Proposing A Data Privacy Aware Protocol for Roadside Accident Video Reporting Service Using 5G In Vehicular Cloud Networks Environment

Zahrah A. Almusaylim[1], Noor Zaman[2] and Low Tang Jung[3]
[1,2] College of Computer Sciences and IT,
King Faisal University, Saudi Arabia.
[3] Computer & Information Sciences Department, Universiti Teknologi PETRONAS,
32610 Seri Iskandar, Perak Darul Ridzuan, Malaysia.
[1] zahra.almusaylim@hotmail.com, [2] nzman@kfu.edu.sa, [3] lowtanjung@utp.edu.my

***Abstract*—The bandwidth hungry applications are growing drastically and soon exceeding the bandwidth limits of existing wireless communication network systems. The current increasing demand for higher capacity and data rates are therefore leading to the 5G technology thus changing the norm of communications in providing the high-speed data rate and lower latency. One of the promising technologies that avail from the 5G would be the vehicular cloud networks (VCN). A prominent service out of this 5G VCN is the roadside accident video reporting by using 5G over the cloud. This service may contain private data/information that can be compromised at any channel (from vehicles to 5G and cloud storage) due to many reasons. This service is vulnerable to security attacks due to its availability for a long time at different channels. Moreover, multiple video reporting can cause huge storage and computation issues leading to inefficient computation and storage management. Consequently, data privacy, security, data management and computing efficiency of data storage become the main challenges in roadside accident vehicular cloud network video reporting services. This research is proposing a solution based on a new protocol to address the stated issues by extending the recent research presented by Lewis protocol et al. The proposed protocol is aimed to provide good data privacy, reduces the data security attacks, improving data management and the computation efficiency at all channels.**

Keywords—5G; vehicukar cloud network; video accident reporting; data privacy; security; storage management; storage efficiency

I. INTRODUCTION

The generations of wireless communication technologies started in 1970s and gradually developing rapidly in the last five decades [1]. These generations are identified by the changes in the data traffic and data rates. The data rate is expected to be increased multiple times around 2020. The bandwidth hungry applications such as multimedia files and live High Definition (HD) video streaming are growing drastically and consuming huge data rate that they exceed the limits of the current wireless communication systems. Therefore, the current 4G wireless communication technology will not be able to meet the high demand for faster data rate [2]. The increasing demand for higher capacity and data rate are leading to intensive projects and research works toward the next generation of wireless communication network systems which is the 5G technology. The 5G is expected to be fully implemented around early 2020 [3].

The 5G technology is becoming one of the most attractive research topics in academics and telecommunication systems industries. The evolving 5G technology shall be a strong base for supporting significant real-time services and it is to mitigate variety of challenges in these domains like low latency, higher data rate demand, energy consumption, operation cost, performance and so on [4]. The deployment of 5G technology with the help of D2D communications can provide reliable and efficient vehicular communications. Vehicular network using cloud communications have recently obtained considerable attention due to its ability to enhance the traffic efficiency and road safety [5]. The research community is aware that critical challenges still exist in the effective deployment of vehicular networks. Some recent studies on the standards used for vehicular networks showed that the IEEE 802.p standard is suffering from the lack of mobility support and scalability, whereas the LTE standard cannot get rigorous delay requirements in the presence of high traffic in cellular networks [6- 8]. With the expansion of 5G technology in vehicular networks, it is obvious that vehicles connected with other associated vehicles having the ability to share information via the cloud computing technologies could provide flexible solutions and services via the vehicular networks. Roadside accident video reporting service is one of the prominent applications of 5G over the VCNs bringing considerable attraction for providing enhanced road safety. Vehicles can communicate and sharing live videos of accident whereby the video can be archived into to the cloud storage to assist the official authorities to investigate the accident in a better perspective for taking undisputed actions [9].

