

Securing OBD II sensor technology using cryptographic method in safety-based driver behavior analysis

Siddhanta Kumar Singh [†]

Vijay Shankar Sharma ^{*}

Sandeep Kumar Sharma [§]

Department of Computer and Communication Engineering

Manipal University Jaipur

Jaipur 303007

Rajasthan

India

Atul Srivastava [‡]

Department of Computer Science and Engineering

Amity School of Engineering and Technology

Lucknow 226028

Uttar Pradesh

India

Anuradha Pillai [@]

Department of Computer Science and Engineering

Symbiosis Institute of Technology

Pune 412115

Maharashtra

India

Abstract

Transportation plays a important role in our everyday life, but increasing vehicle numbers worsen traffic congestion and hence requires to focus the security issues. Safety is a key concern, especially in India, which faces significant road safety challenges. Analyzing driving styles can aid authorities in identifying errors and enhancing security measures. This study investigates integrated sensor and computing systems for assessing driving

[†] E-mail: Siddhanta.singh@jaipur.manipal.edu

^{*} E-mail: vijayshankar.sharma@jaipur.manipal.edu (Corresponding Author)

[§] E-mail: sandeep.sharma@jaipur.manipal.edu

[‡] E-mail: atul.nd2@gmail.com

[@] E-mail: anuradha.pillai@sitpune.edu.in

behaviors and provide security to the system. It evaluates driver performance across speed, acceleration, deceleration, and rpm scenarios using OBD II sensors linked to the Electronic Control Unit (ECU). Torque Pro analyzes raw data from OBD II readers to assess driving styles, categorizing results as safe, normal, aggressive, or dangerous. A t-test, conducted using IBM SPSS, assesses differences between GPS and OBD II speeds to select appropriate datasets. The driving dataset is stored in Firebase cloud for analysis. Securing OBD II dataset in Firebase Cloud involves ensuring data integrity, confidentiality, and availability.

Subject Classification: Primary 68M25, Secondary 94A60.

Keywords: Controller area network, Diagnostic trouble codes, Electronic controller unit, On board diagnostics II, Parameter ID.

1. Introduction

Each car has a small device inside called an ECU [1], or electronic control unit, which is responsible for controlling a particular function. While some vehicles have a single ECU in charge of everything, others have multiple ECUs controlling various features.

The OBD-II port is linked to one or more communication buses inside the car. The CAN protocol broadcasts all network communication to every node on a specific bus at high speed. Any device plugged into the port acts like another ECU. All OBD-II protocols are supported, including ISO9141-2, ISO14230-4 (KWP2000), ISO15765-4 (Controller Area Network), J1850 VPW, and J1850 PWM. supports several apps, including Scan Master for PC, PPC (Windows Mobile) system mobile phone, OBDscope software for Symbian devices, and TORQUE software for Android smartphones. A basic twisted pair system is used to represent the Communications Serial Bus, or CAN. This is how it becomes impervious to noise and electrical interference. The study's analysis of parametric tests focuses mostly on the three t-tests [5].

2. Related works

The literature survey provides a comprehensive overview of research related to OBD II sensor technology. Jaware et al. [10] developed a module for two-wheelers, employing an algorithm and application to analyze data and generate statistics, aiming to ensure adherence to acceptable ranges. Joseph and Kumar [11] aimed to create a functional PSoC platform for monitoring live data in automobiles. Hwang and Chen [9] utilized smartphones to capture OBD-II data for driving behavior analysis. Hermawan and Husni [8] conducted a literature review on driving behavior, focusing on data gathering, analysis, and modeling techniques. Nishita et al. [6] proposed a three layered IoT architecture integrating OBD-II ports with sensors. Kaushitha et al. [12] proposed vehicle overspeed-detecting technologies, while Barbier et al. [4] examined real-world statistics of hybrid cars, and Hamed et al. [7] used machine learning to predict fuel usage. Ali and Alwan [2] differentiated speed changes of vehicles and

pedestrians, and Bánhelyi and Szabó [3] focused on algorithm development for data analysis. Khorsravania et al. [13] proposed a cost-effective CAN data collection approach. Kim and Baek [14] proposed a method for extracting in vehicle information using sensor data.

