Deep-Learning based Trust Management with Self-Adaptation in the Internet of Behavior

Hind Bangui*
Faculty of Informatics, Masaryk University
Brno, Czech Republic
hind.bangui@mail.muni.cz

Emilia Cioroaica
Fraunhofer IESE
Kaiserslautern, Germany
emilia.cioroaica@iese.fraunhofer.de

Mouzhi Ge
Deggendorf Institute of Technology
Deggendorf, Germany
mouzhi.ge@th-deg.de

Barbora Buhnova
Faculty of Informatics, Masaryk University
Brno, Czech Republic
buhnova@fi.muni.cz

ABSTRACT

Internet of Behavior (IoB) has emerged as a new research paradigm within the context of digital ecosystems, with the support for understanding and positively influencing human behavior by merging behavioral sciences with information technology, and fostering mutual trust building between humans and technology. For example, when automated systems identify improper human driving behavior, IoB can support integrated behavioral adaptation to avoid driving risks that could lead to hazardous situations.

In this paper, we propose an ecosystem-level self-adaptation mechanism that aims to provide runtime evidence for trust building in interaction among IoB elements. Our approach employs an indirect trust management scheme based on deep learning, which has the ability to mimic human behaviour and trust building patterns. In order to validate the model, we consider Pay-How-You-Drive vehicle insurance as a showcase of a IoB application aiming to advance the adaptation of business incentives based on improving driver behavior profiling. The experimental results show that the proposed model can identify different driving states with high accuracy, to support the IoB applications.

KEYWORDS

Trust Management, Deep learning, Internet of Behavior, Autonomous Systems

ACM Reference Format:
Hind Bangui, Emilia Cioroaica, Mouzhi Ge, and Barbora Buhnova. 2023. Deep-Learning based Trust Management, with Self-Adaptation in the Internet of Behavior. In *The 38th ACM/SIGAPP Symposium on Applied Computing (SAC '23), March 27-March 31, 2023, Tallinn, Estonia.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3555776.3577694

*Dr. Bangui.

SAC '23, March 27-March 31, 2023, Tallinn, Estonia

ACM ISBN 978-1-4503-9517-5/23/03…$15.00
https://doi.org/10.1145/3555776.3577694

1 INTRODUCTION

Internet of Behavior (IoB) is an advancement of the traditional Internet of Things (IoT) that aims at: (a) the understanding of human behavior and (b) inter-playing of human behaviour with other technical entities, mutually influencing each other. That can be used to positively influence human behavior towards safer and more trusted cooperation in our societies [24, 33]. From the business perspective, IoB builds on consolidating the human acceptance of the technology-driven development and accelerates trustworthy digitization. By combining trust management between humans and machines, IoB aims at leveling up collaboration between humans and machines in various domains such as smart homes, healthcare, and transportation.

However, IoB can only be effective when the interplay of human and machine behaviour is supported with trust management between the human and digital actors. There are three typical trust interactions that need to be supported, which are human-to-machine trust, machine-to-human trust, and machine-to-machine trust. Human-to-machine trust characterizes the trust of a human in devices or machines; machine-to-human trust characterizes the trust of devices in people based on their behaviour; and machine-to-machine trust considers the trust between digital or physical entities. In this paper, we focus on the machine-to-human trust where machines can be used to help humans or prevent unsafe human operations by influencing human behaviour.

The machine-to-human trust assessment with the interconnected effects on human behaviour has recently emerged as a promising research and industrial topic. For example, the concept of Pay-How-You-Drive (PHYD), can have positive effects on safer driving and a direct impact on business for usage-based insurance companies (UBI). Based on data analysis and the interplay of technology with driving behavior, these companies may provide a discount on the premium insurance. In these scenarios, cloud-based technologies can be used to leverage information derived from the process of collecting data on driving behavior, such as proper acceleration or deceleration. As a result, AI algorithms within PHYD can encourage drivers to adopt safer driving behavior with the return of insurance incentives. For the society, PHYD contributes to minimizing speed violations and the number of accidents by motivating drivers to

drive safer, which leads to changes of insurers' behavior and increases road safety within a collaborative business evolving within complex digital ecosystems.

Despite attempts using advanced machine learning or deep learning, automatic classification for driving behaviors with the adoption of PHYD pricing models is still in its infancy stage due to its low acceptability by drivers [10]. This is mainly caused by the lack of trust in automated vehicles, which are usually considered to be untrustworthy by drivers [3]. Moreover, security concerns may affect the driver acceptance as they influence the PHYD trustworthiness [20, 31].

In this paper, we propose a deep-learning-based model to advance the adaptation of business incentives based on IoB by enforcing collaborating practices that leverage self-adaptive approaches from traditional operational levels to the tactical (system collaboration) and business levels (collaboration between businesses) based on the digital computation of *indirect trust* for gathering runtime evidence of behavioral reputation. This model contains a timely prediction of the computational control of collaborative behavior that accounts for reputation computation. The prediction enables a safe prompt reaction within a collaboration. With our approach, we pave the way towards safe collaborative adaptation that can be based on a contractual agreement between complex behaviors that are provided to an orchestration when joining a business collaboration. The self-adaptation mechanisms at the ecosystem level provide a mechanism for (a) assuring a safe driving behavior, and (b) improving and sustaining the health of an ecosystem based on the evidence of safe driving behavior [16]. This self-adaptation mechanism relies on an explicit distinction between handling domain concerns and handling adaptation concerns. Also, it involves real-time feedback designed along with uplifted safety goals and behavioral adaptation based on measurements of indirect trust.

