Article

A Literature Review of Security and Privacy Challenges in 5G-Enabled Vehicular Networks (5GVNs)

Mohammed Ahmed Khammas, Lok Wing Lavin Wong, Alexander Shore

Abstract

Integrating 5G technology into vehicular networks significantly advances intelligent transportation systems. This integration has the potential to significantly improve connectivity, facilitate real-time data exchange, and support new services with ultra-low latency and high data throughput. However, these technological advancements also bring substantial privacy and security challenges that must be addressed to ensure safe and efficient vehicle communication. Significant privacy threats are genuinely potentially risky, such as breaches of data confidentiality, identity theft, location tracking, trajectory inference, and security risks from attacks like eavesdropping impersonation, and man-in-the-middle scenarios are likewise the trend. It evaluates existing privacy-preserving mechanisms and highlights gaps in current frameworks due to the unique features of 5G architectures, including decentralised infrastructures and high-speed transmissions. Mitigation to the potential risks, emerging solutions such as secure autonomous and blockchain-based trust models are common and essential. In this paper, we identify peer-reviewed literature that focuses on security and privacy concerns surrounding 5GVNs, with the 5G technology and the architecture of 5G-enabled vehicular networks utilised and how its vulnerability causes the security and privacy challenges that threaten human life. This review of papers emphasises the importance of proactive privacy and security frameworks to protect the deployment of 5G-driven vehicular technologies, likewise with recommendations for future research emphasises the need for adaptive privacy management, robust authentication strategies, and comprehensive policy-based controls to mitigate evolving risks.

1. Introduction

Vehicle networks have been completely transformed by 5G communication technology, which makes it possible for real-time, fast connection for uses like traffic monitoring and autonomous driving. But there are security and privacy issues with this technology as well. 5G networks' open architecture makes them vulnerable to internet risks like snooping and identity theft. Sensitive data cannot be effectively secured by current privacy-preserving methods, which might destroy public confidence and limit the deployment of 5G. (Li, et al, 2021)

For 5GVNs to reach their full potential, privacy and security concerns must be fixed. The more connected cars there are, the greater the likelihood of data breaches and unauthorised access. Ensuring user safety and establishing technical confidence need the implementation of robust privacy solutions. This will accelerate the implementation of it, enhance operational efficacy

and safety, and encourage the development of innovative improvements in transportation protocols.

The following queries are investigated in this report: What are the key issues with 5GVNs' security and privacy? How might we modify current systems to address these issues? Which newest methods can protect privacy without sacrificing system efficiency? The report is split into sections that address the architecture of 5GVNs, important problems, current fixes, possible future research methods, and a closing analysis. (Lia, et al, 2020)

This essay is organised as follows: The architecture, key characteristics, and services of 5GVNs are outlined in the next section. The following part explores 5GVN-specific security and privacy issues and highlights how they affect users and the system. Then we review current privacy-preserving technologies, assess their performance, and talk about how they may be used with 5GVNs. The penultimate section examines different concepts and possible lines of inquiry to fill in the gaps in the available solutions. The article ends with several important observations and suggestions for more research in the field.

2. Search Methodology

The aim of this search methodology is to find relevant and useful research papers that will provide background knowledge and answer the research questions stated in the introduction. Keyword searches will be used. The key words that have been selected are “5G-vehicular networks” Boolean operator AND “security challenges “Boolean operator OR “privacy challenges” and keyword “solution”. A date range of the last 4 years 2020-2024 was also used to ensure the papers would be up to date and relevant based on the latest technology to ensure our findings were accurate. To ensure the papers are reliable the search was carried out using search engines such as IEEE, MMU library and google scholar. The studies need to contain information and evidence relating to the privacy and security concerns of 5G-verhicular to answer our research questions. What are the key issues with 5GVNs' security and privacy? And how can these be resolved.

3. Findings

Table 1. Key data reported by primary studies and papers.