The built-in camera sensors in the vehicle for recording videos can, in fact, collect a huge amount of vital data or information on real-time basis. These data/information can be consolidated and analyzed to trigger or alert invaluable services [10]. However, it should be noted that some of these data could be sensitive/privacy in nature that if disclosed to adversaries it can be violated during the transmissions between vehicles and/or devices. It can be vulnerable especially if the

978-1-5386-4744-8/18/$31.00 ©2018 IEEE

data/information are being made available for a long-time span. On the other hand, multiple vehicles can send the same data (recorded video) when they communicate via D2D communication over 5G, thus this increases the number of data that each entity receives and creates an overhead in the entity's storage [11]. To address these challenges, researchers need to propose various techniques and schemes to prevent the risk of data privacy leakages.

This paper starts with brief discussion on data privacy and security issues in the roadside accident video reporting service in the 5G enabled VCN. The rest of the paper is organized as follows: Section II highlights the problem statement, Section III presents the literature review, Section IV proposes the protocol and its technique, Section V is about some expected outcomes of the proposed protocol with discussions, and Section VI concludes the paper.

II. Problem Statement

Data privacy is a considerable concern that should be addressed in 5G enabled vehicular network to boost its adoption. The sensitive data from different applications such as real time video service that are transmitted over different entities of 5G enabled vehicular network (such as small cells, base stations, vehicles, or stored in the cloud) should therefore be protected.

There are several researches in the literature [12-14] proposed to solve the data privacy and security issues related to the roadside accident video reporting service over 5G enabled VCNs. They allow registered vehicles to record a live video for any accidents on roadside and store it on cloud using 5G services for uploading. The official authorities will be the destination of uploaded the recorded video that is accessed through the cloud storage, to issue an appropriate response. The researcher Eiza et al. [12] proposed a secure and privacy-aware real time video reporting service protocol for 5G enabled vehicular network. Sang et al. [13] extended and presented another protocol that addressed the limitations of work presented in [12] such as no management of multiple Trusted Authorities (TA), Department of Motor Vehicle (DMV) impersonation attack, forged video upload, Non- separation of responsibilities between Law Enforcement Agency (LEA) and Trusted Authority (TA) etc. The researchers Lewis et al. [14] further extended the work presented in [12,13] by presenting a new protocol. Research addressed the issues such as the usage of conventional public key, the expensive operations, and usage of an Attribute-Based Encryption (ABE) in which the participating vehicle sends the video, where it should know the receiver's public key to achieve the access control. They proposed a secure and lightweight protocol for cloud-assisted video reporting service in 5G enabled vehicular networks.

The proposed scenario in [14] is comparatively better than [12,13]. The following research problems/issues are however still there and need to be addressed. These are: (a) Data privacy issue: as stated, the data forwarded from vehicles to authorities using 5G, it keeps a copy of recorded video at all stations/channels including reporting vehicle, 5G cellular network, cloud, authorities and official vehicles. The availability of the recorded video at first three stations after successful delivery to the destination will rise the issues of data privacy in case of data is compromised at any station due to any reason such as disclosure attack or data leakage. (b) Data storage issue: it will be another issue for multiple copies of recorded video with time at first three stations from vehicles, 5G cellular network and cloud. (c) Vulnerable to security issue: after each successful delivery of recorded video to the final destination, there are vast chance of different security attacks such as replay attack, fabrication attack, traffic analysis attack and traceability attack due to its availability at different stations/ channels. (d) Storage efficiency issue: due to the large storage amount of data with time that may require more computation and capacity at different stations/channels will lead to inefficient computation and storage capacity. This become more issue in case of multiple copies of same video (duplicate) transfer from one station/ channel to another.

It is therefore a significant need to address these stated issues to protect data privacy as well as reduce the chance to become data vulnerable for longer time of possible attacks. In addition, to manage the storage capacity as well as computation and storage efficiency.

III. Literature Review

This section will provide in depth review and recent related studies about data privacy and security related to 5G, vehicular networks using cloud storage and the live video accident reporting service over the 5G enabled vehicular cloud networks.