The rest of this paper is organized as follows. Section 2 introduces the background on trust management and usage-based insurance. Section 3 reviews the related work on self-configuration and machine learning for driver behavior profiling. The self-adaptation mechanism using deep learning for indirect trust management is proposed in Section 4. The experimental setup and results are discussed in Section 5. Conclusions and future work are presented in Section 6.

2 BACKGROUND

This section discusses the essential concepts of trust management and the application scenario chosen for this paper.

2.1 Trust Management

Trust Management is centered around the concept of "trust", which is still hard to define due to various meanings across domains. We adopt definition that focuses on interpreting trust from a digitalization perspective, as: "*Trust, a social psychological concept, seems particularly important for understanding human-automation partnerships. Trust can be defined as the attitude that an agent will help achieve an individual's goals in a situation characterized by uncertainty and vulnerability*" [26].

As depicted in Figure 1, a trust management model [21, 36] is a collection of trust-related evidence acquired from different sources

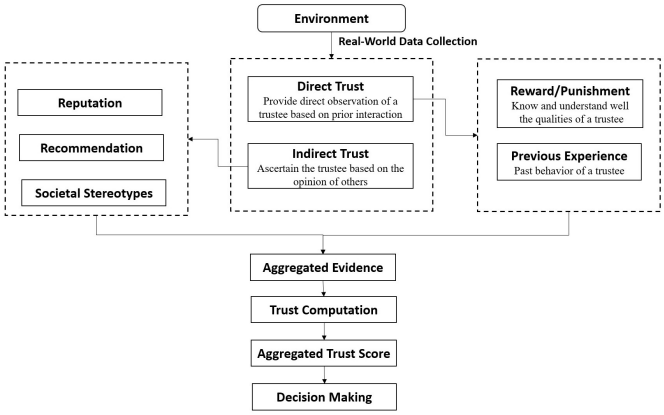

Figure 1: Basic Trust Computation Model

and used to obtain sufficient information about the trustworthiness of a collaborating entity (the trustee). When the collected data are mainly individual feedback given by a trustor who had direct interactions with the trustee in the past, then *direct trust* is formed. In case there are no previous direct interaction experiences, or the existing evidence is insufficient to understand the qualities of the trustee directly, feedback can be given by different peer networks of the trustor. This contributes to a *general belief* propagated to extend pre-existing trustworthiness relation with the trustee, which is called *indirect trust*. The quantification of indirect trust can be based on the evidence reputation that concertizes aggregated data used as an input to compute the trust values of the trustees.

2.2 Application Scenario

The concept we introduce in this paper has its applicability within the context of the Internet of Vehicle (IoV) [4, 34], which is a technological evolution in transportation that facilitates data gathering, sharing, and processing among vehicles, people, and road services. The communication within IoV, e.g. Vehicle-to-Vehicle and Vehicle-to-Roadside, has attracted multiple industrial sectors (such as UBI companies [22]) to gather the knowledge for advancing services-based innovative solutions in transportation.

UBI is a type of vehicle insurance that has benefited from IoV data collection to determine and customize insurance policy premiums dynamically while avoiding traditional insurance problems. Some of these problems are the lack of flexibility and transparency in assessing the risk associated with the monitored driving behavior. As described in Figure 2, UBI uses equipped vehicles with On-Board Units to collect and process data for specific insurance purposes [2, 22]. The first purpose is to calculate dynamically the insurance premium cost based on analyzing driving data in order to estimate the driver's risk exposure, which is known as Pay-As-You-Drive (PAYD) [6]. The second purpose is to monitor driving behavior and decide whether the driver deserves an insurance premium discount or not. This is known as Pay-How-You-Drive [10]. In other words, the idea of PHYD is to build a risk profile for the driver by using IoV data to extract, analyze, and understand driving behavior. As a result, PHYD motivates reckless drivers to adjust their driving behavior if they intend to receive a discount on insurance premiums.

