IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received 23 January 2023, accepted 6 February 2023, date of publication 14 February 2023, date of current version 17 February 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3244883

RESEARCH ARTICLE

Autonomous Vehicles With a 6G-Based Intelligent Cybersecurity Model

ABDULLAH M. ALGARNI AND VIJEY THAYANANTHAN
Computer Science Department, King Abdulaziz University, Jeddah 21589, Saudi Arabia

Corresponding author: Abdullah M. Algarni (amsalgarni@kau.edu.sa)

This work was supported by the Deanship of Scientific Research at King Abdulaziz University, Saudi Arabia, under Grant G-601-611-39.

ABSTRACT Sixth-generation (6G)-based communications have many applications and are emerging as a new system to utilize existing vehicles and communication devices in autonomous vehicles (AVs). Electric vehicles and AVs not supporting the integration of intelligent cybersecurity will become vulnerable, and their internal functions, features, and devices providing services will be damaged. This paper presents an intelligent cybersecurity model integrating intelligent features according to the emerging 6G-based technology based on evolving cyberattacks. The model's novel design was developed using the necessary algorithms to provide quick and proactive decisions with intelligent cybersecurity based on 6G (IC6G) policies when AVs face cyberattacks. In this model, network security algorithms incorporating intelligent techniques are developed using applied cryptography. Money transaction handling services implemented in an AV are considered an example to determine the security and intelligence level depending on the IC6G policies. Intelligence, complexity, and energy efficiency (EE) are assessed. Finally, we conclude that the model results are effective for intelligently detecting and preventing cyberattacks on AVs.

INDEX TERMS 6G security, autonomous vehicles, cybersecurity attacks, intelligent transportation system, risk assessment.

I. INTRODUCTION

All future systems will be automated with intelligent connections; they will dominate all possible services and actions quickly, efficiently, and intelligently. Based on the current perspective in terms of intelligent cybersecurity, the demand for smart and intelligent feature enhancement is growing and becoming a prime concern, especially in terms of achieving maximum security with a minimum associated cost. Intelligent features aid Autonomous Vehicles (AVs) when it comes to the proper maintenance of a vehicle's vulnerable parts, and also with situations regarding reckless driving, severe accidents, lack of instructive driving, and improper decisions, which incur extra expenses for maintenance besides hindering national economic growth.

In AVs, features are added to activate autonomous functions responsible for the internal electronic devices controlling vehicle movements maneuvering, and operation. These services are affected and damage the devices when facing attacks, threats, unintelligent policies, and functional errors because some functions are connected to external services linked with external communication devices, such as sensors. Intelligent cybersecurity is an essential solution that intelligently and proactively solves many problems to secure services internally and proactively.

All AVs have insurance policies that cover usage costs associated with general wear and tear and also cover the intelligent features of these vehicles. However, there are limitations to intelligent cybersecurity based on 6G (IC6G) policies, arising from the fact that these policies must be created by intelligent experts who understand the 6G-based intelligent systems and their security issues. According to [1], the policy pathway to achieve a long-term vision reveals the details of using AVs in the future. Policy packages towards the superblock vision contain 6 themes that provide the necessary processes to improve the overall transportation regulations in the 2050 visions. Encouraging the sustainable adoption of autonomous vehicles and policies for public transport in Western countries [2] will increase economic benefits with affordable security and safety. In [1], [2], [3], [5], and [6],

The associate editor coordinating the review of this manuscript and approving it for publication was Shaohua Wan.

policies have been introduced to improve security and safety in many applications related to our research (AVs and 6G-based systems). Regarding the limitations of the IC6G policies, we must understand the licensed details of the final official release of 6G.

In this paper, we emphasize that the policies implemented are directly proportional to the intelligence level of the vehicle since all policies implemented affect the vulnerabilities of the devices used in AVs. Furthermore, the features of these AV devices should be governed by operational policies with practical limitations. Taking this into account, this work has the following objectives: (1) build an intelligent cybersecurity model that influences the policies implemented in AVs and in their devices, (2) secure the services of all devices integrated within AVs, and (3) improve the reliability of the devices, which would avoid unnecessary vulnerabilities.

The heavy use of AVs has influenced the development of many internal and external devices, such as sensors. With the increase in IC6G users, there comes an increase in the connectivity as well as the vulnerability and mobility of the devices integrated within AVs; this in turn motivates many interactions, increasing the number of unsecured communications. The motivation for this research is to minimize these issues, including overall energy consumption and cost.

When accurate policies are not delivered on time, vulnerabilities increase and the number of hacks made on a system will grow, leaving the system defenseless. For instance, decision-makers of intelligent banking systems must be able to authorize and activate the appropriate policies on time. The intelligent decision-makers of those systems must deliver the policies in a timely manner; otherwise, the services delivered by the banks will be attacked. Here, on-time means that all factors should be considered, taking into account the clients, servers, and all interfacing links and communication.

Researchers have focused on intelligent transportation systems (ITSs) using emerging technologies, including 6G. Some recommended policies are also considered to investigate the security of the services integrated within existing vehicles and AVs. ITS was developed with many policies to improve the safety of vehicles and maintain the regulations of transportation services. In recent papers, intelligent cybersecurity was also discussed with ITS to enhance security solutions of transportation services.

In our proposed approach, we used policies based on the IC6G policies. Intelligent cybersecurity focuses on improving cybersecurity solutions of AV services influenced by policies based on 6G requirements and intelligence levels, which are proportional to the strength of the policies. For instance, when the strength of the policies increases, the intelligence level in intelligent cybersecurity solutions increases as well.

This paper makes the following contributions:

1) Portrays an overview of IC6G and its associated emerging technology in autonomous vehicles,
2) Proposes a taxonomy for IC6G through an extensive literature investigation,
3) Presents a conceptual model for IC6G to motivate future researchers to enhance the level of security solutions in AVs with strength of the policies, advanced integrated devices and technology,
4) Presents a set of challenges and open research issues for the discussion of novel ideas among researchers aimed at enhancing the functions of IC6G, such as the levels of cybersecurity solutions.

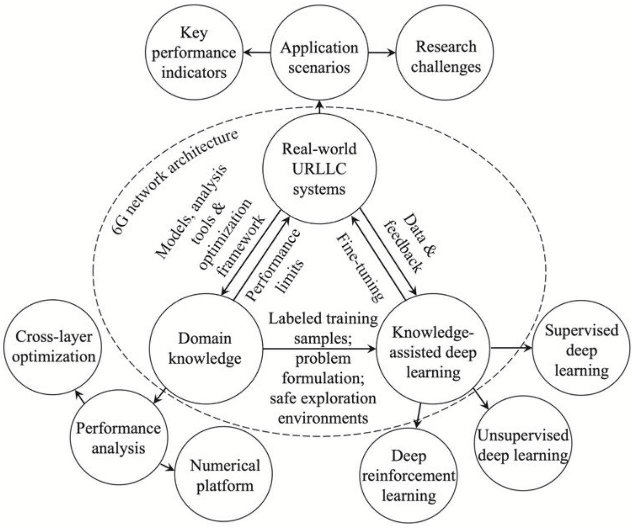

Key performance indicators
Application scenarios
Research challenges
6G network architecture
Real-world URLLC systems
Models, analysis tools & optimization framework
Performance limits
Fine-tuning
Data & feedback
Cross-layer optimization
Domain knowledge
Labeled training samples; problem formulation; safe exploration environments
Knowledge-assisted deep learning
Supervised deep learning
Performance analysis
Numerical platform
Deep reinforcement learning
Unsupervised deep learning

FIGURE 1. The road map towards URLLC in 6G networks [7].

The rest of this paper presents a scheme for managing traffic in the following sections: a literature review and related works are presented in Section II. Following that, Section III presents the proposed research, which involves the design of cybersecurity solutions, the 6G-based architecture of the proposed model, and the intelligent features necessary for autonomous vehicles. Section IV shows the relevant comparison tables and results that support this research as outlined in the contributions list. We discuss the security issues involved in AVs and intelligent management issues in Section V. Intelligent features influenced by policies and their management issues in 6G are considered in Section VI, in which a simple scenario shows the vulnerabilities and cyberattacks that can occur from poorly maintained policies. This section also includes the latest challenges and limitations facing intelligent security management. Finally, in Section VII, we provide conclusions and consider future work involving the development of AVs with intelligent, human-like vision.

II. LITERATURE REVIEW

In an AV with 6G-based intelligent systems and efficient cybersecurity, connectivity is an essential technical concept for improving secure services and infrastructure. Studying 6G networks provides the best intelligent cybersecurity security solutions.