Data privacy is a key concern in 5G enabled vehicular cloud networks, and a lot of researchers are spending time of working for handling this issue. Also, security is considered as one of the most important challenges along with privacy. On the other hand, data storage needs to be managed due to multiple copies of the same data (recorded video) that can be stored at each entity's storage. Furthermore, the large amount of data stored in the storage will require more computation and capacity at different channels and will lead to inefficient and limited computation and capacity capability.

Data privacy protection and security in 5G cellular networks were reviewed by many researchers in the literature [16,17]. Also, there are many researches [12-14, 18-23] addressed the potential issues of security and privacy related to the vehicular using cloud environment and the security and privacy of video reporting service over 5G enabled vehicular networks. Rajput et al. [18] proposed a Cloud Assisted Conditional Privacy Preserving Authentication (CACPPA) protocol. It is a hybrid scheme in which each region is managed by a single Certificate Authority (CA) so a common key pair is assigned to a group of vehicles. Hence, this prevents the attacker from distinguish the vehicles that are communicating differently. The (CA) issues credentials to vehicles that are used for authentication and protect privacy. Researchers in [19] presented a privacy preserving and secure protocol for traffic violation reporting service in vehicular networks using cloud with authentication and without using pairing operations. It provides the vehicles with ability to report the traffic violators. The protocol provides unlink ability among reporting vehicles and achieves a lightweight performance. Authors in [20] provided a conditional tracking mechanism that tracks and revokes the misbehaving vehicles in the network with efficient computation. It

authenticates vehicles with low-cost certificate and signature verification.

Among relevant works on security of real time video data, Liu et al. [21] proposed a real time secure data sharing and searchable platform over video data which took both the advantages of the mobile cloud platform and the 5G technology simultaneously. The scheme allows users to securely upload their real-time videos and share them with whom they want immediately. More specifically, there are only few research works existing for secure and preserving the privacy of the live video accident reporting service in 5G enabled vehicular cloud networks. Our main focus in this proposal is privacy preserving of the roadside accident video reporting service in 5G enabled vehicular cloud networks. One of the pioneers in proposing a video report service in 5G enabled vehicular networks was the Eiza et al. [12]. They proposed a secure and privacy- aware real time video reporting service protocol in 5G enabled vehicular network. The main components of system model are: participating vehicles that send the reporting video to the designated official vehicles, cloud platform to store and access the reporting video, Trusted Authority (TA) that generates pseudonymous certificate, policies and keys and issues them to each vehicle, Department of Motor Vehicle (DMV) that registers the participating vehicles and assigns a unique 5G_ID to them and law enforcement agency (LEA) that registers the designated official vehicles and assigns a unique 5G_ID to them and traces the misbehaving users that are trying to send a fabricated reporting video.

The work in [13] presented to eliminate the security and functionality flaws and limitations that were found in [12], which are: No Management of Multiple Trusted Authorities, DMV Impersonation Attack, Forged Video Upload, Non-separation of Responsibilities between LEA and TA, Privileged Insider Attack in LEA, LEA Impersonation Attack and Exposure of Location of Official Vehicles. They developed an improved scheme that provided a reliable and trusted real-time video reporting service in 5G enabled vehicular networks which resolved the identified security flaws. The system model extended the functionality of [12] with support of multi regions management that are composed of their own participating vehicles and designated official vehicles, cloud platforms, Trusted Authority (TA), Department Motor Vehicle (DMV), and Law Enforcement Agency (LEA).