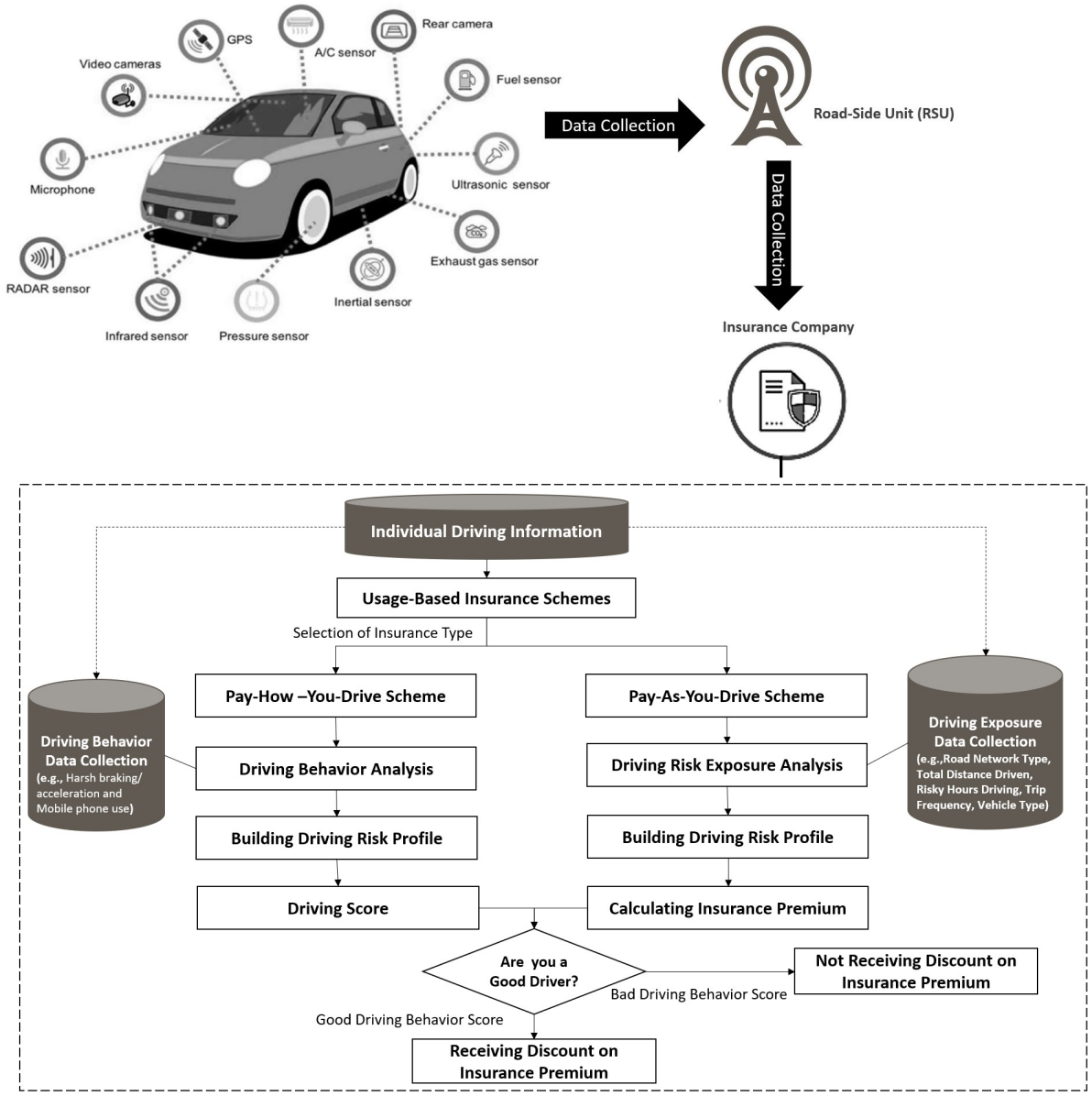

Figure 2: Pay-As-You-Drive and Pay-How-you-Drive schemes

Thus, PHYD contributes to improving road safety as it is aligned with reducing traffic risk and increasing the awareness of drivers about their driving habits [1]. Given the importance of PHYD, we use PHYD as an application scenario in this paper.

3 RELATED WORK

The related work to our approach can be found at the intersection between self-adaptation mechanisms, engineering digital ecosystems and the use of machine learning, in particular the deep learning approaches with applicability in the domain of driving behavior analysis.

3.1 Self-Reconfiguration for Digital Ecosystems

The emerging development of trust-based digital ecosystems [11] accounts for the management of complex tasks between humans and interacting systems. Consequently, a system's tactical reconfiguration needs to account for human behaviors within its self-adaptation mechanism [13].

In this context, automatic mitigation of runtime uncertainties caused by a dynamic changing environment needs to account of novel mechanisms engineered to support the self-adaptation of complex digital ecosystems. In this paper, we consider self-adaptation

to be the property of an ecosystem that emerges around IoT and it is influenced by unexpected events that can potentially endanger human societies. To assuring the self-adaptation property of digital ecosystems, we propose a novel solution where we envision a three-layer feedback loop that supports self-reconfiguration at two out of three levels of concerns: business and tactics, leaving apart the system self-reconfiguration, which is system-specific. For the derivation of the self-adaptation mechanism at the ecosystem level, we extend the interpretation of self-adaptation toward enabling dynamic reactions to runtime changes in the external or internal environment of IoB.

Within IoB in the automotive domain, profiling the driving behavior centers on the collected telematics information (e.g., GPS location) that is considered trusted evidence used to assess driver's safety levels. However, there are some trust concerns that require further use of trust management. For instance, an attacker may perform a masquerade attack [20, 31] to impersonate another driver, violating the driving behavior privacy of the victim by collecting their kinematic driving data. Next, the attacker uses the victim's behavioral data to modify their driving behavior before sending fake behavioral data to the insurance service. Usurpation of the identity of a vehicle leads to perceived security, privacy, and trust concerns that appear to slow the adoption of PHYD car insurance. Trust management can tackle the above issues and help insurance companies achieve their primary purpose, which is: ameliorating the driver's behavior, increasing traffic safety, and saving energy consumption.

3.2 Machine Learning for Driving Behavior

Different Machine-Learning-based PHYD models have been used to analyze driving behavior data. For instance, in [5], a behavior-centric vehicle insurance model has been proposed to personalize vehicle premium calculation by using a Bagging-based classification and calculating the actual driver's risk level using features from its recorded behavior data. Similarly, a PHYD approach has been proposed in [7] to compute the driver aggressiveness through cluster analysis. In [17], the authors have conducted a survey to identify the characteristics of the drivers who would accept this pricing model. They have proposed a new PHYD pricing scheme based on providing recommendations to drivers who are willing to accept the adoption of ecological driving behavior. To model the acceptance of the proposed PHYD scheme, the following four Machine Learning models have been used: Random Forests, Gradient Boosting, Support Vector Machines and Ensemble Learning. They found that travel time, monetary gains, and discounts are the main factors in accepting the proposed pricing model.