Fig. 1 shows the road map toward 6G-based application scenarios, displaying the key performance areas of future intelligent services and the challenges in 6G networks that are part of this research's objectives. Although Enhanced Mobile Broadband (eMBB) and massive Machine Type Communications (mMTC) are important for improving services, Ultra-Reliable Low Latency Communications (URLLC) dominate 6G networks for knowledge-based analysis and optimization, knowledge-assisted training of deep learning, and fine-tuning of deep learning networks. URLLC will definitely improve services due to its low energy consumption, which will also reduce the cost of security solutions.

The authors in [8] offer a security assessment for the evolution of Vehicle-to-Everything Communications (V2X-C) architecture and the integration of 5G and 6G networks. They also provide a comparison of the Quality of Service (QoS) versus security provisions for Connected and AV (CAVs) and illustrate the safety and security enhancement mechanisms for V2X-C. A deep CNN-LSTM architecture is proposed in [9] for CAV intelligence threats and compared with other deep learning algorithms such as DNN, CNN, and LSTM.

Paper [3] proposed a System Dynamic model based on a Causal Loop Diagram that integrated the main interdisciplinary variables and evaluated the impact of the Regulation and Policy Framework (R&PF) on CAVs' cybersecurity by focusing on several aspects, such as the constraints on privacy and data accessibility.

A security model proposed in [10] for 5G satellite-connected Unmanned Aerial Vehicle (UAV) networks aims to make communication more secure, as UAVs have recently become targets for cyberattacks due to an increase in volume and low information security levels. In addition, [10] states that a huge number of UAV connections in the future will not only use 5G or 6G but will also use communication network technologies that are even more advanced. By optimizing leveraging a particle swarm [11] proposed two attacks (poisoning and evasion) versus traffic sign recognition systems in AVs based on which phase of the machine learning process is targeted during an attack.

The authors in [12] presented their perspective on an advanced and autonomous UAV traffic management (UTM) system enabled by 6G communication technology that uses non-terrestrial networks (NTNs) to improve air transportation management in terms of safety and efficiency. For a robust system, [13] uses efficient communication resources and privacy preservation learning to build a Dispersed Federated Learning (DFL) framework for 6G-enabled autonomous driving cars.

The authors in [14] also proposed 6G architecture as an integrated system, enabling technologies to provide security and intelligence. They also discussed core services, KPI, the possible technical challenges of 6G, and potential solutions. The authors in [15] give an overview of how Artificial Intelligence (AI) can solve the challenges of security and privacy of 6G networks, giving suggestions for possible solutions. A model was proposed in [16] for malicious traffic detection within 6G to develop efficiency and security at the same time.

TABLE 1. Comparison of 6G-based intelligent security issues in the AV network.

Ref.	Security Issues	Mechanism	Description
[17]	Untrusted communication in connected and autonomous vehicles	A trusted autonomous vehicle routing protocol.	The mechanism presents an efficient and trusted autonomous-vehicle-routing protocol using 6G networks.
[4]	Cyber attacks	A multi-agent reinforcement learning algorithm with a hybrid deep-anomaly detection.	The mechanism is used for autonomous vehicles in a 6G-V2X environment.
[18]	Cyber threats	A system-dynamics model with six approaches: i) CAVs communication framework, ii) secured physical access, iii) human factors, iv) CAVs penetration, v) regulatory laws and policy framework, and iv) trust—across the CAVs-industry and among the public.	A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles.
[6]	Untrusted environment and network components in AVs	Intelligent zero-trust (ZT) architecture and dynamic-trust algorithm	Introducing key ZT principles as real-time monitoring of the security state of network assets and intelligent zero-trust architecture for 5G/6G networks with machine learning utilized in the open-radio access network (O-RAN) architecture
[19]	Ransomware attack	Deep-learning-based novel ransomware detection framework	Used to secure the supervisory control and data acquisition (SCADA) in electric vehicle charging stations from ransomware attackers

Many researchers have surveyed the relevant security threats, issues, technologies, techniques, and solutions based on the future use of 6G (Tables 1 and 2). Other researchers have also surveyed several Machine Learning techniques that have been applied to vehicular communication networks, especially in terms of security, and have forecast how Artificial Intelligent (AI) will be integrated into 6G vehicular networks [23], [24].

According to the findings in [25], autonomous vehicle vulnerabilities may jeopardize autonomous services. Consequently, researchers have identified various types of autonomous vehicle attacks and their countermeasures. The authors proposed three types of attacks: autonomous control systems, autonomous driving system components, and vehicle-to-everything communications. The authors of [26] provide not only a comprehensive survey of cybersecurity but

TABLE 2. Comparisons of existing/related techniques with the appropriate parameters/variables.

Ref.	Existing/Related Techniques	Parameters/Variables
[8]	Network function virtualization (NFV) and cloud techniques	Using CAVs communication parameters, seven facets of security and safety (i.e., availability, authentication, reliability, confidentiality, integrity, robustness, and trustworthiness) for a smooth ITS operation are considered.
[9]	Deep CNN-LSTM architecture for CAV threat intelligence assessed and compared the performance of the proposed model against other deep learning algorithms, such as DNN, CNN, and LSTM.	CAV-KDD dataset, input & control data, and parameters of CAV threat landscape and intelligence are used.
[3]	Causal loop diagram-based system dynamic model is considered a technique.	Critical interdisciplinary parameters are incorporated with this model for analyzing cybersecurity.
[11]	Poisoning attacks with particle swarm optimization (PAPSO) and evasion attack with particle swarm optimization (EAPSO) are proposed as techniques.	Attacker's goal, knowledge, and capacity are used as parameters.
[13]	Block successive upper bound minimization (BSUM)-based solution proposed a technique supporting the dispersed federated learning (DFL) framework for Avs.	Simulation parameters, such as vehicular network area, number of Avs, and cellular users, are being focused on.
[14]	Emerging techniques of the 6G network are focused on 6G core services influencing intelligence.	Parameters of security issues and other 6G requirements are used to analyze the security performance and intelligence with policies.
[20]	Novel loss based on feature mapping and joint optimization network techniques is used.	Parameters, such as the camera internal, different channels, and affine transformation, are used for improving the intelligence of the Avs.
[21]	Many use cases are discussed as techniques supporting the enhancement of the research objectives, including intelligent security and optimal resource allocation policy.	Security, privacy, energy efficiency, and intelligent traffic are considered.
[22]	Federated learning (FL) of explainable artificial intelligence (XAI) models	Signal-to-interference plus noise ratio (SINR) value measured at a packet reception percentage at the frame arriving simultaneously with its display.
[4]	Hybrid deep anomaly detection (HDAD) Multi-agent reinforcement learning (MARL) algorithm Maximum entropy inverse reinforcement learning (MaxEntIRL).	Policy calculation with frequency rate, previous attack data, current attack data, and QoS parameters.
[6]	Intelligent zero trust architecture for 5G/6G networks is considered with the machine learning and RL algorithms.	Intelligent and dynamic policies are measured with security and network traffic parameters.
[19]	Novel deep learning-based ransomware detection framework with policies and regulations is used as a technique.	Layer1-Layer2 regularly applied penalties on layer parameters or layer activity during optimization.

also current countermeasure strategies for securing AVs and their services.

Another study found that the four dimensions of autonomous driving security are sensors, operating systems, control systems, and vehicle-to-everything communication [27]. Reference [28] described AV attack models and countermeasures for electronic control units (ECUs), sensors, intra-vehicular links, and inter-vehicular links.

Reference [29] provided specific details of autonomous systems to aid the development of future autonomous-mobility services. CAVs are vehicles outfitted with various internet-of-things (IoT) sensors that collect security and safety data from their surroundings. In [30], a new model for developing autonomous services is presented. The authors identified hedonic motivation, trust in AVs, and social influence on security issues as significant factors in performance expectations. Hedonic motivation is used to increase travelers' trust in automated vehicles.

A previous study [1] established a security policy pathway for the future use of AVs. Six themes are detailed in policy packages aimed at the superblock vision and the processes required to improve the overall transportation regulations described in the vision for 2050. The study [31] concentrated on the integration of intelligent transportation systems (ITS) and AV with maximum security and safety.

By 2030, cybersecurity technology for selected security issues (CVs and data communication countermeasures) for autonomous-transportation services can overcome several challenges using four countermeasures: AI-supplemented, AI-generated, AI-mediated, and AI-facilitated. AI will dominate CVs and data communication countermeasures in the next generation of AVs. Consequently, the design of self-driving vehicles must adhere to stricter standards than the ones existing [32], [33], [34], [35], [36].

