Conf. Secur. Cryptogr.*, 2024, pp. 722–729, doi: 10.5220/0012768400003767.
- [18] J. J. Shirley and M. Priya, "A comprehensive survey on ensemble machine learning approaches for detection of intrusion in IoT networks," in *Proc. Int. Conf. Innov. Eng. Technol. (ICIET)*, Jul. 2023, pp. 1–10, doi: 10.1109/ICIET57285.2023.10220795.
- [19] H. M. Kelagadi, J. Chandra Sekhar, R. Rawat, N. Dhaliwal, S. Singh, and B. S. Saravana, "Misbehavior detection in the Internet of Vehicles using machine learning based situation identification," in *Proc. 8th Int. Conf. Commun. Electron. Syst. (ICCES)*, Jun. 2023, pp. 975–983, doi: 10.1109/ICCES57224.2023.10192779.
- [20] A. Mahmood, Q. Z. Sheng, W. E. Zhang, Y. Wang, and S. Sagar, "Toward a distributed trust management system for misbehavior detection in the Internet of Vehicles," *ACM Trans. Cyber-Phys. Syst.*, vol. 7, no. 3, pp. 1–25, Jul. 2023, doi: 10.1145/3594637.

- [21] Y. Zhang, C. Lv, C. Cheong, and Y. Cao, "An introduction to trust management in Internet of Vehicles," in *Communication, Computation and Perception Technologies For Internet of Vehicles*. Singapore: Springer, 2023, pp. 245–260, doi: 10.1007/978-981-99-5439-1_13.
- [22] A. Mahmood, Q. Z. Sheng, W. E. Zhang, and S. Yongchareon, "Trust-IoV: A distributed trust management system for misbehavior detection in the Internet of Vehicles," in *Trust Management in the Internet of Vehicles*. Boca Raton, FL, USA: Chapman and Hall/CRC, 2023, pp. 33–66, doi: 10.1201/9781003365037-3.
- [23] A. Mahmood, Q. Z. Sheng, W. E. Zhang, and S. Yongchareon, "Towards secure and resource efficient IoV networks: A hybrid trust management approach," in *Trust Management in the Internet of Vehicles*. Boca Raton, FL, USA: Chapman and Hall/CRC, 2023, pp. 67–92, doi: 10.1201/9781003365037-4.
- [24] R. Purkait, S. Tripathi, and S. Patnaik, "Location verification and stability with trust management for avoiding malicious vehicles in geographic routing for VANET," in *Proc. Smart City Challenges Outcomes Urban Transform. (SCOUT)*, Dec. 2021, pp. 243–248, doi: 10.1109/SCOUT54618.2021.00058.
- [25] L. Mendiboure, M. A. Chalouf, and F. Krief, "Towards a blockchain-based SD-IoV for applications authentication and trust management," in *Internet of Vehicles—Technologies and Services*, Lecture Notes in Computer Science, vol. 11253. Cham, Switzerland: Springer, 2018, pp. 265–277, doi: 10.1007/978-3-030-05081-8_19.
- [26] Z. Chen *et al.*, "UITDE: A UAV-assisted intelligent true data evaluation method for ubiquitous IoT systems in intelligent transportation of smart city," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 8, pp. 9597–9607, Aug. 2024, doi: 10.1109/TITS.2024.3373411.
- [27] Aarushi, A. Chauhan, S. Wadhawan, A. Kaur, and S. Sharma, "The convergence of blockchain and IoT in secure smart cities: A survey of applications, challenges, and opportunities," *Secur. Priv.*, vol. 8, no. 3, May 2025, doi: 10.1002/spy2.70046.
- [28] A. Jabbari, "Securing smart transportation: Blockchain and IoT for sustainable cities," in *Proc. IEEE Int. Smart Cities Conf. (ISC2)*, Oct. 2024, pp. 1–5, doi: 10.1109/ISC260477.2024.11004209.
- [29] R. Qamar, S. Siraj, and B. A. Zardari, "Cyber security for smart transportation system," in *Driving Green Transportation System Through Artificial Intelligence and Automation*. Cham, Switzerland: Springer, 2025, pp. 619–636, doi: 10.1007/978-3-031-72617-0_32.

