Differential Privacy-based Avatar Update in Cooperative Intelligent Transportation System Metaverse

1st Salabat Khan
School of Computer and Information Engineering,
Qilu Institute of Technology,
Jinan, China
salabatwazir@gmail.com

2nd Fei Luo
School of Computing and Information Technology,
Great Bay University,
Dongguan, China.
luofei2018@outlook.com

3nd Mansoor Khan
School of Intelligent Manufacturing and Control Engineering
Qilu Institute of Technology
Jinan, China.
mansoorkhan@qlit.edu.cn

4th Insaf Ullah
Institute for Analytics and Data Science,
University of Essex,
Colchester, CO4 3SQ, UK
Insaf.ullah@essex.ac.uk

5rd Farhan Amin
School of Computer Science and Engineering
Yeungnam University,
South Korea
farhanamin10@hotmail.com

6th Shamsher Ullah
National Engineering Laboratory for Big Data,
Shenzhen University,
Shenzhen, China
shamsher@mail.ustc.edu.cn

7th Mussadiq Abdul Rahim
King Fahd University of Petroleum and Minerals (KFUPM),
Dhahran 31261, Saudi Arabia
mussadiq.ar@gmail.com

***Abstract*—Metaverse is the next generation and the successor to the Internet. Various sectors allocated capital to adapt the metaverse due to its inherent importance. Cooperative Intelligent Transportation Systems (C-ITS) is one of the important sectors that can benefit from metaverse adaptation and integration. The C-ITS and metaverse integration give rise to new use cases and cyber attacks. However, traditional Pseudonym Certificate (PCert) authentication based on Vehicular Public Key Infrastructure (VPKI) cannot meet the new use cases and thwart cyber attacks. We present a Differential Privacy (DP)-based PCert and avatar update model to ensure the privacy of end-devices (e.g., vehicles) in the C-ITS metaverse. The proposed DP-based model adds noise to avatar attributes (e.g., color, behavior) to prevent avatar linkage during the PCert update process. Our method ensures that PCerts and avatars cannot be linked to end-devices and the previous PCerts and avatars. We simulate the DP-based method to investigate it in terms of privacy, latency, color distortion, and adversarial success rate, and the results show that DP-based is effective and practical for avatar updates.**

***Index Terms*—Privacy, Blockchain, Metaverse, Cooperative Intelligent Transportation Systems (C-ITS), Vehicular Public Key Infrastructure (VPKI)**

I. Introduction

Metaverse is a combination of the terms ”meta” and ”universe,” which can be defined as a ”digitally simulated environment that is connected to the physical environment” [1], [2]. It evolved from Neal Stephenson’s science-fiction book, Snow Crash [3], [4]. It was conveyed as a virtual space where users interacted with each other. Metaverse is envisioned as a successor to the current Internet, which can be released by integrating various technologies such as Virtual Reality (VR), Artificial Intelligence (AI), Augmented Reality (AR), and blockchain [5]. The Covid-19 pandemic shifted the working, entertainment, and social paradigm from the physical to the virtual domains, which soon positioned the Metaverse as a demanding requirement.

Different sectors plan to invest in the metaverse as they realize the importance of the metaverse [1]. Among them, the transportation industry (e.g., Cooperative Intelligent Transportation Systems (C-ITS)) is an important sector where metaverse can play a crucial role in enabling safe, cost-effective, and efficient training and testing of autonomous vehicle driving

[1]https://www.enterpriseappstoday.com/stats/metaverse-statistics.html

algorithms [6]. C-ITS metaverse can be defined as a "digitally simulated C-ITS system that replicates the physical C-ITS system". C-ITS relies on Vehicular Public Key Infrastructure (VPKI) for anonymous and secure communication among V2V, V2I, and V2P, collectively referred to as V2X [7]. VPKI relies on the Pseudonym Certificate (PCert) to ensure anonymous vehicle authentication. However, integration raises new security and privacy concerns due to new complex corner use cases [8].