Research Paper	Key Findings	Categories
Li, et al, 2021 [1]	The article "Privacy for 5G-Supported Vehicular Networks" discusses identity theft, location monitoring, and listening as ways that 5G networks may compromise privacy. Identity privacy, location privacy, direction privacy, and data privacy are important confidentiality goals. Existing privacy-preserving solutions include pseudonymization, multi-party computation, and differential privacy, which strike a balance between system efficiency and privacy protection. Privacy-preserving mechanisms focused on safeguarding users' personal data from unapproved parties.	1. Privacy 2. Developer 3. Protection
Lia, et al, 2020 [2]	The research study "Security and Privacy Challenges in 5G-Enabled Vehicular Networks" examines the design, potential threats to security, and recommended solutions for networks that make use of 5G. The paper highlights key security issues, including replaying attacks, message tampering, and fake identities. Solutions include multi-party computation, distributed group key control, and blockchain technology for trust management. Layered security frameworks for 5G vehicular networks to ensure secure communication and reduce risks.	1. Blockchain 2. Behaviour 3. Developer

Garg, et al, 2019 [3]	Studies suggest using software-defined networking (SDN) for 5G network flexibility, addressing identity spoofing, eavesdropping, and replay attacks, discussing privacy risks, and evaluating elliptic curve cryptography for mutual authentication and intrusion detection. SDN improves network management, but latency concerns may arise. Existing security measures are not scalable for real-time vehicular networks. 5GVNs increase privacy risks, ECC-based mutual authentication incurs computational overhead. Tensor-based dimensionality reduction reduces data size. This includes network management frameworks, layered security frameworks, privacy-preserving communication protocols, mutual authentication models using ECC, intrusion detection models with dimensionality reduction, and performance evaluation frameworks for vehicular networks.	1. Behaviour 2. Privacy 3. Developer
Lu, et al, 2020 [4]	This paper comprehensively explores security and privacy challenges in 5G-enabled vehicle-to-everything (V2X) communications. The authors highlight the layered architecture of 5G V2X, including core, edge, and access networks, each vulnerable to unique threats. Key security risks identified which strength lies in the detailed exploration of real-world threats including denial-of-service (DoS), Sybil, and man-in-the-middle (MITM) attacks, while privacy concerns focus on unauthorised tracking and data inference. The study emphasises the complexity of trust services, given the dynamic roles of vehicles as both service consumers and providers.	1. Security 2. Privacy 3. Trust

Sağlam and Bahtiyar, 2019 [5]	This paper classifies security challenges within 5G Vehicular Networks (5GVNs) into foundational domains of authentication, confidentiality, availability, and integrity. The author systematically highlights attack vectors, including eavesdropping, jamming, and distributed denial-of-service (DDoS), and discusses privacy risks associated with unauthorised data access. The survey in the paper proposes privacy-preserving mechanisms such as pseudonym-based authentication and group-based signature schemes. Additionally, lightweight cryptographic frameworks optimised for the stringent latency requirements of V2X communications.	1. 5G 2. Security 3. Privacy 4. Authentication 5. Encryption
Wazid, et al, 2021 [6]	This paper examines security and privacy concerns within the broader context of 5G-enabled Internet of Things (IoT) ecosystems, with a particular relevance to vehicular networks. It categorises defence mechanisms into key management, access control, and intrusion detection, addressing threats such as impersonation, malicious routing, and password-guessing attacks. The studies advocate for innovative solutions like blockchain-based trust frameworks and AI-driven anomaly detection systems, which hold high potential to combat adaptive and evolving cyber threats. A comprehensive comparison of security protocols highlights gaps in real-time adaptability and cross-layer protections.	1. IoT 2. Privacy 3. Security 4. Blockchain 5. Trust
Manda, 2024 [7]	This document focuses on the security and privacy of 5G technology application. It discusses integrating 5G technology in urban infrastructures, enhancing connectivity and enabling various innovative applications such as traffic management, smart grids, and public safety systems. The study identifies privacy concerns related to data collection and analysis, utilising large-scale data collection and real-time analytics applied to identify potential privacy issues. Also, there are security challenges from the	1. IoT 2. Privacy 3. Security 4. Encryption 5. Compliance