3.3 Deep Learning for Driving Behavior

Due to the imperative assessment of the driving behavior for PHYD, deep learning approaches have been used to build driving behavior profiling by commensurating drivers' competence based on their driving behaviors. For example, Convolution Neural Network (CNN) has been applied in [15] to classify driving data into aggressive, mild, and gentle. Likewise, 2D-CNN has been used in [29] to analyze driving behavior by classifying it into normal, aggressive, distracted, drowsy, and drunk driving. The driver's aggressiveness has been assessed by exploiting Recurrent Neural Networks (RNN) and data collected by smartphone accelerometers. Similarly, in [9], RNN has been employed under an unsupervised learning paradigm to examine the time-series pattern of driving data and then distinguish aggressive driver behaviors from normal behaviors, which leads to achieving an effective driver behavior profiling performance. Equivalently, a novel learning approach based on Soft Thresholding and Temporal Convolutional Network has been proposed in [38] to recognize abnormal driving behavior and assess driver safety levels effectively.

Even though, various mechanisms exist for achieving particular goals of self-adaptation for different actors of the ecosystem (humans, systems, system-of-systems, system components, etc.), a higher mechanism that combines the benefits of all is still missing.

By combining the concepts from the above-mentioned technological development, we propose a novel self-adaptation mechanism conceptualized as a combination of the traditional change-management component that performs the changing of the operational conditions, and the management component for addressing changes in goals at runtime.

4 SELF-ADAPTATION MODEL

This section proposes an adaptation mechanism implemented at the ecosystem level that accounts for the goal-oriented adaptation models of interacting participants within a feedback loop. This model adapts the collaborating systems based on feedback from a reputation voter that compares the derived reputation score against a predictive behavior. As depicted in Figure 3, the reputation voter instantiates the computation of indirect trust in our mechanism. Traditionally, the feedback loop relies on environmental sensing for adapting managed systems to a local configuration that satisfies the adaptation goals. By incorporating a runtime prediction mechanism like the one presented in [12], the feedback loop can actively respond to a violation of the adaptation goals, and by tracking the behavior of the managed collaborating systems can adapt its own behavior in response to the anticipation of possible violations. The predictive simulation builds on the proactive policy of the ecosystem self-adaptation feedback loop. If no internal configuration can be matched to the fulfillment of the adaptation, then the ecosystem orchestrator can trigger the self-adaptation mode through a set of guidelines.

Within the context of PHYD, the role of deep learning is first to classify the driver's behavior into safe and unsafe (aggressive) by collecting driving data (e.g., acceleration, steering, braking, and location). After that, PHYD may charge premium insurance based on the classified individual driving behavior, rewarding drivers for driving safely to provide positive incentives.

The second role of deep learning is to enhance indirect trust management that aims to check the trustworthiness and safety of the awarded drivers. As a result, indirect trust management using deep learning supports PHYD's primary goal of improving road safety. To do so, indirect trust is calculated using driver behavior data. Synthetic data can be created to train the models because it is difficult to collect realistic data in a short amount of time. Figure 3 illustrates a generative adversarial network (GAN) [14] that is trained to generate synthetic data. The basic idea of GAN consists

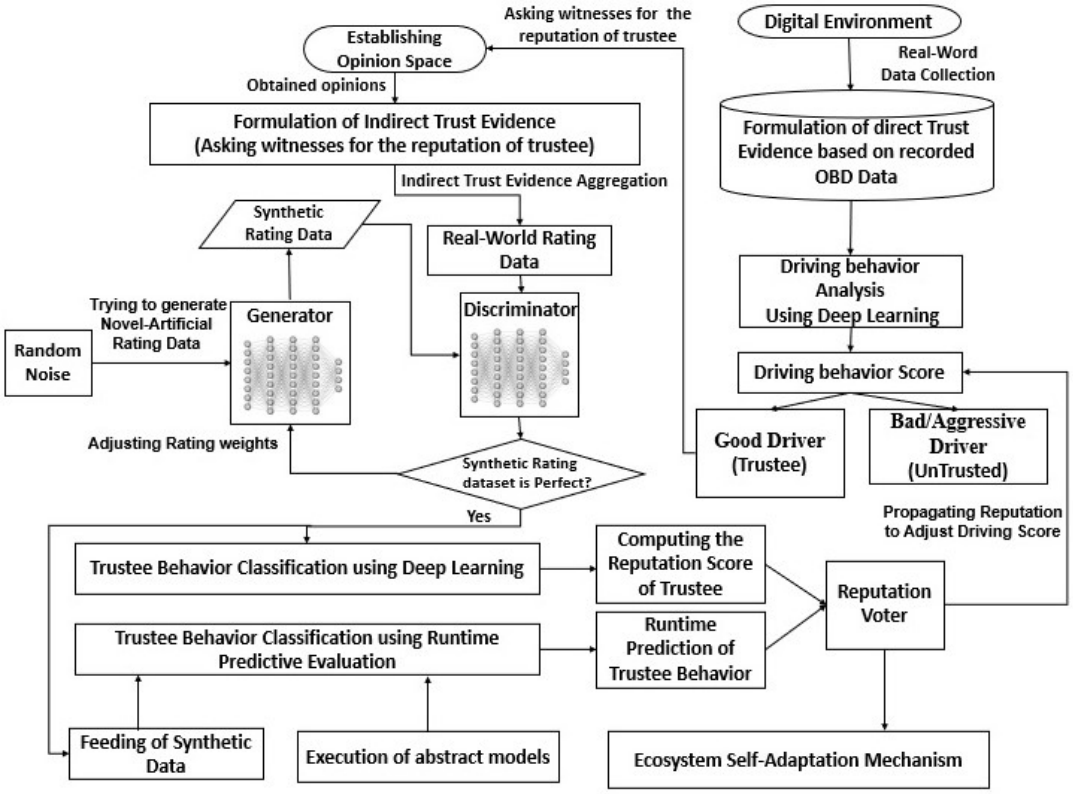

Figure 3: Self-Adaptation Model for Trust Management

of using two separate neural networks. The first is a generator that uses random noise extracted from trained real-world data to generate synthetic data similar to real ones. After that, a second deep neural network, named discriminator, is performed to compare the similarity of the produced synthetic data with real data. The discriminator stops classifying the real input samples from the generated ones when fake and real data are indistinguishable.

