International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

6G-Based Intelligent Cybersecurity Model for Autonomous Vehicles

[1] N. Pravin, [2]Dr. P. Sukumar M.E., Ph.D

[1]PG Scholar, Department of Computer Science and Engineering, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India
[2]Associate Professor, Department of Computer Science and Engineering, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India

ABSTRACT

In the Sixth Generation (6G) mobile system, the importance of security increases even more in the communication system. A comprehensive set of security technology enablers will be critically required for communication systems for the 6G era of the 2030s.The future 6G network is predicted to be implemented with artificial intelligence-driven communication via machine learning, enhanced edge computing, post-quantum cryptography and so forth. The vision of 6G incorporates new radio frequencies and technologies, the integration of sensing, cognitive methods defining both network functions and their management, and new networking approaches for a broader scope of applications and distribution. This paper aims to use 6G Network.6G ecosystems are considered a platform conducive to innovations in computing, artificial intelligence, connectivity and sensors, virtualization, and more. It is designed to meet the requirements of higher global coverage, greater spectral efficiency, and a reduced carbon footprint, emphasizing sustainability, equity, trust, and security through unprecedented architectural evolutions and technology. 6G will be an integrated network system that includes a traditional terrestrial mobile network, space network, and underwater network to provide ubiquitous network access. Even if studies on the vision of the 6G network have already been published, there is still a significant amount of ground to cover. There is no decision made yet regarding anything, and nothing has been ruled out. The focus of this study is to identify a complete picture of changes in architectures, technologies, and challenges that will shape the 6G network. The research results will provide indications for further studies on 6G ecosystems. The results of this review contribute to previous research on 6G network security.

KEYWORDS: 6G Networks, 6G-Based Intelligent Cybersecurity, 6G Management, 6G-Based Industrial Applications, 6G Mobile Networks, 6G Security.

1. INTRODUCTION

1.1 6G NETWORK

However, 5G will not meet all requirements of the future in 2030+. Researchers now start to focus on the sixth generation (6G) wireless communication networks. One of the main distinguishing features of 5G is low latency or more specifically guaranteed (deterministic) latency, which needs deterministic networking (DetNet) to guarantee end-to-end latency with punctuality and accuracy that future use cases demand. The 6G will have additional requirements of high time and phase synchronization accuracy beyond what 5G can deliver. Additionally, 6G will have to provide near 100% geographical coverage, sub-centimeter geo-location accuracy and millisecond geo-location update rate to meet use cases.

1.2 Performance Metrics and Application Scenarios

6G networks are expected to achieve superior performance and have more performance metrics, as illustrated. The peak data rate for 5G is 20 Gbps, while for 6G networks it can be 1–10 Tbps with the aid of THz and optical frequency bands. The user experienced data rate can achieve a Gbps-level with these high frequency bands. The area traffic capacity can be more than 1 Gbps/m2. The spectrum efficiency can increase 3–5 times, while the network energy efficiency must increase by more than 100 times compared to 5G to make-up for the increase in data rate by 100 times. This can be achievable by applying AI to achieve much better network management and automation. The connection density will increase 10–100 times due to the use of extremely heterogeneous networks, diverse communication scenarios, large numbers of antennas, and wide bandwidths. There are multiple types of mobility introduced by satellites, UAVs, and ultra-high-speed trains, which can move with a much higher speed of larger than 500 km/h in comparison to the existing terrestrial terminals. For a selected set of applications, the latency is expected to be less than 1 ms. In addition, other important performance metrics should be introduced, e.g., cost efficiency, security capacity, coverage, intelligence level, etc.**Example Industry Verticals**

The current 5G wireless communication networks have shown the possibility to be the `fundamental infrastructure of modern information society. There have been some potential industry verticals based on 5G networks and it will be deepened in future 6G networks. Here we emphasize on example industry verticals, including cloud VR, IoT industry automation, C-V2X, digital twin body area network, and energy efficient wireless network control and federated learning systems.

1.3 Cloud VR

VR technology has been employed in several professional verticals such as education, healthcare, military [13–16] and so on over the last few years. Since VR provides great immersive and interactive experiences by breaking through cost and risk constraints in the physical world, it has significant potential to reshape our daily life and work eventually. Since VR is a computer-generated world, computing power is one of the key requirements for immersive experiences. Despite small scale solutions already exist today, there are several crucial challenges which should be improved towards 6G era. We summarize the most important aspect as follows. Firstly, cloud VR platforms require the usage of mobile edge computing (MEC) with expensive accelerators which lead to high investment cost. Secondly, the cloud VR services require extremely low latency which is a key challenge for better customer experience. Last but not least, the cloud VR architecture allows the research community to optimize the processing pipeline. To solve the problems, a thorough understanding and exploration of existing academic and industrial research and development can help to improve the cloud VR system towards 6G.