The simulation results given in [37] indicate that the proposed scheme can effectively increase the network throughput for LTE-A small-cell networks with dual-connectivity

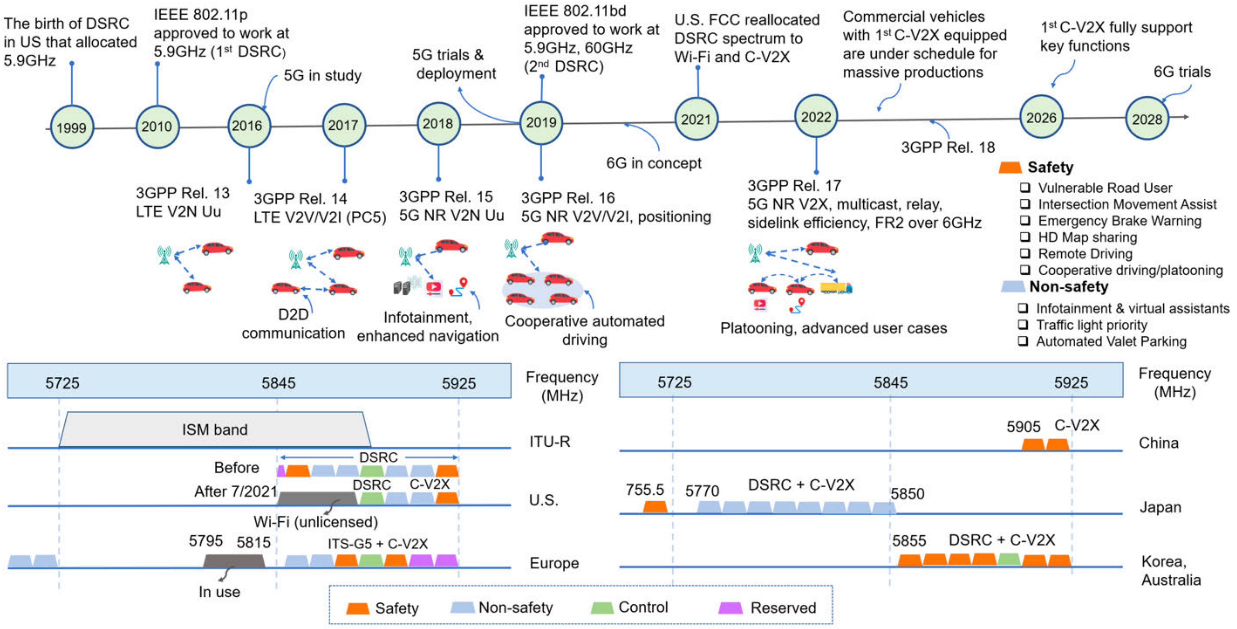

The birth of DSRC in US that allocated 5.9GHz
IEEE 802.11p approved to work at 5.9GHz (1st DSRC)
5G in study
5G trials & deployment
IEEE 802.11bd approved to work at 5.9GHz, 60GHz (2nd DSRC)
U.S. FCC reallocated DSRC spectrum to Wi-Fi and C-V2X
Commercial vehicles with 1st C-V2X equipped are under schedule for massive productions
1st C-V2X fully support key functions
6G trials
1999
2010
2016
2017
2018
2019
2021
2022
2026
2028
6G in concept
3GPP Rel. 18
3GPP Rel. 13 LTE V2N Uu
3GPP Rel. 14 LTE V2V/V2I (PC5)
3GPP Rel. 15 5G NR V2N Uu
3GPP Rel. 16 5G NR V2V/V2I, positioning
3GPP Rel. 17 5G NR V2X, multicast, relay, sidelink efficiency, FR2 over 6GHz
D2D communication
Infotainment, enhanced navigation
Cooperative automated driving
Platooning, advanced user cases
Safety
❑ Vulnerable Road User
❑ Intersection Movement Assist
❑ Emergency Brake Warning
❑ HD Map sharing
❑ Remote Driving
❑ Cooperative driving/platooning
Non-safety
❑ Infotainment & virtual assistants
❑ Traffic light priority
❑ Automated Valet Parking
5725
5845
5925
Frequency (MHz)
ISM band
ITU-R
Before
DSRC
After 7/2021
DSRC
C-V2X
U.S.
Wi-Fi (unlicensed)
5795
5815
ITS-G5 + C-V2X
Europe
In use
5725
5845
5925
Frequency (MHz)
5905
C-V2X
China
755.5
5770
DSRC + C-V2X
5850
Japan
5855
DSRC + C-V2X
Korea, Australia
Safety
Non-safety
Control
Reserved

FIGURE 2. Future of 6G safety influenced to intelligent vehicular network [21].

enhancement. In ITS, dual connectivity supports cybersecurity solutions with intelligent verification.

According to [20], the optimization of accuracy in ITS and intelligent AV (IAV) is the strongest measurement of finding a decision for technical issues and developments. Here, all calculations and measurements must be accurate, with precise values optimized through an efficient optimization method.

According to [5], with blockchain technology, examining enterprise security policy maximizes the strength of the security levels, providing a quality service when hackers' attacks affect the medical data of hospitals. Updating security policy intelligently protects the confidential data of organizations. In addition, managing an intelligent security policy allows users to address the security risks associated with the 6G generation. Building a taxonomy to enhance automotive system security [38] supports the security issues considered in vehicular networks. AI-based security solutions have also been updated with intelligent security policies to enhance automotive systems security. A congestion-aware pre-predictive data-allocation model [39] was used to improve the cooperative intelligent transportation system. This model depends on the intelligence level that can be created from predictive data management employing 6G communication and computation methods.

According to [40], 6G-based intelligent cybersecurity will lead to new techniques; some of these are given below.

1) Cryptographic hash drones are employed to enhance intelligent cybersecurity solutions in AVs and autonomous mobile systems.
2) Lightweight authentication techniques with IC6G-based policies and AI-based emerging technology, such as 6G-based complex networks
3) AI-based cybersecurity techniques with advanced security protocols based on photonic sensor networks and quantum cryptography for autonomous vehicular communication
4) Intelligent cellular technology (7G) can enhance AI-based cybersecurity solutions used in AV.

The requirement for 6G safety and intelligence of AVs will improve with the development of 6G and progress as security demands, as shown in Fig. 2.

Finally, several studies have focused on detection performance in mobile environments [2], which is important for enhancing cybersecurity, encrypting medical images against various threats when transmitting data via wireless broadcasting [41], and using deep-learning algorithms in segmentation tasks with various kinds of networks [42].

A. AUTOMATING THE ADOPTION OF MACHINE INTELLIGENCE WITH POLICIES

All systems work with standard operating policies which provide insurance to all devices and autonomous systems. By using machine-intelligent programs, policies can be maintained according to users' requirements. Adopting machine intelligence with policies will increase cybersecurity solutions since all AV user transactions must be registered. For instance, attacks using ransomware will be difficult because automation with machine intelligence will monitor all transactions intelligently with policies set by the service providers and users. These policies should be set at least 24 hours before the actual and specific transactions. Existing models use anomaly detection (Fig. 3) to improve the security of AVs. However, intelligent cybersecurity solutions can also be enhanced using anomaly detection and other rules, such as policies. Using our proposed model, users

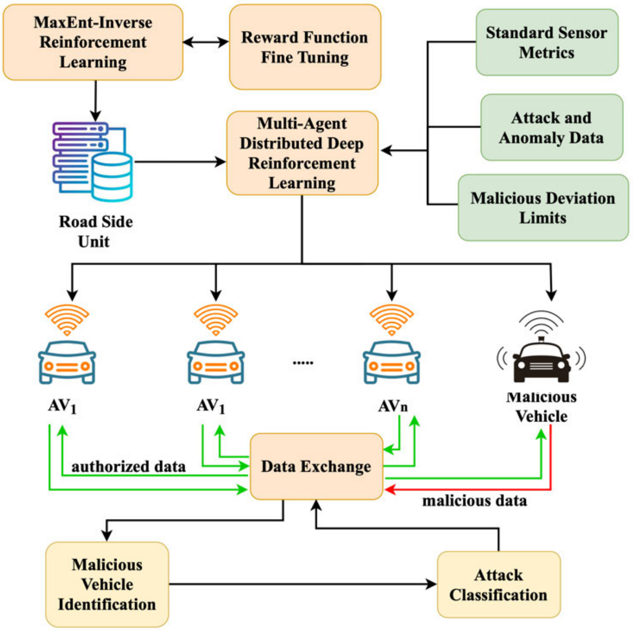

MaxEnt-Inverse Reinforcement Learning
Reward Function Fine Tuning
Standard Sensor Metrics
Attack and Anomaly Data
Multi-Agent Distributed Deep Reinforcement Learning
Malicious Deviation Limits
Road Side Unit
AV$_1$
AV$_1$
.....
AVn
Malicious Vehicle
authorized data
Data Exchange
malicious data
Malicious Vehicle Identification
Attack Classification

FIGURE 3. Workflow of hybrid deep anomaly detection approach [4].

who are vulnerable and elderly will be supported when they use AVs through strong intelligence policies. Adopting machine intelligence with emerging IC6G technologies in combination with specific policies is key to improving the future of cybersecurity solutions. Strong policies secure the public environment, which also includes the banking sector.