	increased number of connected devices. It emphasises the need for robust cybersecurity frameworks (compliance regulations such as GDPR and CCPA) to protect against data breaches and unauthorised access. The author also explores the role of 5G technology in supporting real-time applications while addressing potential vulnerabilities and proposing solutions for secure implementation.	
Eiza, et al, 2016 [8]	This paper demonstrates the growing awareness and potential challenges of the privacy and security sector in 5G-enabled vehicular networks. It particularly highlights the role of 5G in enhancing vehicular network security, especially in the real-time transmission of accident videos by vehicles to official entities like police or ambulances. The study highlights the scalability and latency improvements brought about by 5G technology and introduces a privacy-aware protocol that incorporates secure communication and traceability features. The 5G network system integrates advanced cryptographic mechanisms (pseudonymous authentication and ciphertext-policy attributed-based encryption) to guarantee both security and privacy.	1. Privacy 2. Security 3. Data Transmission Efficiency 4. Encryption
Talpur and Gurusamy, 2022 [9]	The paper shows a range of similar security and privacy concerns mainly stemming from the vast amount of extremely sensitive information collected by diverse services. These concerns primarily arise due to the nature of the data being gathered, its storage and who can access it. The types of data involved are particularly sensitive, including live GPS locations, travel speeds, environmental data, and detailed travel routes. In addition, the collection of usage patterns, such as where users go, how long they stay in specific locations, and their routines, significantly increases the potential privacy risks. When this extensive data is collected, it has the potential to compromise the anonymity of users. By linking data points such as locations and behaviours, it becomes possible to re-identify individuals and correlate their identities	1. Data Collection 2. Privacy 3. Machine Learning

	with other datasets. For example, a user's name or personal details might be revealed by cross-referencing their travel patterns with other datasets that contain identifiable information, thereby eroding privacy. This raises serious concerns about the unintended or malicious use of such information, particularly when third parties have access to it or when it is inadequately protected.	
Feng, et al, 2021 [10]	These papers highlighted three main categories of attacks, infrastructure based, sensor based, and wireless communication based. Infrastructure-based attacks target the supporting network infrastructure, which can include attacks like DDoS (Distributed Denial of Service) attacks, where the attacker floods the network with traffic, rendering the system unable to process legitimate requests. These types of attacks can disrupt critical services that vehicles rely on, such as traffic management and safety alerts. Sensor-based attacks involve manipulating or sabotaging the sensors embedded in vehicles or infrastructure, which are crucial for detecting nearby objects, road conditions, and other vehicles. This can lead to attacks like location tailing, where an attacker tracks the position of a vehicle over time, compromising the privacy and safety of the driver. Wireless communication-based attacks exploit the communication systems that vehicles use to exchange information with each other and with the infrastructure. Common types include Sybil attacks, where an attacker falsifies multiple identities in the network, jamming attacks, where communication is disrupted by overwhelming the system with noise, and spoofing attacks, where a malicious entity pretends to be a legitimate vehicle or infrastructure to gain unauthorised access or influence the system.	1. Cyber attack 2. Network Security 3. System Control

4. Discussion

4.1 Research Paper [1]-[3]

In order to address the research questions regarding security and privacy issues in 5G-enabled vehicular networks (5GVNs), we went over the documents. To help improve these networks' security, effectiveness, and protection, the articles offer insights into the primary challenges and suggested solutions.

Li, et al [1] investigates ways to strengthen security mechanisms in 5GVNs in response to new threats. The main security issues include replay attacks, message manipulation, and impersonation. Although the study recommends using distributed group key management and blockchain-based trust frameworks to improve current systems, it suggests scalability and latency reduction improvement. Another major challenge is striking a balance between security and efficiency; multi-party computation and lightweight encryption techniques have been proposed as workable solutions. The studies also discuss privacy risks like location monitoring, identity theft, and eavesdropping, and they recommend strong privacy-preserving measures. Additionally, the research recommends improving privacy-preserving techniques to manage high transmission speeds and massive data volumes in 5GVNs. The findings report ends by stressing how crucial it is to solve privacy issues in 5GVNs to maintain user confidence.

From the paper by Lia, et al [2], it emphasises the need for scalable solutions to manage real-time applications. It also recommends being guided by artificial intelligence threat detection, standardising privacy procedures, optimising trust frameworks, enhancing privacy mechanisms to manage massive data volumes, and developing scalable solutions for real-time applications. These suggestions aim to improve the reliability, efficiency, and safety of 5G-enabled vehicle networks, opening the door for further study and practical implementations.

Garg, et al [3] proposes a software-defined networking (SDN) framework to improve security and privacy in 5G-enabled vehicular networks. The main challenges identified in the document include spoofing, Sybil attacks, and packet duplication, while privacy concerns arise from unauthorised access to user data. Traditional security protocols are inadequate for the dynamic and high-speed nature of 5GVNs. The proposed framework includes an Authentication Module

using elliptic curve cryptography (ECC) for mutual authentication and an Intrusion Detection Module using tensor-based dimensionality reduction and fuzzy clustering for detection. The document suggests that innovative methods, such as tensor-based dimensionality reduction and fuzzy clustering, can balance privacy protection with system performance. It recommends developing scalable authentication mechanisms, enhancing intrusion detection systems, and focusing on privacy-preserving communication to ensure secure and efficient communication in 5GVNs.