Given how the integration of C-ITS and metaverse can improve the transportation system, it is important to examine PCert change and avatar update–the new use case that arises as a result of the fusion. In this use case, vehicles can select their corresponding avatars in the virtual world. Traditional PCert-based proposals [9]–[11] do not cover the new use case and do not have methods to ensure the privacy of avatars in the virtual world and their corresponding vehicles in the physical world. Very recently, work in [8] identified privacy attacks on migration of vehicles and their Digital Twins (DTs). Luo et al. [8] then proposed the dual update scheme for vehicles and DTs. Another work in [12] proposed a cross-metaverse-based dual PCert management scheme and utilized cross-chain technology for efficient and secure PCert management. This study examines PCert and related avatar update in the context of C-ITS. This study makes the following contributions.

- We identify a new use case and privacy attack on the PCert and avatar update in the C-ITS metaverse
- We propose a Differential Privacy (DP)-based avatar update method framework that ensures privacy of vehicles and related avatars.
- We simulate the DP-based avatar update model to examine its effectiveness in the C-ITS metaverse.

The remainder of the study is organized as follows. In Section II, we define the PCert and avatar update problem and discuss the proposed DP-based avatar update model in Section III. Section IV discusses the performance of the DP-based avatar update model before drawing the final conclusion. Table I lists the abbreviations and symbols used in this study.

TABLE I
ABBREVIATIONS AND SYMBOLS AND THEIR DEFINITION

No	Abbreviation	Definition
1	AV	Avatar
2	AV_C	Current AV
3	AV_N	New AV
4	DP	Differential Privacy
5	DT	Digital Twin
6	PCert	Pseudonym Certificate
7	$PCert_C$	Current PCert
8	$PCert_N$	New PCert
8	VPKI	Vehicular Public Key Infrastructure

II. PROBLEM DEFINITION

This section discusses the integration of C-ITS and metaverse and the new use case. Fig. 1 shows a typical C-ITS metaverse, where a vehicle has an avatar AV_C in C-ITS metaverse and a set of PCert $PCert_1, PCert_2, .., PCert_j$, where $PCert_C$ is the current PCert of the vehicle. As shown in Fig. 1, when a vehicle changes its $PCert_C$ to new PCert $PCert_N$ and maintains the same avatar AV_C, then it exposes the vehicle privacy attack, where an adversary can track the vehicle avatar and track down the vehicle. In this study, we are

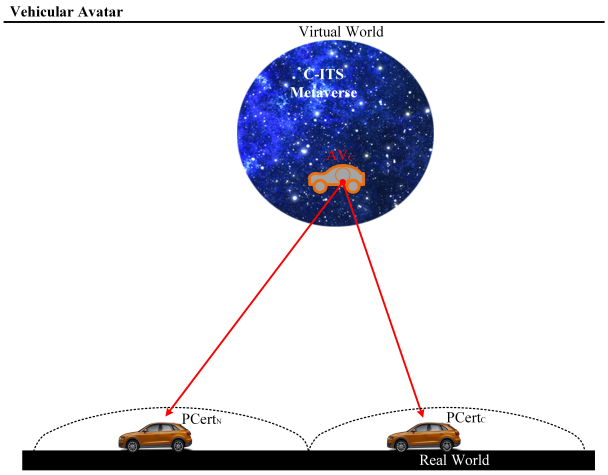

Fig. 1. PCert change and avatar probelm

addressing the avatar update problem with the PCert change problem by obscuring the PCert and avatar update process. This section introduces the DP-based PCert change and avatar update process.

III. PROPOSED DP-BASED AVATAR CHANGE MODEL

This section introduces the DP-based PCert change and avatar update process, which comprises the following components:

- Pseudonym Management System (PMS): It is responsible for managing Pseudonym Certificate (PCert) of devices (e.g., vehicles, commuter devices).
- Avatar Management System (AMS): Manages and handles avatars such as visual effects with pseudonym change.
- Differential Privacy Module (DPM): Introduces noise to avatar updates upon Pcert change to thwart tracking and linking of PCert change.
- Logger: Logs PCert and avatar updates.

As shown in Fig. 2 shows an overview of our proposed DP-based avatar update method triggered by PCert change. Fig. 2 shows how the avatar update process is completed, which is discussed in the next section.

A. Proposed model

This subsection presents a DP-based avatar update model that consists of the following steps.