- [30] C. Korkuc, Y. Genc, and E. Afacan, "Blockchain technology and cyber security in intelligent transportation systems," in *AIoT for Smart Transportation*. United Kingdom: Institution of Engineering and Technology, 2025, pp. 215–234, doi: 10.1049/PBTR047E_ch11.
- [31] "Data penindakan pelanggaran lalu lintas dan angkutan jalan tahun 2017," *Satu Data Jakarta*. Accessed: Aug. 24, 2026. [Online]. Available: https://satudata.jakarta.go.id/open-data/detail?kategori=dataset&page_url=data-penindakan-pelanggaran-lalu-lintas-dan-angkutan-jalan-tahun-2017&data_no=1
- [32] "Kecepatan rata-rata di 41 koridor jalan utama pada jam sibuk," *Satu Data Jakarta*. Accessed: Aug. 24, 2026. [Online]. Available: https://satudata.jakarta.go.id/open-data/detail?kategori=dataset&page_url=kecepatan-rata-rata-di-41-empat-puluh-satu-koridor-jalan-utama-pada-jam-sibuk
- [33] "Portal Satu Data Jakarta—Data terbuka DKI Jakarta," *Satu Data Jakarta*, 2026. [Online]. Available: <https://satudata.jakarta.go.id>
- [34] "Data halte bus Transjakarta," *Satu Data Indonesia*. Accessed: Aug. 24, 2026. [Online]. Available: <https://data.go.id/dataset/dataset/data-halte-bus-transjakarta>
- [35] "Data lokasi lampu lalu lintas ATCS terintegrasi aktif tahun 2022," *Satu Data Indonesia*. Accessed: Aug. 24, 2026. [Online]. Available: <https://data.go.id/dataset/dataset/data-lokasi-lampu-lalu-lintas-atcs-atcs-terintegrasi-aktif-tahun-2022>
- [36] "Data pemetaan lokasi CCTV Dinas Perhubungan Provinsi DKI Jakarta," *Satu Data Indonesia*. Accessed: Aug. 24, 2026. [Online]. Available: <https://data.go.id/dataset/dataset/data-pemetaan-lokasi-cctv-dinas-perhubungan-provinsi-dki-jakarta>
- [37] "Data jumlah bus yang beroperasi dan jumlah penumpang layanan Transjakarta," *Satu Data Indonesia*. Accessed: Aug. 24, 2026. [Online]. Available: <https://data.go.id/dataset/dataset/data-jumlah-bus-yang-beroperasi-dan-jumlah-penumpang-layanan-transjakarta>
- [38] "Data lampu lalu lintas terintegrasi Intelligent Transport System Area Traffic Control System (ITS ATCS)," *Satu Data Indonesia*. Accessed: Aug. 24, 2026. [Online]. Available: <https://data.go.id/dataset/dataset/data-lampu-lalu-lintas-terintegrasi-intelligent-transport-system-area-traffic-control-system-it>

- [39] "Data titik rawan kemacetan di DKI Jakarta," *Satu Data Indonesia*. Accessed: Aug. 24, 2026. [Online]. Available: <https://data.go.id/dataset/dataset/data-titik-rawan-kemacetan-di-dki-jakarta>
- [40] "Persentase perjalanan penduduk menggunakan moda transportasi publik," *Satu Data Indonesia*. Accessed: Aug. 24, 2026. [Online]. Available: <https://data.go.id/dataset/dataset/persentase-perjalanan-penduduk-menggunakan-moda-transportasi-publik>
- [41] A. Attiaoui, M. Elmachkour, A. Kobbane, M. Ayaida, and H. Tembine, "Trust-aware and game-theoretic cooperative detection of misbehavior in connected vehicles," *Internet Things*, vol. 34, Art. no. 101799, Nov. 2025, doi: 10.1016/j.iot.2025.101799.