Overall, the documents under study highlight how important it is to address privacy and security issues in 5GVNs. These networks can increase user trust and dependability by implementing scalable solutions, improving intrusion detection systems, and upgrading authentication procedures. To make sure that these methods can be used in real-world situations, more research is required.

4.2 Research Paper [4]-[8]

Challenges

The integration of 5G technology into vehicular networks has brought transformative capabilities and significant security and privacy challenges. A prominent challenge is scalability and latency, where existing standards like IEEE 802.11p and LTE exhibit high latency and insufficient scalability for real-time applications. Although 5G technology delivers ultra-low latency and higher throughput, the improvements come with new vulnerabilities that must be urgently addressed [4][8]. Another critical security issue is authentication and trust management. Dynamic vehicular roles and decentralised the verification of infrastructure's complicate identity, making the networks susceptible to Sybil attacks, impersonation, and replay attacks [5][8]. Besides, privacy risks associated with vast data generation raise concerns about unauthorised access and tracking as well as identity exposure [4][7]. The diverse architecture of 5G, including small cells, device-to-device (D2D) communication, and cloud integration, creates multiple layers where security vulnerabilities can be exploited [7][8]. Finally, balancing privacy and traceability remains a fundamental challenge, since anonymity must be preserved which also ensuring accountability for malicious actions [5][8].

Solutions

Several solutions have been proposed to address the challenges. Pseudonymous authentication mechanisms ensure privacy by concealing user identities while enabling conditional anonymity. Protocols like the pseudonymous authentication scheme with strong privacy preservation (PASS) reduces certificate verification overhead, making them suitable for real-time vehicular communications [8]. To apply encryption-based frameworks like ciphertext-policy attribute-based encryption (CP-ABE) and public key encryption with keyword search (PEKS), can enhance the confidentiality and secure cloud-assisted data management [6][8]. Particularly, blockchain technology is a significant solution that offers a decentralised alternative that minimises dependence on a central trusted authority (TA) and enhances resilience against single points of failure [4][6]. Besides, having adaptive security frameworks which utilise software-defined networking (SDN) and network function virtualisation (NFV) provide scalable, flexible policy enforcement to counter evolving threats dynamically [4][8]. Finally, AI-based anomaly detection systems have been suggested to enhance real-time threat detection and response [6].

Recommendations

First, to develop decentralised trust management frameworks using blockchain can mitigate vulnerabilities that linked to centralised authorities [6][8]. Second, a crucial aspect of implementation of future research should prioritise empirical evaluations of proposed protocols under real-world conditions [4][5]. This practical validation is essential to assess latency, throughput, and overall performance, and it encourages hands-on research in 5G security. Third, incorporating privacy-by-design principles such as adaptive pseudonym schemes or selective disclosure mechanisms, will boost the privacy protection without sacrificing accountability [4][7]. Fourth, the lightweight cryptographic solutions delivered optimisation for resource-constrained devices should be prioritised to minimise processing overhead and energy consumption [6][8]. Last, to have collaboration among academia, industry, and regulators is essential to strengthen the development of comprehensive security governance frameworks for the secure and scalable deployment of 5G technology in vehicular networks [6][7].

4.3 Research Paper [9]-[10]

Proposed machine learning

A proposed ML program that can be used to detect attacks on vehicular networks based off shared knowledge and previous experience from attacks, which is used to dynamically update the knowledge base of the ML and share with other vehicles. This has a major advantage over traditional detection methods with rely entirely on prior knowledge and patterns of previous attacks that are kept by central body. The decentralised nature of ML will allow vehicles to share information with each other and adapt without waiting for a data base and an update to be released to detect a new method of attack. This ensures if a new attack is detected and then prevented, this knowledge is than added to the knowledge base and shared with other vehicular networks.

However, ML based solutions have several challenges that will make implementing this solution extremely difficult. ML has extremally high energy, data, bandwidth, and processing power consumption making them expensive to run. This also poses the problem of vehicles having limited processing power which makes local ML training extremely difficult which as smart vehicles and vehicular networks need to make spontaneous decisions which if not done locally can cause latency in responses as it will need to communicate with a server. Latency issues are a verify prevalent issue for ML as it relies on an iterative process high latency can cause several safety issues for autonomous vehicles using these networks such as not reacting to changing environments quick enough leading to collisions or delay in detecting a potential attack which could cause catastrophic issues.