5 EXPERIMENT

Automated transportation systems encompass several modern digital technologies with social skills, such as Unmanned Aerial Vehicles (UAVs), which can interact and communicate without human intervention [35, 37]. For instance, within the indirect trust context, multiple UAVs can be used to track vehicles to collect information that can be exploited to analyze driving behavior and then calculate their reputation ratings [30]. Despite the different uses of UAVs (e.g., road safety monitoring), the social acceptance issues discourage the adoption of automated UAVs, such as people becoming suspicious about their privacy being compromised and their safety when they are near UAVs [25]. Likewise, the absence of clear published ethical codes discourages the adoption of autonomous UAVs for monitoring driver behavior [8]. Due to the above issues, this section uses a public driving behavior dataset to study driver behavior in the indirect trust context.

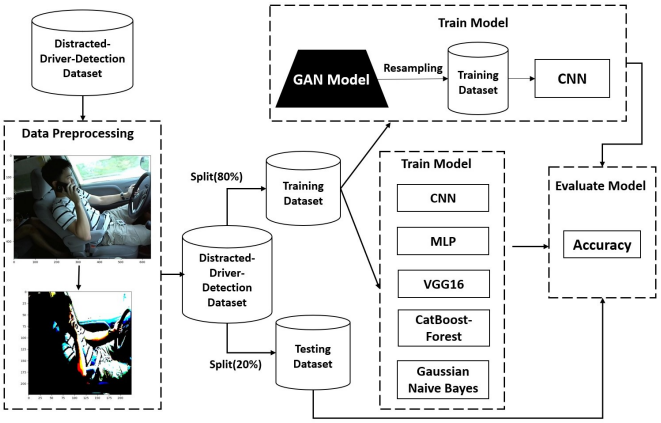

Figure 4: Experiment Workflow Structure

5.1 Experimental Setting

Figure 4 illustrates the experiment workflow structure, where the classification performance of CNN, Multi-layer Perceptron Neural Network (MLP), VGG16[32], CatBoost-Forest [28], and Gaussian Naive Bayes are evaluated in terms of accuracy. Likewise, the classification accuracy of CNN and GAN-CNN are compared after using GAN for augmenting data (Table 5.1). CNN and GAN-CNN are

trained for 200 epochs using a batch size of 64 and Adam as an optimizer. The experiment is performed on a personal computer with the following setting: Windows 10 operating system, AMD Ryzen 7 PRO 5850U with Radeon Graphics 1.90 GHz, 32 GB RAM, and 1 TB SSD Hard Drive.

Distraction is one of the driving behavior patterns [23] that be experienced by drivers anytime. Driver distraction has been described in [27] as: "diversion of attention away from activities critical for safe driving toward a competing activity". In other words, driver distraction is irrelevant to normal driving. For example, distractions can be making and receiving calls, searching for information on their mobile phones, or communicating with passengers.

[h!]

Classes	Driving States	
c0	safe driving	2489
c1	texting – right	2267
c2	talking on the phone – right	2317
c3	texting – left	2346
c4	talking on the phone – left	2326
c5	operating the radio	2312
c6	drinking	2325
c7	reaching behind	2002
c8	hair and makeup	1911
c9	talking to passenger	2129
Total		22424
Training Data		17940
Validation data		4484
Resampled Training data using GAN		19940

We have selected a driver distraction detection dataset from the Kaggle online data science platform[1]. The selected dataset is divided into 10 classes illustrated in Table 5.1. Figure 4 shows an example of a distracted driver who uses a phone while driving and belongs to the class of talking on the phone – right (C2). For image preprocessing as depicted in Figure 4, all original images have been subtracted by the mean value of RGB [18] over all pixels in order to center data around driver behaviors. The dataset has a total of 22,424 images (640 × 480 pixels). We have randomly split the dataset into 80% for a training dataset and 20% for a test dataset.

5.2 Experimental Results

The experimental results in Table 1 show the classification accuracy based on 6 classifiers, which are Gaussian Naive Bayes, CatBoost-Forest, MLP, VGG16, CNN and GAN-CNN. It can be seen that GAN-CNN outperforms other algorithms, as GAN-CNN reaches 96.23% accuracy compared to CatBoost-Forest (90.45%), VGG16 (90.02%), MLP(82%), and Gaussian Naive Bayes (55.48%). It is worth noting that without synthetic data, CatBoost-Forest and VGG16 also archived a good level of classification accuracy. The rest of the algorithms did not perform well in the experiment.

As illustrated in Tables 2 and 3, we can observe that GAN can produce synthetic data that can help improve the performance of CNN, where training loss is reduced while the training accuracy starts converging after 100 epochs.