Lewis et al. [14] resolved the drawbacks of [12] which are: the usage of conventional public key certificates that should be periodically (daily) renewed, the expensive operations that are used to build the protocol and the usage of an Attribute- Based Encryption (ABE) in which the participating vehicle sends the video, it should know the receiver's public key to achieve the access control. They proposed a secure and lightweight protocol for cloud-assisted video reporting service in 5G enabled vehicular networks. The proposed protocol minimizes the computation overhead by using a light-weight security primitive. Moreover, it provides authorization of entities using anonymous credential instead of the conventional public key certificate. The main components of system model are: participating vehicles that send the reporting video to the designated official vehicles, cloud platform to store and access the reporting video, Trusted Authority (TA) that registers all the entities in the system including vehicles, Road Side Cloud (RSC) and DMV and issues the cryptographic certificate, policies and keys, DMV that registers all the vehicles and assigns a unique 5G ID to them and RSCs that are cloud servers accessible by the vehicles and are located along the roads.

Authors in [22] overcame the weaknesses of [12] which are vulnerable to replay, message fabrication and DoS attacks. They proposed an authenticated scheme inspired by Eiza et al. protocol. The scheme preserved additional security attributes which can be robust against potential attacks in 5G enabled vehicular networks. Gopi et al. [23] developed an Enhanced Role- Based Access Control (ERBAC) mechanism for secure communication and allowing the authority to securely view the video stored in the cloud.

However, to enhance the data storage management efficiently to allow the data received from multiple vehicles to be aggregated, several studies have been conducted in the literature [24,25]. They manage the data storage to eliminate the duplication and redundant of the data and thus reduce its overhead.

The literature reviews about improving the security, privacy preserving and the storage data management in 5G technology, vehicular cloud networks and live video accident reporting service over 5G enabled VCNs show that developing effective frameworks for them is a challenge due to the amount of sensitive data/information that is collected by vehicles' cameras sensors which will be susceptible to privacy threats, leakage, and disclosure. Table I shows a comparison summary on the literature reviewed.

The comparative analysis in Table I reveals that the prior works/studies were either not supporting fully the 5G technology or they were having shortcomings/lack of security and privacy requirements. Also, there is a lack of studies that include challenges and issues for data privacy of video accident reporting service in 5G enabled VCNs. There are only a handful of studies which claim that they built a useful secure and privacy protocols for this service. But based on detailed literature review we found that the studies in [12-14, 18-23] have shortcomings and they didn't provide proper solutions for about: (1) the privacy of untrusted data storage which will be vulnerable to privacy violation, disclosure attack and data leakage if these entities are compromised; (2) security against data vulnerable in case of longer time available for possible attacks such as replay attack, fabrication attack, traffic analysis attack and traceability attack; (3) data storage management in case of huge data storage with time due to the multiple/repeated copies of same data are stored in the entity's storage and (4) Storage inefficiency due to the huge size of data stored and the computation required in the storage that will lead to inefficient computation and storage capacity. In this research we therefore intend to extend the work of [14] to address the issues mentioned above.

IV. Proposed Protocol Model

To address the stated issues in problem statement section, these calls to propose a new protocol which provides data privacy, enhanced data security chances against possible

attacks and improves the data management and computation efficiency at all stations/ channels.

Our new proposed protocol is depicted in Figure 1. It delivers data privacy after a successful delivery of recorded video to the authorities via the roadside accident video reporting service over the 5G enabled VCNs. The proposed data privacy protocol will provide efficient data storage management by deleting the successful delivered accident videos from all channels. It shall work on a three-way handshake approach. The three-way handshake approach is used to verify data has been received successfully and to verify and protect data between two computers. Where the client sends data packet to the server, then the server responds to the client with synchronization and acknowledgment signal bits and finally the client acknowledges the response of the server that the connection can be established, and data can be sent successfully. In our three-way handshake: (A) In the first handshake, it will deliver the recorded video of an accident to the authorities from road side registered vehicle to the authorities using 5G and cloud services. (B) In the second handshake, it will receive acknowledgement/confirmation from authorities to the forwarding vehicle, and (C) In third handshake, it will acknowledge (confirmation) the successful deleting of the delivered data. Computation and storage efficiency can therefore be enhanced by reducing/removing the huge volume of data at all channels.