B. AN OVERVIEW OF INTELLIGENT CYBERSECURITY

Emerging technological trends have been focused on the many flexible features of 6G based security devices used in AV where we can add intelligent security solutions, such as intelligent cybersecurity. Attacks on the 6G architecture and 6G-based emerging networks (Fig. 4) will affect the services used in Avs if service providers do not employ the appropriate or proactive security mechanisms. Therefore, 6G architecture should be secured using a 6G-based intelligent cybersecurity model. In this paper, IC6G is portrayed with the combined features of intelligent and cybersecurity solutions for AVs. This novel usage of IC6G and its emerging technologies in AV will enhance EE and overall security performance.

As shown in Fig. 5, the following attacks illustrate the security issues in the AVs that rely on 6G-based intelligent services and cybersecurity solutions:

1) Adversarial attacks: All traffic signals and communication channels between the vehicles and service providers, such as banks, should be cleaned and secured dynamically by the AV's intelligent service providers.

2) Data poisoning: All transactions depend on data that comes from many different sources but has been cleaned for service creation. Here, an injection poisons the data and must be removed from the communication channels of V2X and AVs.

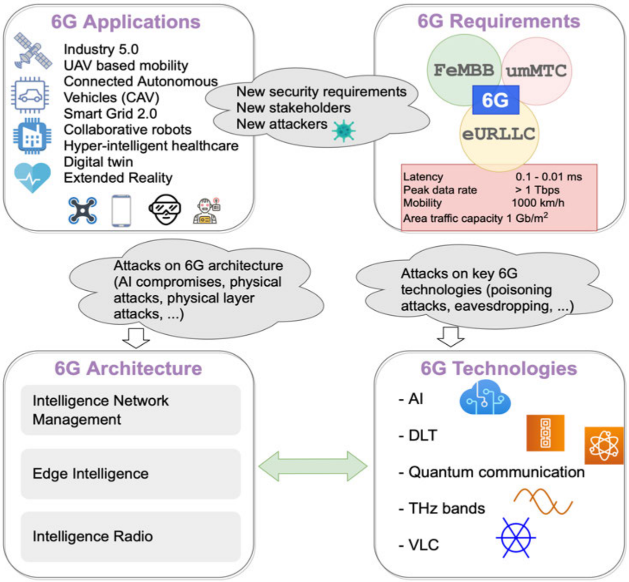


FIGURE 4. 6G landscape and security composition [43].

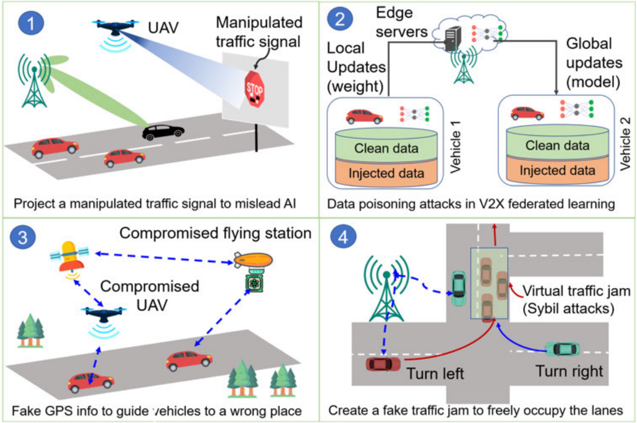

1
UAV
Manipulated traffic signal
STOP
Project a manipulated traffic signal to mislead AI
2
Edge servers
Local Updates (weight)
Global updates (model)
Clean data
Injected data
Vehicle 1
Clean data
Injected data
Vehicle 2
Data poisoning attacks in V2X federated learning
3
Compromised flying station
Compromised UAV
Fake GPS info to guide vehicles to a wrong place
4
Virtual traffic jam (Sybil attacks)
Turn left
Turn right
Create a fake traffic jam to freely occupy the lanes

FIGURE 5. An illustration of four typical security attacks in 6G V2X [29].

3) Compromised UAVs: Fake GPS information damages all services, including communication links between users.

4) Sybil attacks: Virtual traffic jams create signal interference between users. A significant attack on autonomous vehicle networks known as a (Sybil attack) occurs when an attacker maliciously assumes or steals several identities and utilizes those identities to disrupt the AVs' network's functionality by spreading fictitious identities. The research model should be able to detect these attacks and provide the best services to all AV users.

Different categories of policies and delivery times of reports influence the policies created at each level of intelligence. The following levels of intelligence prevent attacks, threats, and vulnerabilities (Table 3). These levels of intelligence provide an automation system that can adjust the machine's intelligence, allowing it to identify vulnerabilities proactively.

TABLE 3. Intelligence that depends on policies.

Intelligence Level	Policies	Description
1	Enacted according to the situation	Users' regular time, place, cost of the transaction, frequency of use, etc.
2	Ensure timely and confidential delivery of policy	Authorized items should be delivered on time with the tracking scheme (intelligent cybersecurity through management)
3	Based on the operational conditions of the devices	Technical requirements which affect IC6G, and the cybersecurity solutions integrated in AVs

III. PROPOSED RESEARCH

The communication features, services, and transactions integrated within autonomous vehicles should all be secured using the proposed model. The constant evolution of cyberattacks has been taken into account in the problem statement; as such, the proposed model should detect such attacks instantly. To resolve all possible security problems, the IC6G approach with suitable security algorithms was employed in the proposed model.

A. PROBLEM STATEMENT

AVs have one of many compulsory services involved with money transactions for automatic charges when using autonomous vehicles. Many users have reported the loss of millions of dollars after paying charges for bogus services while traveling. Hackers act as authorized persons and steal users' money, and unfortunately, banks are unable to directly stop those transactions, as they still operate under the assumption of protecting deposited money from thieves, hackers, and physical violators. The problems this creates are many, and the services established by the service providers and the providers' policies create even more cybersecurity problems, as they inadvertently support hackers. Thus, these policies should be handled intelligently and according to the situation, location, time and other major relevant factors.

In cyberattacks such as phishing, solutions with a 6G-based intelligent cybersecurity model can solve these problems intelligently and proactively. Scientists have developed many cybersecurity solutions for many illegal activities, but it is the policies that block personal interests and encourage hackers to get involved in illegal activities when they see the ease with which these transactions can be attacked.

In autonomous vehicles, the following policies are executed proactively when the system works intelligently (Table 4). When these policies are handled intelligently and with political support, each transaction can be secured. The policies enacted should protect both users and service providers from the vulnerabilities created by the communication devices used in AVs. Further, these policies should encourage service providers to make the necessary decisions proactively.

TABLE 4. Examples of policies influenced by intelligent cybersecurity.

Policies	Description
Limits should be controlled	They can be controlled by the intelligent system rather than AV users. The IC6G will have proactive security solutions
Accessing features or services with authorized codes	All services must be monitored with time, type of service, etc. Machine intelligence will record all transactions proactively
Maximum transactions per day	Intelligent systems should verify both the senders' and receivers' details. Reliance on IC6G to do so with updated policies
Proper security codes for each transaction when exceeding the limit	A receipt should be exchanged clearly with the authentication and authorization codes. Fake users will be blocked from entering any intelligent systems

Intelligent sensors placed peripherally around the AV are in direct contact with the AV's electronic devices, including the communicating transmitters and receivers. An intelligent cybersecurity model detects the vulnerabilities of these devices when they face cyberattacks and threats.

The energy consumption, E_d, is a function of several transceiver variables, with the most important variable being distance, d, and is summarized as

$$E_d = E_{sd} + \eta w d^n \tag{1}$$

In (1), E_{sd} is the distance-independent term that accounts for the overhead of radio electronics and digital processing. $\eta w d^n$ is the distance-dependent term, where η stands for the amplifier inefficiency factor, w is the free-space path loss, d is the distance, and n is the environmental factor. n can be set as a number between 2 and 4 depending on the condition of the environment and the vulnerability of devices and communication channels; η determines the inefficiency of the transmitter when producing maximum power wd^n at the antenna. Energy (E) is equal to the multiplication of power (P) and time (t).

$$EE = (E_o/E_i)100\% \tag{2}$$

Here, E_i and $E_o = E_i - E_d$ are the input and output energy, and they verify the EE of the overall model with (2). The policies and level of intelligence change, thus, verifications depend on the vulnerabilities of the devices used in the AVs. Intelligence and policies affect not only the vulnerabilities of all components integrated within the AV but also the communication channels from the AV. In this research, we assume that the input parameters of (1), (2), and (3) take different values according to the levels of policies and intelligence.