Moreover, the confusion matrix results in Tables 4 and 5 reflect perfectly the advantage of using GAN to resample training data

[1]https://www.kaggle.com/competitions/state-farm-distracted-driver-detection/data

Table 1: Classifier Comparison Using Accuracy

Classifier	Accuracy (%)
Gaussian Naive Bayes	55.48
CatBoost-Forest [28]	90.45
MLP	82
VGG16 [32]	90.02
CNN	79.50
GAN-CNN	96.23

Table 2: Epochs of GAN-CNN

	GAN-CNN			
Epoch	Training loss	Training accuracy	Validation loss	Validation accuracy
1	2.1866	0.1815	1.8784	0.3321
2	1.6302	0.4210	1.5959	0.4737
3	1.2208	0.5763	1.1775	0.6044
4	0.9580	0.6759	0.9638	0.6907
5	0.7783	0.7399	0.8396	0.7368
10	0.4394	0.8564	0.5362	0.8457
100	0.0925	0.9686	0.1619	0.9558
Best epoch: 185	0.0639	0.9795	0.1266	0.9623

Table 3: Epochs of CNN

	CNN			
Epoch	Training loss	Training accuracy	Validation loss	Validation accuracy
1	2.2244	0.1706	1.9768	0.2739
2	1.6889	0.3950	1.3268	0.5216
3	1.3084	0.5344	1.0781	0.6073
4	1.0840	0.6224	1.0059	0.6481
5	0.9054	0.6858	0.9359	0.6971
10	0.7966	0.7292	0.8259	0.7426
100	0.5357	0.8218	0.6283	0.7975
Best epoch: 120	0.3295	0.8934	0.6941	0.7950

while dealing with the class imbalance problem that usually deteriorates the classification performance of learner models. Thus, the accuracy results of CNN and GAN-CNN attain respectively 79.50 % and 96.23%.

By comparing with CNN, GAN can be considered as an intensifier for CNN to increase the accuracy. More recently, GAN has emerged as an up-to-date deep learning method that are applied in several domains, for example using GAN to augment an urban traffic image dataset and improve the quality of generated images [19]. However, finding a suitable number of synthetic data needed to balance class data, particularly minority class, is still a challenge since GAN's basic idea is to sample original random data [14]. Thus, we intend

to extend and apply GAN in trust management by learning how to augment real trust data and allow deep learning to be trained more effectively.

Table 4: Confusion matrix of validation data (4484) obtained using CNN

	CNN									
	Predicted Class									
Truth	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
C1	337	39	26	10	0	2	0	0	3	38
C2	0	458	8	0	0	0	0	0	1	0
C3	0	16	432	0	0	0	0	0	2	0
C4	5	65	3	375	5	0	0	0	1	2
C5	20	21	52	9	342	5	9	1	4	1
C6	2	5	4	7	1	425	0	0	3	2
C7	0	31	109	0	1	0	316	0	12	0
C8	1	11	11	0	0	0	0	399	0	3
C9	1	20	103	4	10	0	25	40	170	19
C10	51	41	12	5	10	0	2	6	19	311

As shown in Table 5, the results reflect that GAN can improve the classification accuracy effectively due to its ability to replicate the original data, which helps improve the CNN classification performance compared to other classifiers. Only a few data are misclassified in the experiment. However, it is still important that GAN-CNN can be further tested and validated with various datasets. Also, in certain real-time situations, the prediction accuracy of GAN-CNN might be decreased as the synthetic dataset is always originated from the initial dataset.

Table 5: Confusion matrix of validation data (4484) obtained using GAN-CNN

	GAN-CNN									
	Predicted Class									
Truth	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
C1	429	4	0	4	1	0	1	0	7	9
C2	0	458	0	0	0	1	6	0	2	0
C3	0	3	406	0	4	0	20	1	16	0
C4	2	2	0	449	0	0	0	0	2	1
C5	2	3	0	0	454	3	0	0	2	0
C6	2	0	0	1	0	442	1	0	2	1
C7	1	1	0	1	0	1	455	1	9	0
C8	0	0	0	0	1	0	0	416	7	1
C9	0	0	0	0	4	0	3	0	383	2
C10	7	1	0	1	0	0	0	10	15	423

5.3 Discussion

Trust is the foundation of digital ecosystems. In a variety of circumstances, a system's reputation must be calculated within an ecosystem using an evaluation of the service's functional and non-functional characteristics. These situations are typically captured using verification scenarios. The verification scenario, on the other hand, must be able to accurately reflect the technical situation that occurs in specific circumstances when a decision to enter an ecosystem is to be made during runtime. This, in our opinion, can be accomplished by constructing models of systems and their interconnected components, as well as actors within digital ecosystems. Then, during runtime, simulated systems and system components are fed with real-time information to reflect a specific technical situation.

The runtime evidence of trust can then be gathered directly from the field and fed into a dynamic procedure of trust management that can implement an adaptation mechanism at the ecosystem level. The goal-oriented adaptation models of interacting participants can then be explained by this adaptation mechanism. Tactic reconfigurations are usually carried out based on evidence obtained at the operation level. When self-adaptation must account for external system factors like image recognition, the interplay of machine learning algorithms becomes critical. Deep learning is used in the use case we're presenting to classify drivers as aggressive or non-aggressive. PHYD charges insurance premiums based on classified individual driving behavior. Afterward, indirect trust is calculated by collecting all driver behavior data and classifying actual (un)safe drivers using sanctions or rewards, as well as performing a business reconfiguration that is equivalent to a digital ecosystem's strategic reconfiguration.