2. Methodology

The methodology used to determine the driving behavior is represented by the equations 1, 2, 3 and 4 as mentioned below. The driving behavior is categorized as Safe, Normal, Aggressive and Dangerous based on the accelerations.

$$\text{Safe Driving: } |a| \leq 2m/s^2: |G| \leq \frac{2}{9.8121} \approx 0.203G \quad (1)$$

$$\text{Normal Driving: } 2m/s^2 < |a| \leq 4m/s^2: 0.203G < |G| \leq 0.407G \quad (2)$$

$$\text{Aggressive Driving: } 4m/s^2 < |a| \leq 7m/s^2: 0.407G < |G| \leq 0.713G \quad (3)$$

$$\text{Dangerous Driving: } |a| > 7m/s^2: |G| > 0.713G \quad (4)$$

Table 1 mentions the various statistics of GPS and OBD - standard error means and mean standard deviation. Using the SPSS, we compute independent sample of t test. Equation 5 provides formula for computing independent sample t test. Here the first group's sample size is n_1 , and the second group's sample size is n_2 . The sample means for the first and second groups are $\bar{X}_1$ and $\bar{X}_2$, respectively. According to the theory of null-hypothesis(H_0), there is no variation in the mean of the groups. When the H_0 is rejected, there will be sufficient proof to conclude that not all means are equal. Test Statistics: We can obtain the Lavene statistics equation 6 given M , sample size N , which is split into k subgroups, and N_i , the size of the sample in the i th subgroup.

$$H_0: \sigma_1^2 = \sigma_2^2 = \sigma_3^2 \dots = \sigma_k^2 \text{ and } H_a: \sigma_i^2 \neq \sigma_j^2 \text{ for at least the pair } (i,j)$$

1. $Z_{ij} = |M_{ij} - \bar{M}_l|$ where, $\bar{M}_l$ is i^{th} subgroup mean
2. $Z_{ij} = |M_{ij} - \tilde{M}|$ where, $\tilde{M}$ is the i^{th} subgroup median
3. $Z_{ij} = |M_{ij} - \bar{M}'|$ Where, $\bar{M}'_l$ is the i^{th} subgroup, 10% trimmed mean. Z_{ij} and $\bar{Z}_l$ have group means $\bar{Z}_l$ and overall mean of Z_{ij}

$$t = \frac{\bar{X}_1 - \bar{X}_2}{\sqrt{\frac{\sum_{i=1}^n x_{i1}^2 - \frac{(\sum_{i=1}^n x_{i1})^2}{n_1} + \sum_{i=1}^n x_{i2}^2 - \frac{(\sum_{i=1}^n x_{i2})^2}{n_2}}{n_1 n_2 (1 - \frac{2}{n_1 + n_2})}}} \quad (5)$$

Table 1
OBD vs GPS Group statics

	Group	N	μ	σ	Std. Error Mean
Speed	1	357	31.1317	12.85035	.68011
	2	357	30.4548	12.23935	.64777

Table 2(a)
Test for Independent Sample

		<i>Equality_of_Variances</i> _{Levene Test}		<i>Equality_of_Means</i> _{t-test}	
		F	Sig.	t	df
Speed	Assumed Equal variances	.892	.345	.721	712
	Not assumed Equal variances			.721	710.317

Table 2(b)
Test for Independent Sample

		<i>Equality of Meanst-test</i>			
		Sig		Mean_Diff	Std. Error_Diff
		One_Sided _n	Two_Sided _n		
Speed	Assumed Equal variances	.236	.471	.67681	.93924
	Not assumed Equal variances	.236	.471	.67681	.93924