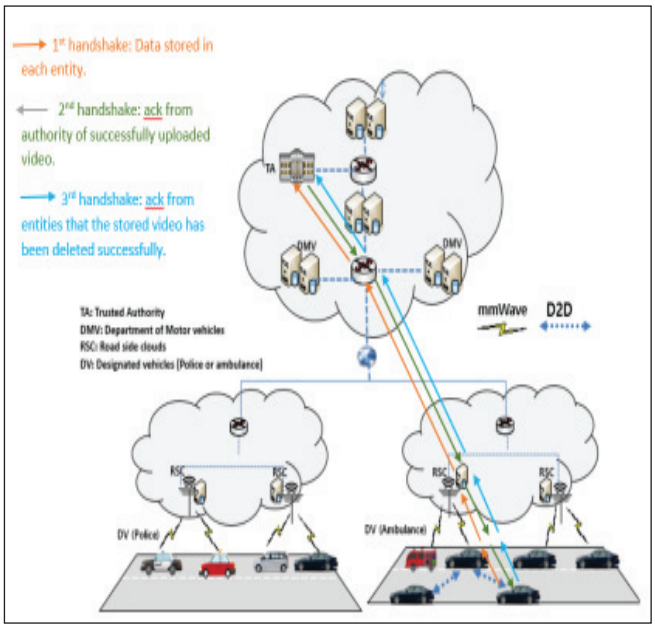

Fig. 1. System model of the proposed protocol adopted from [14]

V. Expected Outcomes and Discussions

This research presents a new data privacy-aware protocol that delivers data privacy of roadside accident video reporting service over 5G enabled VCNs. The expected results of this proposed protocol include: (A) it can significantly protect data privacy on all stations/ channels including vehicles, 5G services, and cloud services against attacks such as disclosure attacks and data leakages after successful delivery of recorded video. (B) It can improve the data security by reducing the chances of several attacks, such as replay attack, fabrication attack, traffic analysis attack and traceability attack by removing the data of delivered recorded videos. (C) It can address the data storage and capacity management and its computation issues efficiently by deleting unnecessary data upon successful delivery. Hence, this protocol will extend an enhanced system model previously proposed by Lewis et al. [14] to reduce the risks of existing security issues for possible security and privacy attacks due to availability of delivered data at different stations/ channels.

VI. Conclusion

The contemporary 4G wireless data throughput is the main challenge for high data rate real-time video delivery. However, with the emergence of the 5G technology, this challenge could be mitigated due to the better data rate offers in 5G. Roadside accident live video reporting services could become a reality by leveraging on the 5G enabled VCNs for sending accident occurring videos to the relevant authorities on real-time basis. The private/sensitive data/information collected by the built-in camera sensors in vehicles can be prevented from being disclosed to adversaries by the proposed 3-way handshake protocol. In addition, the proposed protocol is to provide data privacy, enhanced data security against possible attacks and to improve data management and computation efficiency at all channels.

Acknowledgment

We acknowledge with thanks and appreciations to the College of Computer Sciences & IT, King Faisal University, Saudi Arabia for providing the opportunity to conduct this research.

References

[1] Parashar, P., Chauhan, N., & Gonsai, S. K. (2017). BASICS OF 5G TECHNOLOGY AND ITS EVOLUTION, International Research Journal of Engineering and Technology (IRJET), 04(04), (PP. 2007-2008).

[2] Gohil, A., Modi, H., & Patel, S. K. (2013, March). 5G Technology of Mobile Communication: A Survey. IEEE In International Conference on Intelligent Systems and Signal Processing (ISSP), 2013 (pp. 288- 292).

[3] Pirinen, P. (2014, November). A Brief Overview of 5G Research Activities. IEEE In 1st International Conference on 5G for Ubiquitous Connectivity (5GU), 2014 (PP. 17-22).