The sum capacity (E_C) is proportional to E_{sd}; we can also assume that $E_{sd} = E_C$ because the energy during secure and insecure communication is different due to many factors and influences, as given in (3).

$$E_C = \sum\nolimits_{k=1} \sum\nolimits_{i=1} B_{k,i} log_2 \left[1 + P_{k,i}/(N_{k,i} + I_{k,i})\right] \tag{3}$$

The sum capacity (E_C) of 6G-enabling technologies as given in (3) influences E_{sd} and is dependent on the network coverage (k), bandwidth (B), loss noise (N), loss

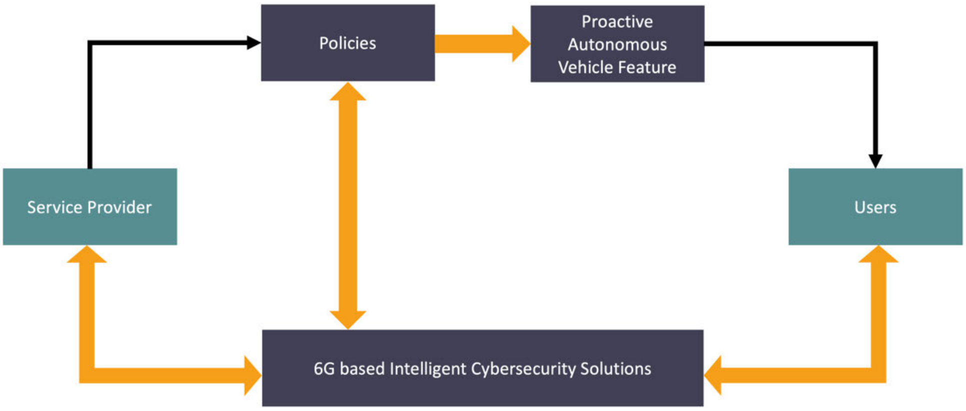

Policies
Proactive Autonomous Vehicle Feature
Service Provider
Users
6G based Intelligent Cybersecurity Solutions

FIGURE 6. The proposed model for intelligent cybersecurity solutions.

interference (I), channels (i), and power (P). Intelligent cybersecurity depends on these parameters, which work with the policies and conditions of operations adjusted according to natural attacks and internal and external security issues. When accounting for all vulnerabilities, the overhead increases with the level of intelligence, which is dependent on the operation of services, which in turn influences the policies that service providers set.

B. PROPOSED MODEL

In this research, an autonomous service is considered an example of a feature integrated within the proposed model. The proposed method used the model developed in this study, as shown in Fig. 6. In this method, intelligent cybersecurity is considered using intelligent features and the IC6G policies. The proactive AV features and IC6G-based policies considered in the proposed model were implemented in the novel design of this method. Intelligence-based policies are created from available or collected data related to intelligence-dependent services. In this study, we collected data from service users who were influenced by cyberattacks. In the 6G-based intelligent cybersecurity solution, network security algorithms incorporating intelligent techniques developed from applied cryptography were used.

All cybersecurity policies that allow service providers to secure their services will be considered in the following section, where the results will be focused on the reflection of those policies. According to (3), 6G-based intelligent cybersecurity solutions (Fig. 7) depend on the policy and conditions of the parameters used in (3).

To secure a user's identity or personal information, a Remote Procedure Call (RPC) can be used to secure remote procedures with an authentication technique. The host and the user who is requesting a service are both authenticated through the Diffie-Hellman authentication technique. Data Encryption Standard (DES) encryption is used by that authentication mechanism.

Here is a scenario: Travelers can use autonomous vehicles for short visits or other such journeys. After a long day, the user or traveler is tired and sleeps during the journey. When they finally arrive at home, they receive a call from a visa office regarding identity verification of a visa they had applied for. Tired, they take the call, not realizing that it is not genuine, and answer ''Yes'' to their questions, after which they go back to sleep. This was, in fact, a call by a hacker. The next morning, they wake up to messages from the bank, and upon checking their bank account, find that their money has been stolen by the hacker. According to the messages from the bank, 18 transactions happened during that night from that single ''Yes.'' In this situation, what are the bank's and account holders' responsibilities?

The bank should have contacted the client personally and verified the situation. If their phone was switched off or if the bank was unable to contact the person during the night, the bank should have stopped all transactions; what happens instead is that the blame is directed solely at the account holder for having said ''Yes''. In this situation, the user/traveler/account holder could not have done anything because they were unaware and asleep.

Many hackers find opportunities to attack when users or passengers of AVs transfer or pay money from their accounts to real senders or vendors. Intelligent and automated networks supported by 6G-based communication technologies enhance the cybersecurity solutions during transactions established between the 2 authorized nodes (sender and receiver). Here, 6G-based intelligent cybersecurity solutions depend on the following questions, which simplify the transactions within autonomous vehicles:

What type of AI-based cybersecurity algorithms does the proposed model use?

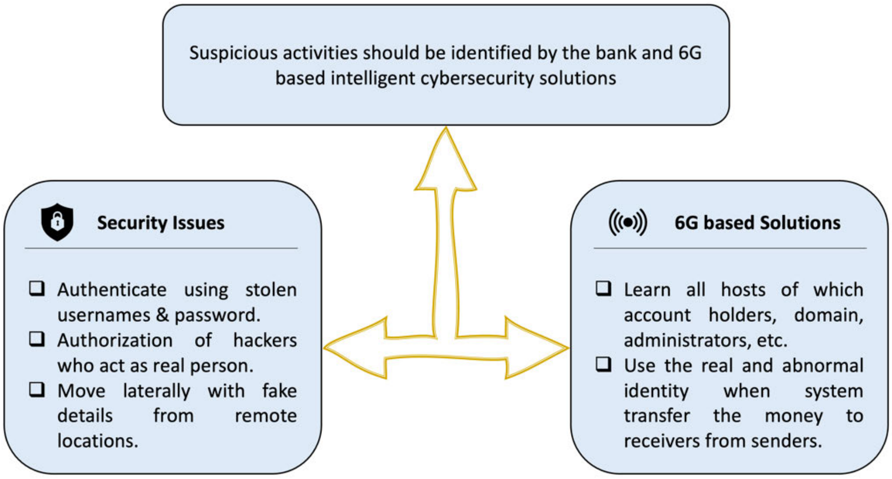
How many AI-based cybersecurity algorithms does your 6G-based intelligent cybersecurity model have?

How frequently do service providers (banks) update security policies, such as transactions limits?

How long until AI-based cybersecurity algorithms can trigger detections in each 6G-based transaction?

How many 6G-based intelligent algorithms require a learning period for normal and abnormal transactions?

How does your transaction prioritize critical and high-risk hosts that require immediate attention from the service provider or bank?



Suspicious activities should be identified by the bank and 6G based intelligent cybersecurity solutions

Security Issues

❑ Authenticate using stolen usernames & password.
❑ Authorization of hackers who act as real person.
❑ Move laterally with fake details from remote locations.

6G based Solutions

❑ Learn all hosts of which account holders, domain, administrators, etc.
❑ Use the real and abnormal identity when system transfer the money to receivers from senders.

FIGURE 7. Security issues and 6G-based intelligent cybersecurity solutions.

What is the complexity reduction that the proposed model provides for security analysts?

IV. RESULTS

The experimental setup and actual parameters for each AV should be considered in each result. Generally, security limits (High, Medium, and Low) should be set either by the experts or the intelligent approach of the systems designed by the experts. In other words, the service providers advised by these experts must provide the necessary security solutions that would allow us to update the IC6G approach considered in the AVs.

In this experiment, we collected data from 100 random users attacked by hackers from different banks. Table 5 lists the structure of the data used in this experiment. However, we have elaborated on the details of the data sizes, columns, and rows considered in this table. Moreover, 70% of bank users are attacked a few times (less than 3% of the users within a fixed time) by hackers when the security limit is set to the low bank balance of the users. In addition, 20% of bank users are attacked several times (less than 17% of the users within a fixed time) by hackers when the security limit is set to the medium bank balance of the users. Finally, 10% of bank users are attacked more times (less than 50% of the users within a fixed time) by hackers when the security limit is set to the high bank balance of the users. To improve the results, 6 random places where international banks are located were chosen when AV is moving. The average percentage of all 3 security limits when hackers' activities are involved is recorded in Table 5.

TABLE 5. Hackers' activities against autonomous vehicle users who were attacked.