Table 2(c)
Independent Sample test

		Equality of Means t-test	
		Confidence Interval(95%)	
		Lower	Upper
Speed	Equal_variances _{assumed}	-1.16720	2.52081
	Equal variances _{Not assumed}	-1.16721	2.52082

As we can see in the Independent Sample test in the above in Table 2(a), 2(b) and 2(c), the value of Significance is quite higher than 0.05, hence the H₀ is accepted. The Independent Samples Effect Sizes are given in Table 3 at 95% Confidence Interval.

$$W = \frac{(N-k) \sum_{i=1}^k N_i (\bar{Z}_i - \bar{Z}_c)^2}{(k-1) \sum_{i=1}^k \sum_{j=1}^{N_i} (\bar{Z}_{ij} - \bar{Z}_i)^2} \quad (6)$$

Table 3
Effect Sizes of Independent Samples

		Standardiser ^a	Point_Estimation	Interval of Confidence 95%	
				Low	High
Speed	Cohens-d	12.54857	.054	-.093	.201
	Hedges' correction	12.56181	.054	-.093	.200
	Glass's delta	12.23935	.055	-.091	.202

The t test effect size of independent samples is measured by using Cohen's d as given by equation 7.

$$\text{Cohen's } d = \frac{\mu_1 - \mu_2}{\sigma} \quad (7)$$

Where, μ_1 , μ_2 mean of the sample 1 and 2 respectively, μ_2 is the standard deviation. We can estimate it by combining the standard deviations of our two groups as given in equation 8. In this case, M is the group mean (as indicated by the group numbers), and V^2 denotes the group variance.. The hedges(g), also known as d, is used in order to find the effect size. The Corrected version of Hedge's of the Cohen's d as shown in equation 9.

$$\sigma = \sqrt{\frac{(M_1 - 1) * V_1^2 + (M_2 - 1) * V_2^2}{M_1 + M_2 - 2}} \quad (8)$$

$$d = \frac{\bar{x}_1 - \bar{x}_2}{\hat{\sigma}} \quad (9)$$

Where, $\bar{x}_1$ sample1 mean, $\bar{x}_2$ sample2 mean, $\hat{\sigma}$ estimated standard deviation. The Glass's delta is an accurate measure of effect size if the standard deviations of the two sample groups are different as given below in equation 10.

$$\delta = \frac{\bar{x}_1 - \bar{x}_2}{\sigma_2} \quad (10)$$

Where, $\bar{x}_1$ denotes sample1 mean, $\bar{x}_2$ denotes sample2 mean, σ_2 is standard deviation. But if the standard deviations of the two groups do not significantly differ, then Cohen's d and Hedges' g are more suitable for measuring the effect size. Cohens d and Hedges g are more sensitive to small differences in means than Glass delta. A positive G value means acceleration and a negative G value stands for deceleration. By using the key components—encryption, access control, and integrity, we can efficiently secure the OBD II dataset in Firebase Cloud. Encrypt the OBD II dataset using AES before storing it in Firebase. For encryption, store C in Firebase using the equation 11 and 12.

$$C = E_k(P) \quad (11)$$

$$P = D_k(C) \quad (12)$$

Implement RBAC policies in Firebase security rules for access control as

$\text{canAccess}(u, p) \iff \exists r \in \text{such that } (u, r) \in RA \text{ and } (r, p) \in PA$

Where, Roles (R): $R = \{r_1, r_2, \dots, r_n\}$, Permissions (P): $P = \{p_1, p_2, \dots, p_m\}$, Users (U): $U = \{u_1, u_2, \dots, u_k\}$, Role Assignment (RA): $RA \subseteq U \times R$, Permission Assignment (PA) : $PA \subseteq R \times P$. For integrity, generate hash H, store H alongside C and on retrieval, recompute H' using the following equation 13 and 14.