Block chains are public legers with chains of blocks each containing data such as transactions without having to be verified by a central body. This means minimal data can be given such as an alias and the data they are adding to the block making it anonymous for users. These blocks are then validated to ensure they are legitimate by random. They propose that the anonymiser creates and proposes the block and then the AP verifies the block and once it is accepted block is then added to the block chain. This has a number of benefits such as only allowing verified vehicles onto the network and ensures each transaction of data is legitimate and verified.

5. Conclusion and Future work

This report has comprehensively reviewed the security and privacy challenges in 5G-enabled vehicular networks (5GVNs) by analysing peer-reviewed research papers and exploring innovative solutions to mitigate these risks. Our research has revealed the significant potential of 5G technology, which enhances vehicular networks by improving connectivity, reducing latency, and enabling real-time data exchanges. However, it also brings new vulnerabilities, which include identity theft, location tracking, eavesdropping, replay attacks, Sybil attacks, and so on. These threats are serious troubles to user privacy and system security.

The findings across the reviewed papers emphasise that a multi-faceted approach is required to address the security and privacy challenges. Solutions such as blockchain-based trust frameworks, pseudonymisation techniques, multi-party computation, elliptic curve cryptography (ECC), and AI-driven threat detection systems have been proposed to improve security without sacrificing system efficiency. These approaches strengthen authentication processes, detect real-time anomalies, and safeguard users' sensitive personal data from unauthorised access. However, implementing these solutions presents challenges simultaneously, particularly in ensuring scalability, minimising computational overhead, and maintaining real-time adaptability. The studies reviewed emphasise the necessity of creating lightweight, scalable cryptographic solutions and adaptive security frameworks to address these concerns effectively. Additionally, adopting privacy-by-design principles can incorporate privacy considerations into the design and operation of systems, which is crucial for balancing privacy protection with system accountability.

The review of this paper also points to the growing role of machine learning in improving vehicular network security. Decentralised machine learning systems, which dynamically update their knowledge base and share attack prevention measures with other vehicles, offer promising potential to combat evolving threats. Besides, blockchain technology is recognised as a viable solution for ensuring secure, anonymous, and decentralised communication within 5GVNs, which can reduce dependence on central authorities and improve system resilience. These advancements bring hope for a more secure and efficient 5GVNs in the future.

In conclusion, the report highlights the urgent need for ongoing research and collaboration among academia, industry, and policymakers to strengthen 5GVNs' security and privacy frameworks. Future research directions should focus on real-world validation of proposed solutions to ensure their practical applicability in diverse vehicular environments. By addressing the identified challenges, 5GVNs can potentially achieve excellent reliability, efficiency, and safety, building user trust. They can also have a robust security system for privacy protection, and the adoption of 5G-driven vehicular technologies is encouraged to continue for the human future.

References

1. M. Li, L. Zhu, Z. Zhang, C. Lal, M. Conti and F. Martinelli, "Privacy for 5G-Supported Vehicular Networks," in IEEE Open Journal of the Communications Society, vol. 2, pp. 1935-1956, 2021, doi: 10.1109/OJCOMS.2021.3103445.
2. C. Lai, R. Lu, D. Zheng and X. Shen, "Security and Privacy Challenges in 5G-Enabled Vehicular Networks," in IEEE Network, vol. 34, no. 2, pp. 37-45, March/April 2020, doi: 10.1109/MNET.001.1900220.
3. S. Garg, K. Kaur, G. Kaddoum, S. H. Ahmed and D. N. K. Jayakody, "SDN-Based Secure and Privacy-Preserving Scheme for Vehicular Networks: A 5G Perspective," in IEEE Transactions on Vehicular Technology, vol. 68, no. 9, pp. 8421-8434, Sept. 2019, doi: 10.1109/TVT.2019.2917776.
4. R. Lu, L. Zhang, J. Ni and Y. Fang, "5G Vehicle-to-Everything Services: Gearing Up for Security and Privacy," in Proceedings of the IEEE, vol. 108, no. 2, pp. 373-389, Feb. 2020, doi: 10.1109/JPROC.2019.2948302.
5. E. T. Sağlam and Ş. Bahtiyar, "A Survey: Security and Privacy in 5G Vehicular Networks," 2019 4th International Conference on Computer Science and Engineering (UBMK), Samsun, Turkey, 2019, pp. 108-112, doi: 10.1109/UBMK.2019.8907026.
6. M. Wazid, A. K. Das, S. Shetty, P. Gope and J. J. P. C. Rodrigues, "Security in 5G-Enabled Internet of Things Communication: Issues, Challenges, and Future Research Roadmap," in IEEE Access, vol. 9, pp. 4466-4489, 2021, doi: 10.1109/ACCESS.2020.3047895.
7. Manda, J.K., 2024. 5G-enabled Smart Cities: Security and Privacy Considerations. Innovative Engineering Sciences Journal, 4(1).
8. M. Hashem Eiza, Q. Ni and Q. Shi, "Secure and Privacy-Aware Cloud-Assisted Video Reporting Service in 5G-Enabled Vehicular Networks," in IEEE Transactions on Vehicular Technology, vol. 65, no. 10, pp. 7868-7881, Oct. 2016, doi: 10.1109/TVT.2016.2541862.
9. Talpur, A. and Gurusamy, M. (2022) “Machine Learning for Security in Vehicular Networks: A Comprehensive Survey,” IEEE Communications Surveys & Tutorials, 24(1). Available at: https://doi.org/10.1109/COMST.2021.3129079.
10. Feng, J. et al. (2021) “Blockchain-Based Data Management and Edge-Assisted Trusted Cloaking Area Construction for Location Privacy Protection in Vehicular Networks,” IEEE Internet of