	User 1	User 2	User 3	User 4	User 5	User 6
Low (70 users)	2%	2.5%	2.4%	1.9%	1.7%	1.2%
Medium (20 users)	15%	10%	11%	17%	9%	14%
High (10 users)	31%	43%	49%	27%	34%	42%

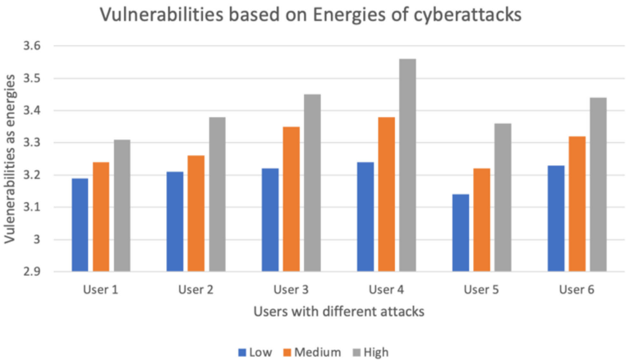


FIGURE 8. Vulnerabilities as E_d against different cyberattacks based on security limits.

The different security limits are sometimes set according to a user's earnings and preference and are set by the users. In many places, it is set by the banks or systems authorized by expert service providers. Within the current system of bank transactions for paying expenses and services, clues were left that indicated they were hacked. In these studies, people who kept their withdrawal limit low never lost their money but were still attacked in multiple ways. The people with a medium limit had mixed attacks (2% lost the money, 15% were attacked, but did not lose money) in public locations, where they were most probably targeted by expert hackers who were sacked from public organizations. People with high limits were also attacked by hackers; in those cases, a high limit was set by the service providers without the users' official authorization.

Fig. 8 shows the different security limits when an AV faces cyberattacks or threats, classified into the following categories:

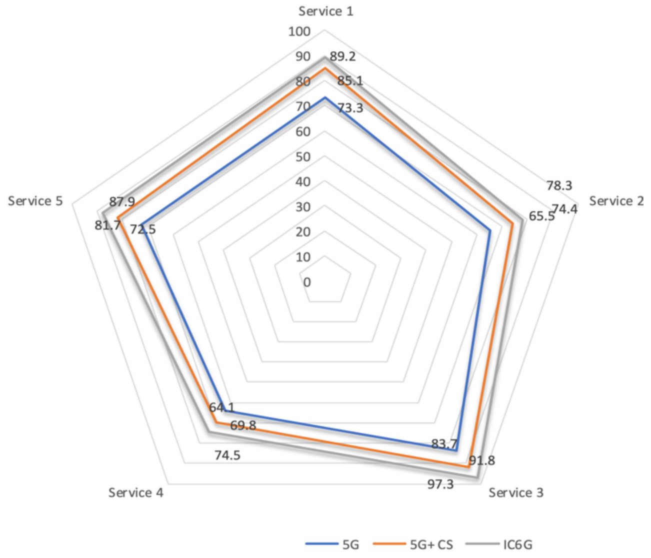


FIGURE 9. **Results of the proposed model.**

1. High limit: The threats encountered by the high limit tend to damage the configurations of the communication services, which include services such as transferring cash for users' expenses. This specific feature, integrated as AV onboard diagnostics (OBD), sends a warning when a high limit is set. The limits may be set by the bank or users or autonomous system, but they must be set intelligently and recorded with maximum evidence or verifications and/or mutual understanding of users. These recorded verifications must be kept at least a few weeks for minimizing illegal transactions. When we use the IC6G approach in autonomous vehicles, users get the correct information on verification procedures through the OBD.

2. Medium limit: These threats weaken and slow down the communication services of AVs. In all communication services, both users and service providers should be alert during the number of continuous transactions.

3. Low limit: Selected threats, such as cyberbullying, may be extracted from the profiles of users because the transaction is set to a low limit. It is the users' responsibility.

As shown in Fig. 8 and 9, the policies of the devices used in an AV will change the vulnerabilities and secrecy rate of the services, respectively. Using IC6G, the overall security facilities of an AV can be better maintained dynamically and proactively.

All policies set for improving cybersecurity solutions need to be reviewed according to the users' financial circumstances. The service providers' responsibilities should be to support all depositors who expect protection and security above other facilities.

According to [44], the parameters considered for determining vulnerabilities (Fig. 8) are proportionally equal to energy consumption, as given in (1). The parameters given in (3) are dependent on the policies of technical and operational limits which affect the sum capacity (E_C) and energy consumption (E_{sd}) of devices used in AVs.

The results of this research depend on the policies written by experts and expert systems intelligently. The management of financial transactions by AVs is seen as an illustration of an intelligent cybersecurity solution based on 6G. The proposed model's cybersecurity solutions rely on the intelligence levels which would in turn influence policies. As shown in Fig. 9, the results of the proposed model show 5 different services: banking (Service 1), ticketing (Service 2), school fees (Service 3), hospital charges (Service 4), and parking payment (Service 5). In this comparison, EE is considered for the proposed (IC6G) and 2 other (5G and 5G+ with cybersecurity (CS)) existing schemes.

Assume that all services are policy-dependent, and these policies support the levels of intelligence considered in the solutions of intelligent cybersecurity integrated with AVs.

Intelligence, security, complexity, energy efficiency, trustworthiness, scalability, and privacy were used in this study. The following explanations are provided below.

- Intelligence: Although the behavior of the same user is acceptable, intelligence can be noted from policies or keywords entered in the field of the service. Furthermore, intelligence analyzed against policies or keywords depends on the previous behaviors of users when the service is being used.
- Security: Strong policies increase the security of all services when cyberattacks occur during mobile transactions. The automation of these policy generations will improve the security of services considered in AVs with some delays, which is the trade-off between policy and security.
- Complexity: The complexity increases when users expect maximum security because there is a tradeoff between the cost of energy and security.
- Energy efficiency (EE): Analyzing the enhancement of EE with the complexity and intelligence levels and the strength of the policies is a common technique for enhancing security.
- Trustworthiness: The reputation of the packet and its trustworthiness are evaluated based on one or more of the four verifications: data quality, location of service users, time of accessing services, and travel direction of the AV.
- Scalability: The use of sensors with intelligent cybersecurity increases when more service users and AVs are involved.
- Privacy: Policies will also enhance intelligent cybersecurity because some of the data used in automated and connected vehicles are personal and sensitive.

V. DISCUSSION AND ANALYSIS

Although appropriate cybersecurity solutions are assessed in this study, the following points are noted as having a substantial impact on the outcome results, as they provide zero or minimum cybercrime, which can result in loss of control of critical equipment used in AVs. Furthermore, cybercrime attacks the warning systems responsible for services integrated into AVs. In addition, they can cause damage to human health and the environment resulting from catastrophic spills, waste discharges, and air emissions.

All results we obtained in this research depend on the limits set by the intelligent experts who provide the intelligent cybersecurity solutions to many sectors such as business. Within the business sectors, banking system is considered as an example or scenario in these results. Although many sectors and systems (medical, business, etc.) use the secure services through the intelligent cybersecurity, we have considered some selected services in this result. Intelligent cybersecurity solutions vary with the EE affected by the security limits and vulnerabilities Although 5 services are considered in the results, a specific service is to provide the necessary discussion and analysis. In some international banks and their services, the transferring procedures of the policies used in the system need to be investigated, as they are the real problem. A hacker can fool people and transfer millions of dollars ($) or Saudi riyals (SR) within a minute if the transferring policy in some international banks is not secured. For example, a hacker can act as a legal officer and ask for verification from a person who has paid visa fees from their account to an official account. The average person trusts third parties in many situations and circumstances to enact such payments. Intelligent experts and systems should have some procedures which depend on the policies, steps, and evidence collected from banks. To design and develop the intelligent procedure, the following evidence is collected from the bank:

- The receiver's account details were not properly checked; the receiver can open the account and delete the account without references.
- The senders' confirmation must be verified personally for securing the transactions.
- The bank must have the proper verifications before sending the one-time password.
- Account holders must trust the banks, but banks must not trust the receivers without proper verifications.
- The bank should make sure that the receiver's account number is active for at least the last 3 months and valid for at least the next 3 months after the transactions.

Among the many services used in AVs, communication services are deployed for users who would like to communicate or exchange online transactions when they pay for their expenses during a journey. Users should be able to use the services (banking, ticketing, schooling (Tuition and other fees for academic services), etc.) comfortably and securely. In this discussion, 5 different services are considered, as previously mentioned: services 1, 2, 3, 4, and 5, banking, ticketing, school fees, hospital charge, and parking payment, respectively. When we deploy the IC6G approach in our proposed model, all 5 services are improved because policies are set up intelligently according to users' financial situation and transaction history. Whatever the situation, one of all 3 security limits should be selected and issued intelligently, instantly, and dynamically by the service provider. If the account holder's phone is switched off, but the bank has allowed the hackers to transfer money (the bank should have waited until verbal confirmation from the account holder).