$$\text{Store } H = h(P) \quad (13)$$

$$\text{Verify } H' = h(P) \quad (14)$$

Where, h = Cryptographic hash function (SHA-256), P = Plaintext OBD II dataset, H = Hash value, P=Plaintext OBD II dataset, k = Symmetric encryption key, E_k = AES encryption function, C = Ciphertext. In the end, we can determine the percentage driving of a driving behavioral mode in the whole

course of the journey. This parameter is very important as it would tell us how much percentage of the journey the vehicle was in safe, normal, aggressive and dangerous mode. We can find the PDM (percentage of driving mode) using the following equation 11.

$$\text{PDM} = \frac{\text{Total driving at a particular mode given by def variable}}{\text{Total driving baviours of all modes given by sum of all def}} * 100 \quad (11)$$

3. Result Analysis

Figure 1 shows the acceleration during the course of journey. Though, we can see here some of the journeys have quite higher acceleration such as 11.87m/sec^2 at time 11:25:20 AM on the time axis but no sign of dangerous acceleration. That is because of the slow speed ($<24\text{km/hr}$) which was not considered dangerous driving. Figure 2 shows the driving style during the entire course of the journey. A magnitude of 1 represents Safe, 2 represents Normal, 3 represents Aggressive and 4 represents Dangerous driving style. The data logger logged 207 safe, 74 normal, 26 aggressive and 0 dangerous driving styles at an interval of 0.5 seconds for 545 instances in the course of the journey. According to algorithm we can find the following results using the equation 1 regarding the behavior of the driver.

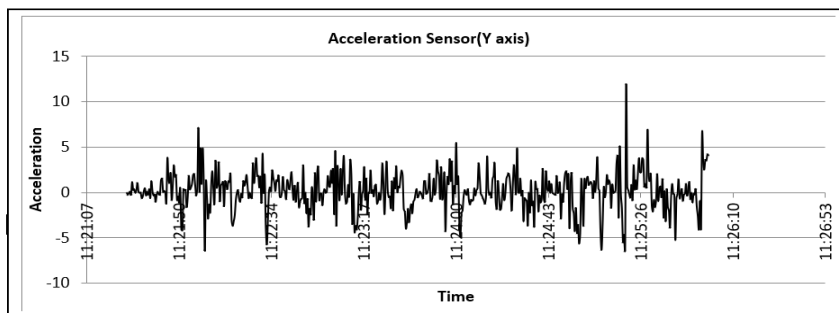


Figure 1
Acceleration Sensor data

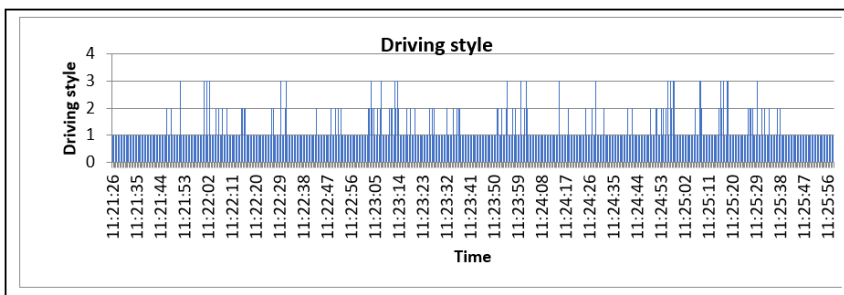


Figure 2
Driving style

$$\begin{aligned} \text{PDM}_{\text{safe}} (\text{percentage of driving mode}) &= \frac{207}{207+74+26+0} * 100 \% \\ &= 67.43\% \end{aligned}$$

Similarly, we can calculate the percentage of driving modes for normal, aggressive, and dangerous styles as 24.10%, 8.47% and 0% respectively. The figure of PDM can be increased by the nature of driving of the driver.