Things Journal, 8(4). Available at: https://doi.org/10.1109/JIOT.2020.3038468.

Group Work Reflection

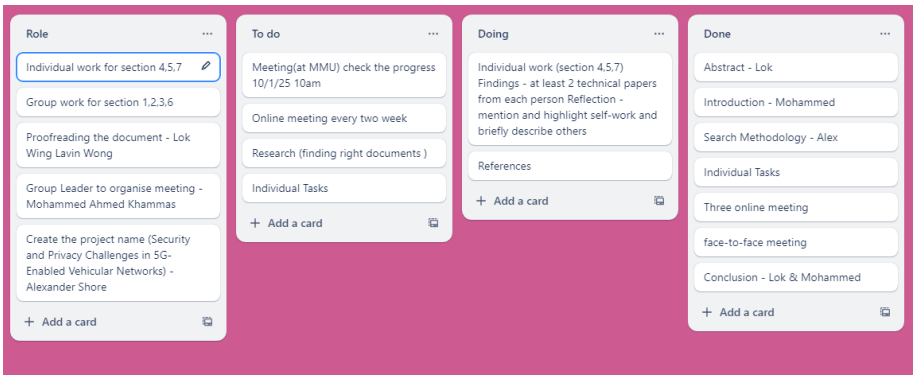

Figure 1: Trello record

In the group collaboration, I was working collaboratively with Mohammad and Alex on this paper. Our group work distribution is shown on the Trello board above in Figure 1 (Me – Abstract & Conclusion, Mohammed – Introduction & Conclusion, Alex – Search Methodology). We split the group work sections (1,2,3,6) which can be found under the Done list. For the roles to the paper, I was responsible to proofread the whole work of our paper including grammar checking and sentence structure issues, and simply organisation such as putting the right thing on the appropriate parts. Mohammed, the group leader, who organised every physical and online meeting to follow-up the working progress. Alex created the theme and topic for the paper, as well as finding key words for the group to search for resources to use. Trello and Teams were the planning and communication tools that we utilised.

For my individual contribution, I focused on reading, analysing and synthesising the key content from the research papers [4]-[8]. It was to ensure that our discussion was grounded simultaneously in robust with the current research. In the discussion section, I deliver a comprehensive summary of challenges and proposed solutions related to our topic.

By working this project of literature review, I realised some gains and challenges during the process. Personally, my ability enhanced to critically access academic technical papers and how to find key connections between different studies with relevant content of knowledge. This group work experience also honed my collaborative skills, as I worked closely with my group to ensure that our individual parts aligned cohesively within this project. This project has been a valuable learning experience in both research and teamwork management to me.