In this discussion, the evidence mentioned above should be considered carefully to improve security when transferring or withdrawing money from an account. In addition, we proposed a model with solutions using the IC6G-based policies to prevent cyberattacks and cybercrimes. The bogus services during movement, unintelligent behaviors, and the interruption of the handling services attacked by hackers are the problems discussed in this study. Intelligence levels were obtained from the policies concluded by the previous behaviors of the users of the services. We solved the research problem by analyzing intelligence levels with these policies.

VI. CHALLENGES AND LIMITATIONS

The AVs with an IC6G will have many challenges which affect the users' daily life. The architecture we proposed in this research will present new opportunities for many potential systems and future applications:

- Autonomous vehicles' basic and luxury features will influence 6G-based gadgets.
- An introduction of cybersecurity solutions in 6G networks and related platforms used in autonomous vehicles.
- An increase in intelligent features and proactive cybersecurity solutions.

The above points will spur research that support improving transportation policies.

Brain Controlled Vehicles (BCV) may be introduced for simplifying the operations of the devices used in autonomous systems, including AVs. Further, the functions of 6G networks will make BCVs possible and will support IC6G in improving the intelligent features of the AVs.

Regarding the cost of energy and intelligent cybersecurity, the most challenging aspect of cost and EE is determining the trade-off between five aspects:

i. Evolution of AV technology
ii. Access to AV technology by stakeholders (communication service providers, road operators, automakers, AV consumers, repairers, and the general public)
iii. Limiting hackers' access to AV technology
iv. Widespread dynamic strategy for avoiding hacker amplification
v. Efficient usage of AV operating logfiles [45].

According to [46] and [47], tons of CO2 emissions and millions of hours of driving every year will be saved with AVs, creating vulnerabilities in the communication devices used in those AVs. To solve these challenges, we need tough security policies that need to be applied intelligently. Our research model and approach provide a basic idea: intelligent cybersecurity with machine learning and AI algorithms should be considered to solve these problems. Intelligent cybersecurity with UAVs may offer some unique security challenges to 6G networks, especially regarding AVs used on land; it is possible that advances in UAV will lead to AVs getting low-cost energy and security.

The strength of this work lies in the IC6G policies, which should be the best for improving cybersecurity solutions because these policies are generated from the users' behaviors noted in each previous handling of the services.

For instance, the limits and changes in bank transactions in banking services are noted to generate policies.

On the other hand, the weakness and limitations of the research lie in the collection of previous behaviors for the last 7 days to 3 months, which will increase the time complexity and storage, creating unnecessary delays when services are being used during the transactions. In addition, there are several other limitations regarding the cost of energy and intelligent cybersecurity for users and others: the collection of confidential data and generated policies depends on the behavior of the previous history of the services allocated in the Avs and regarding the importance of licensed details of the final official 6G release in relation to the IC6G-based policies.

VII. CONCLUSION AND FUTURE WORK

This study presented the results from the proposed model that might be effective for intelligently detecting and thwarting cyberattacks on AVs and intelligent cybersecurity solutions that maintain secure services from all vulnerabilities created by attackers, faulty devices, or fake messages.

Policies developed for AVs should enhance the protection of all users and communication devices integrated within the Avs. When securing service policies are maintained by intelligent experts, both users and service providers can secure services using a proactive approach. As the strength of the policies increases, the intelligence level also provides more intelligent cybersecurity solutions.

Therefore, the security limits discussed in the results should be set and fit by service providers based on the situation and important security factors, such as authentication.

The main contribution of the proposed approach is intelligent cybersecurity solutions that provide the necessary security to all services used in AVs when cyberattacks occur. Furthermore, cyberattacks affect the electronic functions of AVs, which damage the AVs' operations and maneuvering of vehicle movements. The influence of intelligent cybersecurity not only solves the AVs safety issues of electronic control systems, but also provides secure services to passengers using the AV.

Insights from this study are provided through the proposed model, which includes 6G-based cybersecurity solutions and policies. Intelligent cybersecurity is considered to maximize security and minimize energy costs for all passengers using autonomous and mobile services while traveling. The proposed solutions use IC6G-based policies to prevent cyberattacks and cybercrimes and intelligently enhance the effectiveness of cybersecurity solutions.

In this paper, previous researchers and authors provided an overview of IC6G and the related emerging technology in autonomous vehicles, proposed a taxonomy for IC6G through a thorough literature review, presented a conceptual model for IC6G to improve the level of security solutions in AVs with cutting-edge integrated devices and technology, and presented the challenges and issues for the discussion of novel IC6G applications.

Furthering the work of the proposed model, we can add more features and services to keep up with the emerging security technology as long as it is suitable for the situation and environmental conditions. Securing future services with intelligent cybersecurity in AVs will depend on emerging security technology (7G) and the strength of policies at the time. Furthermore, these features and services depend on energy-efficient algorithms and emerging technologies considered at the time. This research will continue to develop AVs with intelligent vision and 'human-like' thinking capabilities.

ACKNOWLEDGMENT

This project was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, under grant no. G-601-611-39. The authors, therefore, gratefully acknowledge with thanks the DSR for technical and financial support.

REFERENCES

[1] E. Vitale Brovarone, J. Scudellari, and L. Staricco, "Planning the transition to autonomous driving: A policy pathway towards urban liveability," *Cities*, vol. 108, Jan. 2021, Art. no. 102996.

[2] Y. Wu, H. Guo, C. Chakraborty, M. Khosravi, S. Berretti, and S. Wan, "Edge computing driven low-light image dynamic enhancement for object detection," *IEEE Trans. Netw. Sci. Eng.*, early access, Feb. 14, 2022, doi: 10.1109/TNSE.2022.3151502.

[3] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and M. Warren, "Dynamic assessment of regulation and policy framework in the cybersecurity of connected and autonomous vehicles," in *Proc. Australas. Transp. Res. Forum (ATRF)*, 2021, pp. 1–14.

[4] S. B. Prathiba, G. Raja, S. Anbalagan, K. S. Arikumar, S. Gurumoorthy, and K. Dev, "A hybrid deep sensor anomaly detection for autonomous vehicles in 6G-V2X environment," *IEEE Trans. Netw. Sci. Eng.*, early access, Jul. 4, 2022, doi: 10.1109/TNSE.2022.3188304.

[5] M. A. Nafchi and Z. A. Shahraki, "IT governance and enterprise security policy in the 6G era," in *Next-Generation Enterprise Security and Governance*. Boca Raton, FL, USA: CRC Press, 2022, pp. 227–245.

[6] K. Ramezanpour and J. Jagannath, "Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN," *Comput. Netw.*, vol. 217, Nov. 2022, Art. no. 109358.

[7] C. She, C. Sun, Z. Gu, Y. Li, C. Yang, H. V. Poor, and B. Vucetic, "A tutorial on ultrareliable and low-latency communications in 6G: Integrating domain knowledge into deep learning," *Proc. IEEE*, vol. 109 no. 3, pp. 204–246, Mar. 2021.

[8] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and M. Warren, "Security assessment in vehicle-to-everything communications with the integration of 5G and 6G networks," in *Proc. Int. Symp. Comput. Sci. Intell. Controls (ISCSIC)*, Nov. 2021, pp. 154–158.

[9] M. Basnet and M. Hasan Ali, "A deep learning perspective on connected automated vehicle (CAV) cybersecurity and threat intelligence," 2021, *arXiv:2109.10763*.

[10] R. Shrestha, A. Omidkar, S. A. Roudi, R. Abbas, and S. Kim, "Machine-learning-enabled intrusion detection system for cellular connected UAV networks," *Electronics*, vol. 10, no. 13, p. 1549, Jun. 2021.

[11] W. Jiang, H. Li, S. Liu, X. Luo, and R. Lu, "Poisoning and evasion attacks against deep learning algorithms in autonomous vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4439–4449, Apr. 2020.

[12] R. Shrestha, R. Bajracharya, and S. Kim, "6G enabled unmanned aerial vehicle traffic management: A perspective," *IEEE Access*, vol. 9, pp. 91119–91136, 2021.

[13] L. U. Khan, Y. Kyaw Tun, M. Alsenwi, M. Imran, Z. Han, and C. Seon Hong, "A dispersed federated learning framework for 6G-enabled autonomous driving cars," 2021, *arXiv:2105.09641*.

[14] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6G: Opening new horizons for integration of comfort, security, and intelligence," *IEEE Wireless Commun.*, vol. 27, no. 5, pp. 126–132, Oct. 2020.

[15] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "AI and 6G security: Opportunities and challenges," in *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, Jun. 2021, pp. 616–621.

[16] H. Ghorbani, M. S. Mohammadzadeh, and M. H. Ahmadzadegan, "Modeling for malicious traffic detection in 6G next generation networks," in *Proc. Int. Conf. Technol. Entrepreneurship-Virtual (ICTE-V)*, Apr. 2020, pp. 1–6.