Together with the emergence of autonomous driving behavior, multiple assumptions regarding the achievement of overall safe driving behavior are made. While some practitioners claim that automated driving behavior is likely to bring more safety to the roads, assurance companies are starting to devise schemes with cost reductions for automated driving behavior. In this context, PHYD concept brings such schemes closer to practice. However, what is missing yet is the statistical data that would compare the safety of the two types of driving: human driving and automated driving. For paving the way towards such comparison, in this paper, we have presented a concept that enables automotive ecosystem self-adaptation based on analyzed human driving behavior. Future work can leverage the same concept by iterating over data provided by autonomous vehicles that employ automated driving behavior.

6 CONCLUSION

In this paper, we have proposed a self-adaptation model for trust management based on deep learning in the context of the Internet of Behavior. This model first identifies the safe and unsafe drivers. Among the safe drivers, it further classified the driver behaviors with deep learning. In order to validate the behavior classification, we have compared the GAN-CNN used in the proposed model with a set of up-to-date algorithms such as CatBoost-Forest, VGG16 and MLP. The experimental results have shown that GAN-CNN outperforms other algorithms in terms of accuracy. Thus in the demonstrated Pay-How-You-Drive scenario, our model can identify the driving behavior in real-time and accordingly suggest adaption operations. On the other hand, the experimental results have indicated that our proposed model can reduce the driving risks, strengthen the trust management for the insurance company and assure the trust between automated systems and drivers.

In future work, we plan to further validate the model by collaborating with an insurance company. As data privacy plays an important role in testing the self-adaptation model, we also plan to improve the model by adding the privacy-preserving component, which could further contribute to trust management.

ACKNOWLEDGEMENTS

The work was supported from ERDF/ESF "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01/0.0/0.0/16_019/0000822) and by the European Union's Horizon 2020 research and innovation programe under grant agreement No 952702 (BIECO).

REFERENCES

[1] Yasir Ali, Anshuman Sharma, Md Mazharul Haque, Zuduo Zheng, and Mohammad Saifuzzaman. 2020. The impact of the connected environment on driving behavior and safety: A driving simulator study. *Accident Analysis & Prevention* 144 (2020), 105643.

[2] Subramanian Arumugam and R Bhargavi. 2019. A survey on driving behavior analysis in usage based insurance using big data. *Journal of Big Data* 6, 1 (2019), 1–21.

[3] Subho S Banerjee, Saurabh Jha, James Cyriac, Zbigniew T Kalbarczyk, and Ravishankar K Iyer. 2018. Hands off the wheel in autonomous vehicles?: A systems perspective on over a million miles of field data. In *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. IEEE, 586–597.

[4] Elhadja Benalia, Salim Bitam, and Abdelhamid Mellouk. 2020. Data dissemination for Internet of vehicle based on 5G communications: A survey. *Transactions on Emerging Telecommunications Technologies* 31, 5 (2020), e3881.

[5] Yiyang Bian, Chen Yang, J Leon Zhao, and Liang Liang. 2018. Good drivers pay less: A study of usage-based vehicle insurance models. *Transportation research part A: policy and practice* 107 (2018), 20–34.

[6] Jason Bordoff and Pascal Noel. 2010. Pay-as-you-drive auto insurance. *Issues of the Day: 100 Commentaries on Climate, Energy, the Environment, Transportation, and Public Health Policy* 150 (2010).

[7] Maria Francesca Carfora, Fabio Martinelli, Francesco Mercaldo, Vittoria Nardone, Albina Orlando, Antonella Santone, and Gigliola Vaglini. 2019. A "pay-how-you-drive" car insurance approach through cluster analysis. *Soft Computing* 23, 9 (2019), 2863–2875.

[8] Dylan Cawthorne and Arne Devos. 2020. Capability caution in UAV design. In *2020 International Conference on Unmanned Aircraft Systems (ICUAS)*. IEEE, 1572–1581.

[9] Young Ah Choi, Kyung Ho Park, Eunji Park, and Huy Kang Kim. 2021. Unsupervised Driver Behavior Profiling Leveraging Recurrent Neural Networks. In *International Conference on Information Security Applications*. Springer, 28–38.

[10] Kyriaki Christovasili, Eleni Mantouka, and Eleni Vlahogianni. 2020. A User Acceptance Survey of Pay-How-You-Drive Urban Pricing Schemes. In *Conference on Sustainable Urban Mobility*. Springer, 584–594.

[11] Emilia Cioroaica, Stanislav Chren, Barbora Buhnova, Thomas Kuhn, and Dimitar Dimitrov. 2020. Reference architecture for trust-based digital ecosystems. In *2020 IEEE International Conference on Software Architecture Companion (ICSA-C)*. IEEE, 266–273.

[12] Emilia Cioroaica, Thomas Kuhn, and Barbora Buhnova. 2019. (Do not) trust in ecosystems. In *2019 IEEE/ACM 41st International Conference on Software Engineering: New Ideas and Emerging Results (ICSE-NIER)*. IEEE, 9–12.

[13] Emilia Cioroaica, Akanksha Purohit, Barbora Buhnova, and Daniel Schneider. 2021. Goals within trust-based digital ecosystems. In *2021 IEEE/ACM Joint 9th International Workshop on Software Engineering for Systems-of-Systems and 15th Workshop on Distributed Software Development, Software Ecosystems and Systems-of-Systems (SESoS/WDES)*. IEEE, 1–7.

[14] Antonia Creswell, Tom White, Vincent Dumoulin, Kai Arulkumaran, Biswa Sengupta, and Anil A Bharath. 2018. Generative adversarial networks: An overview. *IEEE signal processing magazine* 35, 1 (2018), 53–65.

[15] Aslıhan Cura, Haluk Küçük, Erdem Ergen, and İsmail Burak Öksüzoğlu. 2020. Driver profiling using long short term memory (LSTM) and convolutional neural network (CNN) methods. *IEEE Transactions on Intelligent Transportation Systems* 22, 10 (2020), 6572–6582.