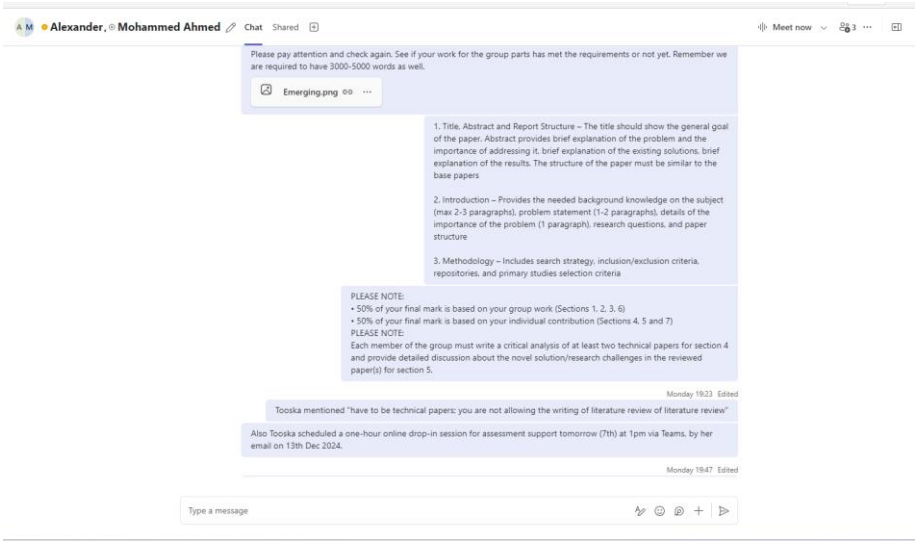

Figure 2: Teams meeting record (1)

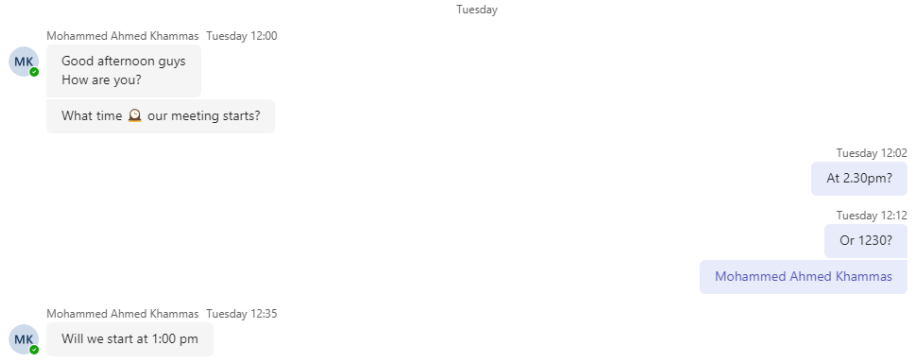

Figure 3: Teams meeting record (2)

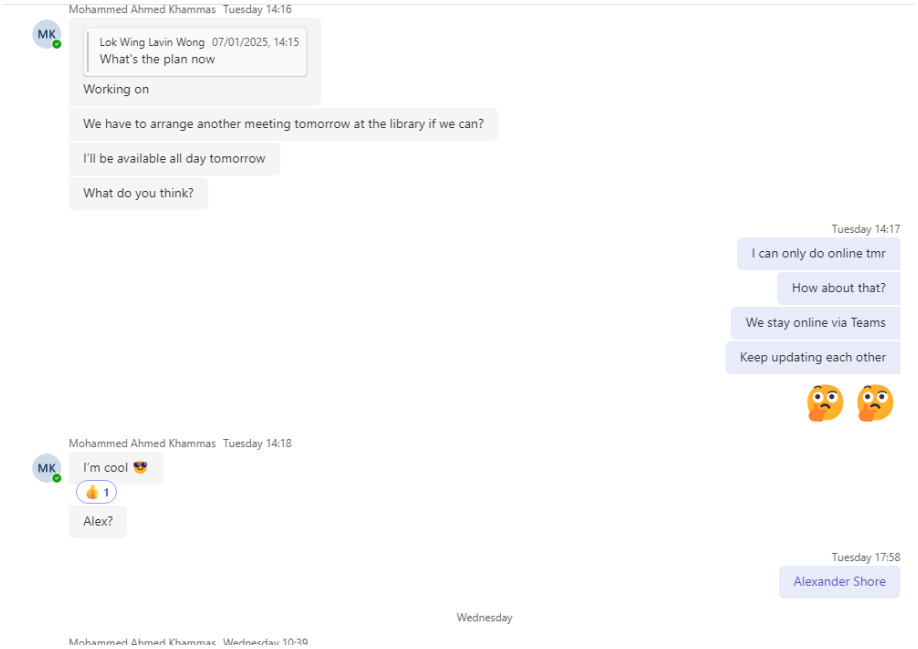

Figure 4: Teams meeting record (3)