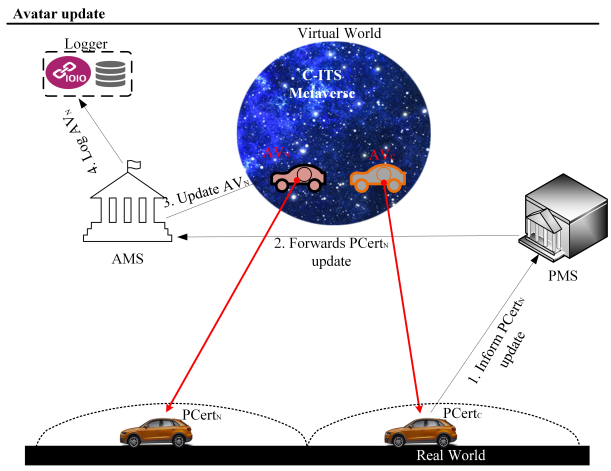

Fig. 2. Proposed DP-based Avatar Update Model

1) PCert and Avatar change: Vehicles need to change their Pcert to prevent tracking based on specific Pcert change criteria. Let $P = PCert_1, PCert_2, .., PCert_n$ be the set of PCerts assigned to a vehicle V_i, and $PCert_C$ be the current PCert before the change and $PCert_N$ be the new PCert after the change. Upon a PCert change, the PMS sends a notification to AMS that a $PCert_C$ change has occurred to $PCert_N$. Upon receiving the notification, AMS tracks the avatar associated with $PCert_C$.

2) Differential Privacy-Based (DP) Avatar Update: After PCert and avatar linkage, the DPM preparation changes to be applied to an avatar in three aspects: 1) appearance, 2) behavior, and 3) time. Let AV_N, and AT_N be the new avatar and its attribute and AV_C and AT_C be the current one; then each attribute AT_N is updated by adding noise as: $AT_N[i]$=$AT_C[i]$ + $Laplace(S/\epsilon)$ to ensure that AV_N is visually different from AV_C. Similarly, behavioral properties such as speed and movement patterns are randomized by adding noise through an exponential method such as $Pr(b) \propto \exp(2S\epsilon \cdot u(b))$, which selects the common properties of the avatar while ensuring unpredictable linkability to the old avatar and tracking of PCert changes. To further enhance privacy, noise is added to the time interval using the Laplacelac method to update PCert and avatar as T_{New} =T_{Change}+$Laplace(S/\epsilon)$, making the update time unpredictable.

3) Avatar Update in the Metaverse: After applying the DP process, AMS generates a new avatar AV_N corresponding to the new PCert AV_N. The new avatar AV_N is linked to the corresponding PCert and is registered in the metaverse. PCerts and their corresponding avatars are logged into a secure logging platform such as blockchain or distributed ledger technologies as in our previous work [10]. However, the DP procedure should be applied before logging in to prevent linkage between PCerts and avatars. We leave the DP-based secure logger method for our future work.Algorithm 1 shows the avatar update process in response to PCert change.

Algorithm 1 Avatar Update Process in C-ITS with Differential Privacy

Components:
PMS, AMS, DPM, Logger
Function `PCertUpdate(vehicleID,` $PCert_N$`)`
    $PCert_C \leftarrow PMS.getPCert_C(vehicleID)$
    $newPCert \leftarrow PCert_N$
    PMS.updatePCert(vehicleID, $newPCert$)
        AMS.notifyAVChange(vehicleID, $PCert_C$, $newPCert$)

Function `DPAVUpdate(vehicleID)`
    $AV_C \leftarrow$ AMS.getAV(vehicleID)
    currentAttributes $\leftarrow AV_C.attributes$
for each attribute in currentAttributes **do**
    newAttribute $\leftarrow$ attribute + LaplaceNoise(Sensitivity, ϵ)
    AV_N.setAttribute(newAttribute)
end for
newBehavior $\leftarrow$ AV_C.behavior + ExponentialNoise(Sensitivity, ϵ)
AV_N.setBehavior(newBehavior)
newTime $\leftarrow$ AV_C.time + LaplaceNoise(Sensitivity, ϵ)
AV_N.setTime(newTime)
AMS.updateAV(vehicleID, newAvatar)

Function `LogAVUpdate(vehicleID,` $PCert_N$`)`
    Logger.log(vehicleID, $newPCert$, AV_N)

Main Function `AVUpdateProcess(vehicleID,` $PCert_C$`)`
    `PCertUpdate(vehicleID,` $PCert_N$`)`
    `DPAVUpdate(vehicleID)`
    `LogAVUpdate(vehicleID,` $PCert_N$`)`

IV. Performance Analysis

This section investigates our DP-based avatar update model in terms of DP guarantee (ϵ), communication cost, and memory overheads. Python is used to simulate a DP-based model and compute the performance metrics. Table II gives values adapted during the simulations.