4. Conclusion

The use of intelligent sensors with computation in the cloud for local authority can revolutionize security and safety challenges and produce more sophisticated, next-generation safe driving. This research work can also be extended to find the driving behavior at a slow speed. In that case, besides accelerations, we can consider other parameters such as vectored directions of accelerations besides magnitude to determine the accidents and their behavior. This work to determine the driving behavior will be useful in the transport department to figure the nature of the driving and eventually determine the fuel consumption causes, and the driver of the vehicle might be awarded accordingly for the nature of driving. This work can also be useful for the insurance and local authority to find reckless driving nature of the driver to take final decision against or for the driver.

References

- [1] <https://www.keihin-na.com/automotive/electronic-control-units/> [Accessed in Mar, 2024]
- [2] Hamid M. Ali and Zainab S. Alwan, "Car Accident Detection and Notification System Using Smartphone", *International Journal of Computer Science and Mobile Computing*, vol. 4, no. 4, pp. 620 – 635 (2015).
- [3] Balázs Bánhelyi and Tamás Szabó, "Data Mining and Analysis for Data From Vehicles Based on the OBDII Standard", 11th International Conference on Applied Informatics, pp. 30-37 (2020).
- [4] Alvin Barbier, Jose M. Salavert, Carlos E. Palau and Carlos Guardiola, "Analysis of Real-Driving Data Variability for Connected Vehicle Diagnostics", *IFAC-PapersOnLine*, vol. 55, no. 24, pp. 45-50 (2022).
- [5] Banda Gerald, "A Brief Review of Independent, Dependent and One Samplet-test", *International Journal of Applied Mathematics and Theoretical Physics*, vol. 4, no. 2, pp. 50-54 (2018).
- [6] Goyal Nishita, Goel Vibhu, Anand Manan, and Garg Sahil, "Smart Vehicle: Online Prognosis for Vehicle Health Monitoring", *Smart*

- Vehicle: Online Prognosis for Vehicle Health Monitoring, vol. 9, no. 2, pp.12- 22 (2020).
- [7] Mohamed A. HAMED, Mohammed H. Khafagy, Rasha M. Badry and Fayoum University, "Fuel Consumption Prediction Model using Machine Learning", *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 11 (2021).
 - [8] Galih Hermawan and Emir Husni, "Acquisition, Modeling, and Evaluating Method of Driving Behavior Based on OBD-II: A Literature Survey", *IOP Conference Series. Materials Science and Engineering*, vol. 879, no. 1 (2020).
 - [9] Shu-Lin Hwang and Yen-Jen Chen, "Combining OBD Technology with Acceleration Sensor to Analyze Aggressive Driving Behavior", *American Journal of Engineering Research (AJER)*, vol. 7, no. 12, pp. 139-144 (2018).
 - [10] Kamlesh Jaware, Rana Tonpe, Pritam Jadhav, Deepak Parmar and Bhushan Pawar, "On Board Diagnostics and Troubleshooting for Two Wheelers", *International Journal of Innovative Research in Technology*, Vol 9, Issue 2, pp. 496 – 500 (2022).
 - [11] Pretty C. Joseph and S. Pratap Kumar, "Design and Development of OBD-II Compliant Driver Information System", *Indian Journal of Science and Technology*, vol. 8, no. 21, pp. 1-7 (2015).
 - [12] K. K. S. Kaushitha, K. Prajna, K. Kavana, Akshatha, and S. N. R. Sharathchandra, "A Literature Review Paper on Different Techniques used in Vehicle Over Speed Detection", *International Journal of Engineering Research & Technology (IJERT)*, vol. 7, no. 8, pp. 1-3 (2019).
 - [13] Kavian Khorsravinia, M. Hassan, R. A. Rahman and S. Al-Haddad, "Integrated OBD-II and mobile application for electric vehicle (EV) monitoring system", *IEEE 2nd International Conference on Automatic Control and Intelligent Systems (I2CACIS)*, pp. 202-206 (2017).
 - [14] Beomjun Kim and Yunju Baek, "Sensor-Based Extraction Approaches of In-Vehicle Information for Driver Behavior Analysis", *Sensors*, vol. 20, no. 18 (2020).

Received October, 2024