[16] Simone da Silva Amorim, Félix Simas S Neto, John D McGregor, Eduardo Santana de Almeida, and Christina von Flach G. Chavez. 2017. How has the health of software ecosystems been evaluated? A systematic review. In *Proceedings of the 31st Brazilian symposium on software engineering*. 14–23.

[17] Panagiotis Fafoutellis, Eleni G Mantouka, and Eleni I Vlahogianni. 2022. Acceptance of a Pay-How-You-Drive pricing scheme for city traffic: The case of Athens. *Transportation Research Part A: Policy and Practice* 156 (2022), 270–284.

[18] Vishesh Goel, Sahil Singhal, Tarun Jain, and Silica Kole. 2017. Specific color detection in images using RGB modelling in MATLAB. *International Journal of Computer Applications* 161, 8 (2017), 38–42.

[19] Xi Guo, Zhicheng Wang, Qin Yang, Weifeng Lv, Xianglong Liu, Qiong Wu, and Jian Huang. 2020. Gan-based virtual-to-real image translation for urban scene semantic segmentation. *Neurocomputing* 394 (2020), 127–135.

[20] Hamssa Hasrouny, Abed Ellatif Samhat, Carole Bassil, and Anis Laouiti. 2017. VANet security challenges and solutions: A survey. *Vehicular Communications* 7 (2017), 7–20.

[21] Amal Hbaieb, Samiha Ayed, and Lamia Chaari. 2022. A survey of trust management in the Internet of Vehicles. *Computer Networks* 203 (2022), 108558.

[22] Roel Henckaerts and Katrien Antonio. 2022. The added value of dynamically updating motor insurance prices with telematics collected driving behavior data. *Insurance: Mathematics and Economics* 105 (2022), 79–95.

[23] Md Mahmud Hossain, Xiaoduan Sun, Elisabeta Mitran, and M Ashifur Rahman. 2021. Investigating fatal and injury crash patterns of teen drivers with unsupervised learning algorithms. *IATSS Research* 45, 4 (2021), 561–573.

[24] Mohd Javaid, Abid Haleem, Ravi Pratap Singh, Shanay Rab, and Rajiv Suman. 2021. Internet of Behaviours (IoB) and its role in customer services. *Sensors International* 2 (2021), 100122.

[25] Idris Jeelani and Masoud Gheisari. 2021. Safety challenges of UAV integration in construction: Conceptual analysis and future research roadmap. *Safety science* 144 (2021), 105473.

[26] John D Lee and Katrina A See. 2004. Trust in automation: Designing for appropriate reliance. *Human factors* 46, 1 (2004), 50–80.

[27] Michael A Regan and Eve Mitsopoulos. 2001. *Understanding passenger influences on driver behaviour: Implications for road safety and recommendations for countermeasure development.* Number 180.

[28] Alim Samat, Erzhu Li, Peijun Du, Sicong Liu, and Junshi Xia. 2021. GPU-accelerated catboost-forest for hyperspectral image classification via parallelized mRMR ensemble subspace feature selection. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing* 14 (2021), 3200–3214.

[29] Mohammad Shahverdy, Mahmood Fathy, Reza Berangi, and Mohammad Sabokrou. 2020. Driver behavior detection and classification using deep convolutional neural networks. *Expert Systems with Applications* 149 (2020), 113240.

[30] Vishal Sharma, Hsing-Chung Chen, and Rajesh Kumar. 2017. Driver behaviour detection and vehicle rating using multi-UAV coordinated vehicular networks. *J. Comput. System Sci.* 86 (2017), 3–32.

[31] Shubha R Shetty and DH Manjaiah. 2022. A Comprehensive Study of Security Attack on VANET. In *Data Management, Analytics and Innovation*. Springer, 407–428.

[32] Karen Simonyan and Andrew Zisserman. 2014. Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556* (2014).

[33] Christian Stary. 2020. The Internet-of-Behavior as organizational transformation space with choreographic intelligence. In *International Conference on Subject-Oriented Business Process Management*. Springer, 113–132.

[34] Carlos Renato Storck and Fátima Duarte-Figueiredo. 2020. A survey of 5G technology evolution, standards, and infrastructure associated with vehicle-to-everything communications by internet of vehicles. *IEEE access* 8 (2020), 117593–117614.

[35] Chaogang Tang, Xianglin Wei, Chong Liu, Haifeng Jiang, Huaming Wu, and Qing Li. 2020. Uav-enabled social internet of vehicles: Roles, security issues and use cases. In *International Symposium on Security and Privacy in Social Networks and Big Data*. Springer, 153–163.

[36] Hannah Lim Jing Ting, Xin Kang, Tieyan Li, Haiguang Wang, and Cheng-Kang Chu. 2021. On the trust and trust modeling for the future fully-connected digital world: A comprehensive study. *IEEE Access* 9 (2021), 106743–106783.

[37] Zhen Xue, Jinlong Wang, Guoru Ding, Qihui Wu, Yun Lin, and Theodoros A Tsiftsis. 2018. Device-to-device communications underlying UAV-supported social networking. *IEEE Access* 6 (2018), 34488–34502.

[38] Yunyun Zhao, Hongwei Jia, Haiyong Luo, Fang Zhao, Yanjun Qin, and Yueyue Wang. 2022. An abnormal driving behavior recognition algorithm based on the temporal convolutional network and soft thresholding. *International Journal of Intelligent Systems* (2022).