TABLE II
Simulation Parameters

No.	Parameter	Values
1	Vehicles	100
2	Simulation Steps	50
3.	ϵ	{0.1, 0.5, 1.0, 5.0}
4.	PCert Update Interval	5
5.	Adversial Threshold	0.8
6.	Color Range	(0, 255)

A. Linkability Score (LS)

LS shows the likelihood of avatar linkage and is inversely proportional to avatar similarity, which can be interpreted as $LS = 1 - AC$, where AC is avatar consistency. As the ϵ

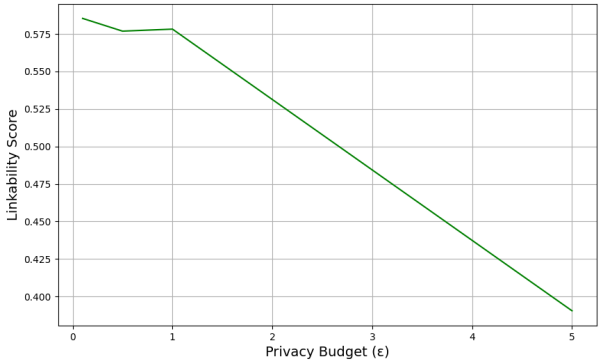

Fig. 3. Linkability Score vs Privacy Budget

values increase, the LS values decrease, which increases the likelyhood of linkage.

B. Adversial Sucess Rate (ASR)

It measures the success chances of an adversary to linkage AV_N with AV_C during PCert update. It increases with increase in ϵ values as high ϵ values result in higher avatar similarity. Fig. 4 plots the ASR against ϵ and shows that the ASR is

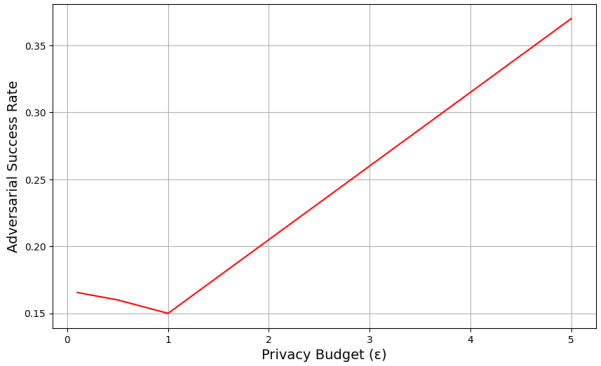

Fig. 4. Adversarial Success Rate vs Privacy Budget

lower when the value ϵ is set to close to 0.

C. Avatar Consistency (AC)

AC increases directly with ϵ as reduced noise ensures consistent avatars and a better user experience. However, it exposes avatars to privacy attacks, as adversaries have higher chances of linking them. Fig. 5 shows that AC increases with the value of ϵ.

D. Commulative Privacy Budget (CPB)

CPB refers to the budget spent on privacy after performing operations. It increases with each PCert update by ϵ color and ϵ accessory, which is computed as $\epsilon_{color} + \epsilon_{Accessory}$. Fig. 6 shows CPB consumption over steps, which helps to monitor CPB usage over the simulation. It can be induced from Fig. 6 that privacy loss increases with increase in CPB.