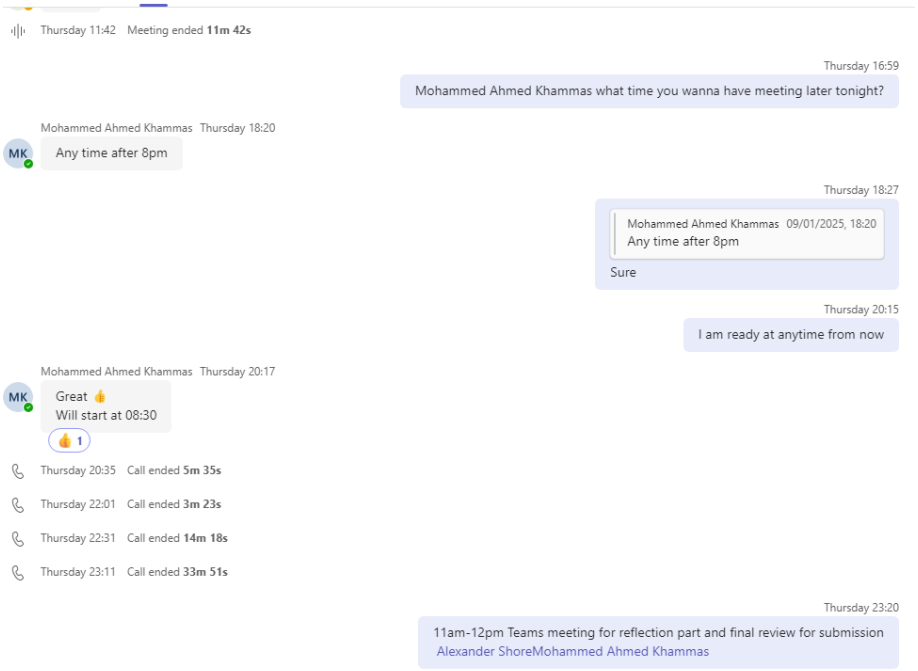

Figure 5: Teams meeting record (4)

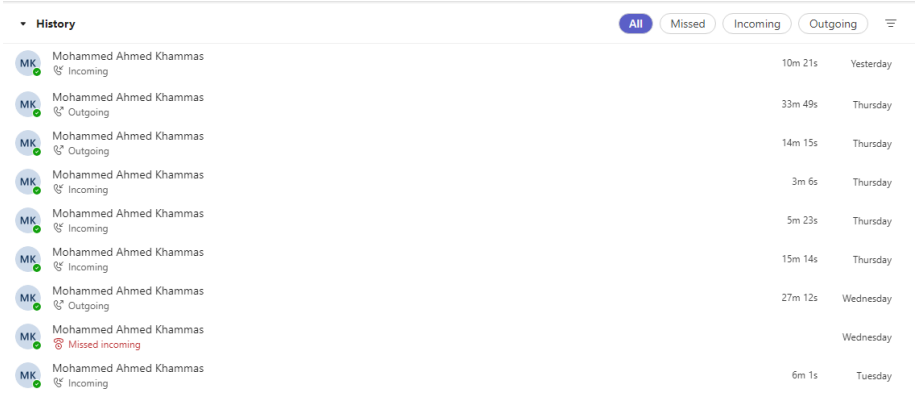

Figure 6: Teams calling history

On the other hand, we had challenges as well. One was writing organisation issue; however, it was sorted since I outlined the requirements and criteria from the assignment brief to remind my group to know that we just need to follow them to work on right track (Figure 2). I reckon that this problem came because of overthinking, however the criteria listed were for us to achieve. Also, we had several meetings including physical and online meetings to follow-up the work (Figure 1 and 3-6).

Another challenge was communication issue. During the project, one member was not actively checking the messages on Teams and there was a difficult time that we did not know how to start and reach the

conclusion part since the person did not reply, mainly only two of us interacting in the group chat. Finally, just two of us worked on the conclusion. This is a part that I am now still struggling, not just for the project, but how can it be solved if I suffer from it again in the future. I also realised that in a group work, although deadline is important, cohesion is more significant to have a person to push everyone working efficiently and to understand the importance to meet deadline, and ultimately contribute together to more effective collaboration outcomes. This is a key element that I will definitely bring into the workplace in my future.