[4] Hossain, E., & Hasan, M. (2015). 5G Cellular: Key Enabling Technologies and Research Challenges. IEEE Instrumentation & Measurement Magazine, 18(03), (PP. 11- 21).

[5] Liang, L., Li, G., & Xu, W. (2017). Resource Allocation for D2D-Enabled Vehicular Communications. IEEE Transactions on Communications, 65(07), (PP. 3186 – 3197).

[6] Mir, Z. H., & Filali, F. (2014). LTE and IEEE 802.11 P for Vehicular Networking: a Performance Evaluation. Springer EURASIP Journal on Wireless Communications and Networking, 2014(01), 89.

[7] Vinel, A. (2012). 3GPP LTE versus IEEE 802.11 P/WAVE: Which Technology is Able to Support Cooperative Vehicular Safety Applications? IEEE Wireless Communications Letters, 01(02), (PP. 125-128).

[8] Bellalta, B., Belyaev, E., Jonsson, M., & Vinel, A. (2014). Performance Evaluation of IEEE 802.11 P-Enabled Vehicular Video Surveillance System. IEEE Communications Letters, 18(04), (PP. 708- 711).

[9] Smida, E. B., Fantar, S. G., & Youssef, H. (2017, February). Video Streaming Challenges over Vehicular Ad- Hoc Networks in Smart Cities. IEEE In International Conference on Smart, Monitored and Controlled Cities (SM2C), 2017 (PP. 12- 16).

[10] Lee, E., Lee, E. K., Gerla, M., & Oh, S. Y. (2014). Vehicular Cloud Networking: Architecture and Design Principles. IEEE Communications Magazine, 52(02), (PP. 148-155).

[11] Yu, R., Zhang, Y., Gjessing, S., Xia, W., & Yang, K. (2013). Toward Cloud- Based Vehicular Networks with Efficient Resource Management. IEEE Network, 27(05), (PP. 48- 55).

[12] Eiza, M. H., Ni, Q., & Shi, Q. (2016). Secure and Privacy- Aware Cloud-Assisted Video Reporting Service in 5G- Enabled Vehicular Networks. IEEE Transactions on Vehicular Technology, 65(10), (PP. 7868- 7881).

[13] Yoo, S. G. (2017). 5G-VRSec: Secure Video Reporting Service in 5G Enabled Vehicular Networks. Hindawi Wireless Communications and Mobile Computing, 2017(PP. 1- 22).

[14] Nkenyereye, L., Kwon, J., & Choi, Y. H. (2017). Secure and Lightweight Cloud-Assisted Video Reporting Protocol over 5G-Enabled Vehicular Networks. MDPI Sensors Journal, 17(10), (PP. 2191).

[15] Cisco (2017). Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021, Cisco White Paper, (2017), (PP. 1- 35).

[16] Tiburski, R. T., Amaral, L. A., & Hessel, F. (2016). Security Challenges in 5G-Based IoT Middleware Systems. Springer In Internet of Things (IoT) in 5G Mobile Technologies, (PP. 399- 418).

[17] Khan, A. S., Javed, Y., Abdullah, J., Nazim, J. M., & Khan, N. (2017). Security Issues in 5G Device to Device Communication. International Journal of Computer Science and Network Security (IJCSNS), 17(05), (PP. 366).

[18] Rajput, U., Abbas, F., Wang, J., Eun, H., & Oh, H. (2016, May). CACPPA: A Cloud- Assisted Conditional Privacy Preserving Authentication Protocol for VANET. IEEE In 16th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), 2016 (PP. 434- 442).

[19] Nkenyereye, L., & Rhee, K. H. (2016). Secure and Privacy Preserving Protocol for Traffic Violation Reporting in Vehicular Cloud Environment. KOREASCIENCE Journal of Korea Multimedia Society, 19(07), (PP. 1159- 1165).