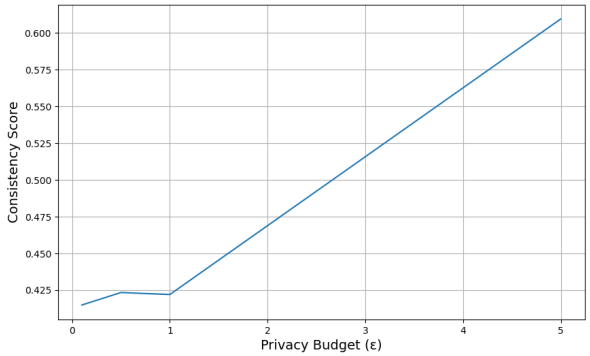

Fig. 5. Avatar Consistency vs Privacy Budget

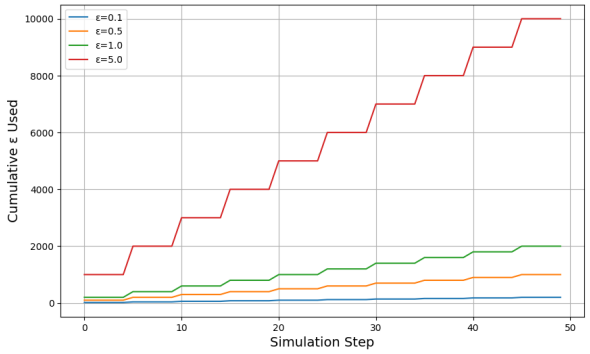

Fig. 6. Cumulative Privacy Budget Used Over Time

E. Color Distortion

It shows the change in the color of avatars with the PCert update. Fig. 7 depicts the distortion that shows the trade-off between privacy preservation and color used as a utility. Lower values of ϵ offer higher privacy but greater distortion, while higher values of ϵ offer weaker privacy but less distortion.

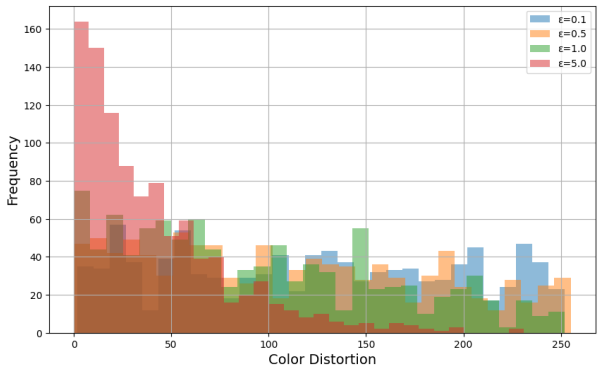

Fig. 7. Distribution of Color Distortions

F. Latency

Finally, we also compare computational overhead per avatar update, which is computed as.

$$\text{Computational Overhead} = \frac{\text{Total Processing Time}}{\text{Total Avatar Updates}}$$

TABLE III
PRIVACY AND DISTORTION METRICS AT DIFFERENT EPSILON VALUES

Epsilon	Total Privacy Budget Used	Average Color Distortion	Average Accessory Distortion	Average Avatar Similarity
0.1	200.00	125.90	0.68	0.42
0.5	1000.00	110.20	0.63	0.44
1.0	2000.00	90.10	0.59	0.45
5.0	10000.00	39.58	0.37	0.63

Similarly, latency for all avatar updates is computed as.

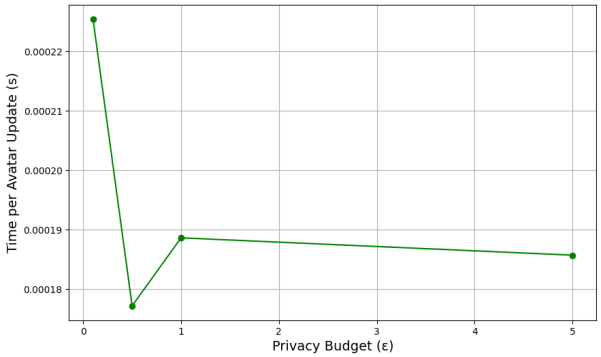

Fig. 8. Distribution of Color Distortions

$$\text{Total Latency} = \sum_{t=1}^{n} \text{Processing Time}_t$$

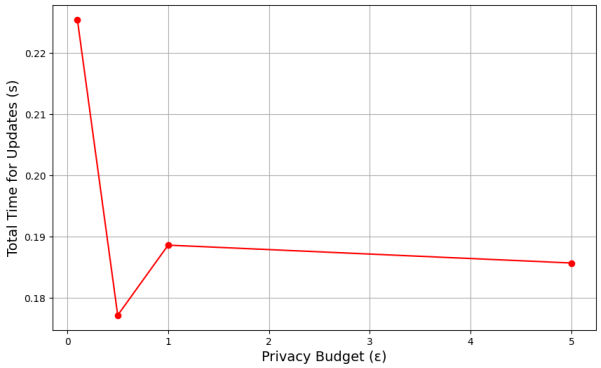

Fig. 9. Distribution of Color Distortions

Fig. 8 and Fig. 9 show the per avatar update and total latency. It can be deduced from Fig. 8 and Fig. 9 that latency remains relatively stable irrespective of ϵ