[17] K. Haseeb, A. Rehman, T. Saba, S. A. Bahaj, H. Wang, and H. Song, "Efficient and trusted autonomous vehicle routing protocol for 6G networks with computational intelligence," *ISA Trans.*, vol. 132, pp. 61–68, Jan. 2023.

[18] S. Khalid Khan, N. Shiwakoti, and P. Stasinopoulos, "A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles," *Accident Anal. Prevention*, vol. 165, Feb. 2022, Art. no. 106515.

[19] M. Basnet, S. Poudyal, M. H. Ali, and D. Dasgupta, "Ransomware detection using deep learning in the SCADA system of electric vehicle charging station," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf.-Latin Amer. (ISGT Latin America)*, Sep. 2021, pp. 1–5.

[20] Y. Gao, F. Tian, J. Li, Z. Fang, S. Al-Rubaye, W. Song, and Y. Yan, "Joint optimization of depth and ego-motion for intelligent autonomous vehicles," *IEEE Trans. Intell. Transp. Syst.*, early access, Mar. 24, 2022, doi: 10.1109/TITS.2022.3159275.

[21] V.-L. Nguyen, R.-H. Hwang, P.-C. Lin, A. Vyas, and V.-T. Nguyen, "Towards the age of intelligent vehicular networks for connected and autonomous vehicles in 6G," *IEEE Netw.*, early access, Sep. 12, 2022, doi: 10.1109/MNET.010.2100509.

[22] A. Renda, P. Ducange, F. Marcelloni, D. Sabella, M. C. Filippou, G. Nardini, G. Stea, A. Virdis, D. Micheli, D. Rapone, and L. G. Baltar, "Federated learning of explainable AI models in 6G systems: Towards secure and automated vehicle networking," *Information*, vol. 13, no. 8, p. 395, 2022.

[23] F. Tang, Y. Kawamoto, N. Kato, and J. Liu, "Future intelligent and secure vehicular network toward 6G: Machine-learning approaches," *Proc. IEEE*, vol. 108, no. 2, pp. 292–307, Feb. 2020.

[24] P. Porambage, G. Gur, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6G security and privacy," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1094–1122, 2021.

[25] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, and H. K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense," *Comput. Secur.*, vol. 103, Apr. 2021, Art. no. 102150.

[26] X. Sun, F. R. Yu, and P. Zhang, "A survey on cyber-security of connected and autonomous vehicles (CAVs)," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 6240–6259, Jul. 2022.

[27] C. Gao, G. Wang, W. Shi, Z. Wang, and Y. Chen, "Autonomous driving security: State of the art and challenges," *IEEE Internet Things J.*, vol. 9, no. 10, pp. 7572–7595, May 2022.

[28] M. C. Chow, M. Ma, and Z. Pan, "Attack models and countermeasures for autonomous vehicles," in *Intelligent Technologies for Internet of Vehicles*. Cham, Switzerland: Springer, 2021, pp. 375–401.

[29] T. Campisi, A. Severino, M. A. Al-Rashid, and G. Pau, "The development of the smart cities in the connected and autonomous vehicles (CAVs) era: From mobility patterns to scaling in cities," *Infrastructures*, vol. 6, no. 7, p. 100, 2021.

[30] M. A. Ribeiro, D. Gursoy, and O. H. Chi, "Customer acceptance of AVin travel and tourism," *J. Travel Res.*, vol. 61, no. 3, pp. 620–636, Mar. 2022.

[31] A. Aldakkhelallah and M. Simic, "AVin intelligent transportation systems," in *Proc. Int. Conf. Hum.-Centered Intell. Syst.* Singapore: Springer, 2021, pp. 185–198.

[32] V. Thayananthan. *Advanced Security Issues of IoT Based 5G Plus Wireless Communication for Industry 4.0*. Accessed: Jan. 5, 2023. [Online]. Available: https://novapublishers.com/shop/advanced-security-issues-of-iot-based-5g-plus-wireless-communication-for-industry-4-0/

[33] R. A. Shaikh and V. Thayananthan, "Trust evaluation wireless network for routing data packets," U.S. Patent 10 225 708 B2, Mar. 5, 2019. [Online]. Available: https://patents.google.com/patent/US10225708B2

[34] A. Algarni and V. Thayananthan, "Improvement of 5G transportation services with SDN-based security solutions and beyond 5G," *Electronics*, vol. 10, no. 20, p. 2490, Oct. 2021.

[35] R. A. Shaikh and V. Thayananthan, "Risk-based decision methods for vehicular networks," *Electronics*, vol. 8, no. 6, p. 627, Jun. 2019.

[36] V. Thayananthan and J. Yazdani, *Secure Cyber-Physical Systems for Improving Transportation Facilities in Smart Cities and Industry 4.0*. Hershey, PA, USA: IGI Global, 2019.

[37] M.-S. Pan, T.-M. Lin, C.-Y. Chiu, and C.-Y. Wang, "Downlink traffic scheduling for LTE—A small cell networks with dual connectivity enhancement," *IEEE Commun. Lett.*, vol. 20, no. 4, pp. 796–799, Apr. 2016.

[38] A. Haddaji, S. Ayed, and L. C. Fourati, "Artificial intelligence techniques to mitigate cyber-attacks within vehicular networks: Survey," *Comput. Electr. Eng.*, vol. 104, Dec. 2022, Art. no. 108460.

[39] G. Manogaran, I. Alrayes, A. Alshaikhi, and D. B. Rawat, "Pre-predictive congestion-based data allocation for sixth generation cooperative intelligent transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 10, pp. 18655–18667, Oct. 2022.

[40] A. S. Khan, M. A. Sattar, K. Nisar, A. A. A. Ibrahim, N. B. Annuar, J. B. Abdullah, and S. Karim Memon, "A survey on 6G enabled light weight authentication protocol for UAVs, security, open research issues and future directions," *Appl. Sci.*, vol. 13, no. 1, p. 277, Dec. 2022.

[41] Y. Wu, L. Zhang, S. Berretti, and S. Wan, "Medical image encryption by content-aware DNA computing for secure healthcare," *IEEE Trans. Ind. Informat.*, vol. 19, no. 2, pp. 2089–2098, Feb. 2023.

[42] G. Shi, Y. Wu, J. Liu, S. Wan, W. Wang, and T. Lu, "Incremental few-shot semantic segmentation via embedding adaptive-update and hyper-class representation," in *Proc. 30th ACM Int. Conf. Multimedia*, Oct. 2022, pp. 5547–5556.

[43] P. Porambage, G. Gur, D. P. Moya Osorio, M. Livanage, and M. Ylianttila, "6G security challenges and potential solutions," in *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, Jun. 2021, pp. 622–627.

[44] N. F. Mir, *Computer and Communication Networks*, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2015.

[45] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and W. Matthew, "Governing connected and automated vehicles: Cybersecurity regulations and operational framework," Australas. Transp. Res. Forum, Australia, Tech. Rep., 2022.

[46] D. P. Moya Osorio, I. Ahmad, J. D. V. Sanchez, A. Gurtov, J. Scholliers, M. Kutila, and P. Porambage, "Towards 6G-enabled internet of vehicles: Security and privacy," *IEEE Open J. Commun. Soc.*, vol. 3, pp. 82–105, 2022.

[47] M. S. Obaid, "Macroscopic modelling of the effects of autonomous vehicles and cooperative intelligent transport systems," Ph.D. dissertation, Budapest Univ. Technol. Econ., Hungary, 2022.

ABDULLAH M. ALGARNI received the master's degree in software systems engineering from The University of Melbourne, Australia, in 2008, the master's degree in computer science from Colorado State University, in 2014, and the Ph.D. degree in computer science from the College of Natural Sciences, Colorado State University, Fort Collins, CO, USA, in 2016. He is currently an Associate Professor with the Computer Science Department, King Abdulaziz University, Jeddah, Saudi Arabia. His research interests include software engineering, software security, and cybersecurity.

VIJEY THAYANANTHAN received the Ph.D. degree in engineering, communication systems from Lancaster University, U.K., in 1998. Since 2000, he has been working as a Research Engineer and a Senior Algorithm Development Engineer with Advantech Ltd., Southampton University Science Park, U.K., and Amfax Ltd., U.K. He worked with the Department of Electrical and Electronic Engineering, University of Strathclyde, Glasgow, U.K. as a Postdoctoral Research Fellow. He is currently a Professor with the Computer Science Department, King Abdulaziz University, Jeddah, Saudi Arabia. His research interests include wireless networks, cybersecurity, and information theory and coding. He is a member of the IET. He is a Reviewer of various international journals, such as *Journal of Fundamentals of Renewable Energy and Applications*, *Mobile Networks and Applications*, and Springer book chapters. He is also a Chartered Engineer (CEng).