[20] Azees, M., Vijayakumar, P., & Deboarh, L. J. (2017). EAAP: Efficient Anonymous Authentication with Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks. IEEE Transactions on Intelligent Transportation Systems, 18(09), (PP. 2467- 2476).

[21] Liu, J. K., Au, M. H., Susilo, W., Liang, K., Lu, R., & Srinivasan, B. (2015). Secure Sharing and Searching for Real- Time Video Data in Mobile Cloud. IEEE Network, 29(02), (PP. 46- 50).

[22] Mohseni-Ejiyeh, A., & Ashouri-Talouki, M. (2017, May). SeVR+: Secure and Privacy- Aware cloud Assisted Video Reporting Service for 5G Vehicular Networks. IEEE In Iranian Conference on Electrical Engineering (ICEE), 2017 (PP. 2159- 2164).

[23] Gopi, R., & Rajesh, A. (2017). Securing Video Cloud Storage by ERBAC Mechanisms in 5G Enabled Vehicular Networks. Springer Cluster Computing, 20(04), (PP. 3489- 3497).

[24] Yu, B., Xu, C. Z., & Guo, M. (2012). Adaptive Forwarding Delay Control for VANET Data Aggregation. IEEE Transactions on Parallel and Distributed systems, 23(01), (PP. 11- 18).

[25] Kakkasageri, M S., & Manvi, S. S. (2011, December). Safety Information Aggregation in VANETs using Vehicle Beliefs. IEEE In 5th International Conference on Advanced Networks and Telecommunication Systems (ANTS), 2011 (PP. 1- 6)

TABLE I. COMPARATIVE SUMMARY OF LITERATURE REVIEW

References	Features	Limitations	Future Work
Ref. [18]	Authentication, Message integrity, Non-repudiation, Pseudonym revocation, Conditional anonymity.	Support single cloud authority only. It does not support of 5G technology.	They aim to optimize and implement the protocol.
Ref. [19]	Identity privacy preserving, Authentication, Unlink ability, Traceability.	Untrusted storage It does not support of 5G technology.	Not available
Ref. [20]	Secure against impersonation attack, message integrity, conditional privacy preservation, message authentication.	High computation overhead, It does not support of 5G technology.	To efficiently provide a batch authentication with low computation overhead.
Ref. [21]	Secure data sharing and searching, Data confidentiality, Authentication.	The computation and communication costs are overhead and inefficient.	Not available
Ref. [12]	Authentication, Non-Repudiation, Conditional Anonymity and Privacy, Traceability, Resistance against eavesdropping attack.	Distributed notification (from different areas), location exposure of designated vehicles, Untrusted cloud storage, Lack of Efficiency.	Management of distributed notifications from different areas, protecting the location of the designated official vehicles.
Ref. [13]	Authentication & Non-repudiation; Conditional Anonymity & Privacy; Secure against: DMV & LEA impersonation attack, forged video & replay attack, insider attack in LEA, exposure of location of DV; Separate responsibility between LEA & TA.	No participation of DV in Pseudo-Certificate Revocation Protocol, of DV in handover protocol in TA management, No encryption of ID of CV sent to DMV for Pseudo-Certificate Revocation protocol, Untrusted cloud storage.	Not available
Ref. [14]	Authentication, Authorization, Identity privacy preservation, Fine grained access control, Non-repudiation, Traceability, Better performance.	No encryption of real identity and 5G_ID sent to TA, No management between regions, Exposure of location of vehicles. Untrusted data storage.	Not available
Ref. [22]	Conditional privacy and anonymity preservation, System Traceability, Resistance against man-in-the-middle, replay, participant vehicle impersonation and DoS attack.	Distributed notification (from different areas), Location exposure of vehicle, Lack of efficiency, untrusted data storage.	Not available
Ref. [23]	Secure cloud storage, enhanced role-based access control over the video reporting and sharing.	Lack of efficiency, untrusted vehicle's data storage	Investigate different technics in cryptography for video reporting service and access control policies analysis.