Table III shows the privacy budget, color and accessory distortion, and the similarity of avatars. It can be observed that on average the lowest ϵ obsfucate avatar, however, it introduces higher color and accessory distortion.

V. CONCLUSION

In this study, we investigated PCert-based authentication in the context of the C-ITS metaverse. We found that traditional PCert-based authentication falls short and can expose vehicles to privacy attacks when applied in combination with avatars in the C-ITS metaverse. We proposed a DP-based avatar update model to complement PCert-based authentication and to ensure privacy in the new use case. We evaluated our DP-based avatar update model in terms of various performance metrics such as latency and adversarial success rate. The results showed that the DP-based avatar update model is effective and practical. In the future, we plan to conduct real-world experiments to evaluate the feasibility of the DP-based model in the practice of C-ITS metaverse.

REFERENCES

[1] Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, T. H. Luan, and X. Shen, "A survey on metaverse: Fundamentals, security, and privacy," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 319–352, 2023.

[2] J. N. Njoku, C. I. Nwakanma, G. C. Amaizu, and D.-S. Kim, "Prospects and challenges of metaverse application in data-driven intelligent transportation systems," *IET Intelligent Transport Systems*, vol. 17, no. 1, pp. 1–21, 2023.

[3] N. Stephenson, *Snow crash*. Penguin UK, 1994.

[4] H. Duan, J. Li, S. Fan, Z. Lin, X. Wu, and W. Cai, "Metaverse for social good: A university campus prototype," in *Proceedings of the 29th ACM International Conference on Multimedia*, ser. MM '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 153–161. [Online]. Available: https://doi.org/10.1145/3474085.3479238

[5] M. Xu, W. C. Ng, W. Y. B. Lim, J. Kang, Z. Xiong, D. Niyato, Q. Yang, X. Shen, and C. Miao, "A full dive into realizing the edge-enabled metaverse: Visions, enabling technologies, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 656–700, 2023.

[6] D. S. Sarwatt, Y. Lin, J. Ding, Y. Sun, and H. Ning, "Metaverse for intelligent transportation systems (its): A comprehensive review of technologies, applications, implications, challenges and future directions," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 7, pp. 6290–6308, 2024.

[7] S. Khan, F. Luo, Z. Zhang, M. A. Rahim, M. Ahmad, and K. Wu, "Survey on issues and recent advances in vehicular public-key infrastructure (vpki)," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1574–1601, 2022.

[8] X. Luo, J. Wen, J. Kang, J. Nie, Z. Xiong, Y. Zhang, Z. Yang, and S. Xie, "Privacy attacks and defenses for digital twin migrations in vehicular metaverses," *IEEE Network*, vol. 37, no. 6, pp. 82–91, 2023.

[9] B. Brecht, D. Therriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn, and R. Goudy, "A security credential management system for v2x communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 12, pp. 3850–3871, 2018.

[10] S. Khan, L. Zhu, X. Yu, Z. Zhang, M. A. Rahim, M. Khan, X. Du, and M. Guizani, "Accountable credential management system for vehicular communication," *Vehicular Communications*, vol. 25, p. 100279, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214209620300504

[11] S. Khan, F. Luo, Z. Zhang, M. A. Rahim, S. Khan, S. F. Qadri, and K. Wu, "A privacy-preserving and transparent identity management scheme for vehicular social networking," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 11, pp. 11 555–11 570, 2022.

[12] J. Kang, X. Luo, J. Nie, T. Wu, H. Zhou, Y. Wang, D. Niyato, S. Mao, and S. Xie, "Blockchain-based pseudonym management for vehicle twin migrations in vehicular edge metaverse," *IEEE Internet of Things Journal*, pp. 1–1, 2024.