1.4 Evolution of 6G

The New 6G applications will have more requirements and a greater network capacity than the current 5G networks. As a result, new 6G applications will need a more extensive network capacity than 5G networks. Next-generation wireless networks will be one of the significant components in our future lifestyles, industries, and societies. Wireless networks will be the link between humans and intelligent machines. The 2030 era will witness a considerable improvement in wireless communication. Future communication should have fundamental divers: systems trustworthiness; sustainability of devices efficiency, automatization and digitalization for a simplified life, and limitless connectivity to satisfy application demands. It is expected that this era will have a great transformation towards automatization, where 6G will play a vital role as a communication and information backbone. 6G should allow anything to communicate anywhere and anytime.

1.5 New scenarios of 6G beyond 2030

New application scenarios will continue to rise until 2030. The scenarios are divided into three categories: intelligent production, intelligent life, and intelligent society.

- **Smart Production**: The digital economy might overgrow by applying developing technology to agriculture and industry.6G will achieve intelligent manufacturing via information. For example, drones are utilized in agriculture. Robotics and virtual reality will boost production efficiency. With modern technologies like digital twins, 6G will have more significant intelligent manufacturing.
- **Smart Life**: Twin body area network Synesthesia internet and intelligent interaction will likely transform our lives in 2030.
- **Smart Society:** The ubiquitous coverage network in 2030 will considerably extend public service coverage, bridging the digital divide between areas. Overall, a 6G network will strengthen social governance and provide a firm basis for a better society.

2. LITERATURE REVIEW

2.1 Towards 6G-Enabled Internet of Vehicles: Security and Privacy

The conceptualization of the 6th era of versatile remote systems (6G) has as of now begun with a few potential troublesome advances resounding as enablers for driving the rise of a number of imaginative applications. Especially, 6G will be a conspicuous supporter for the advancement towards a really Brilliantly Transportation Framework and the realization of the Keen City concept by satisfying the confinements of 5G, once vehicular systems are getting to be profoundly energetic and complex with exacting necessities on ultra-low idleness, tall unwavering quality, and gigantic associations. More vitally, giving security and security to such basic frameworks ought to be a beat need as vulnerabilities can be disastrous, hence there are colossal concerns with respect to information collected from sensors, individuals and their propensities. In this paper, we offer a opportune consideration of the part that promissory 6G empowering innovations such as manufactured insights, organize softwarisation, arrange cutting, piece chain, edge computing, shrewdly reflecting surfaces, backscatter communications, terahertz joins, unmistakable light communications, physical layer verification, and cell-free gigantic multiple-input multiple-output (MIMO) will play on giving the anticipated level of security and protection for the Web of Vehicles

2.2 Proactively Predicting Dynamic 6G Link Blockages Using LiDAR and In-Band Signatures

1. Line-of-sight interface blockages speak to a key challenge for the unwavering quality and idleness of millimeter wave (mmWave) and terahertz (THz) communication systems. To address this challenge, this paper leverages mmWave and LiDAR tactile information to supply mindfulness almost the communication environment and proactively foresee energetic interface blockages some time recently they happen. This allows the organize to create proactive choices for hand-off/beam exchanging, improving the arrange unwavering quality and idleness. More particularly, this paper addresses the taking after key questions: (i) Can we foresee a line-of-sight connect blockage, some time recently it happens, utilizing in-band mmWave/THz flag and LiDAR detecting information? (ii) Can we moreover anticipate when this blockage will happen? (iii) Can we anticipate the blockage length? And (iv) can we foresee the heading of the moving blockage? For that, we create machine learning arrangements that learn extraordinary designs of the gotten flag and tactile information, which we call pre-blockage marks, to induce

future blockages. To assess the proposed approaches, we construct a large-scale real-world dataset that comprises co-existing LiDAR and mmWave communication estimations in open air vehicular scenarios. At that point, we create an effective LiDAR information denoising calculation that applies a few pre-processing to the LiDAR information. Based on the real-world dataset, the created approaches are appeared to attain over 95% exactness in anticipating blockages happening inside 100 ms and more than 80% forecast precision for blockages happening inside one moment. Given this future blockage expectation capability, the paper moreover appears that the created arrangements can accomplish an arrange of greatness sparing in organize inactivity, which advance highlights the potential of the created blockage forecast arrangements for remote systems.

2.3 The Roadmap to 6G Security and Privacy

1. Visionaries of the 6th era (6G) resound frameworks have as of now come into the discourse. Hence, in arrange to solidify and set the security and protection in 6G systems, we overview how security may affect the imagined 6G remote frameworks, conceivable challenges with distinctive 6G advances, and the potential arrangements. We offer our vision on 6G security and security key execution pointers (KPIs) w/ith the conditional risk scene based on the predicted 6G organize engineering. In addition, we examine the security and protection challenges which will experience with the accessible 6G prerequisites and potential 6G applications. We moreover grant the peruser a few experiences into the standardization endeavors and research-level ventures important to 6G security. In specific, we examine the security contemplations with 6G empowering innovations such as conveyed record innovation (DLT), physical layer security, disseminated AI/ML, obvious light communication (VLC), THz, and quantum computing. All in all, this work extreme to supply edifying direction for the consequent inquire about of 6G security and security at this beginning stage of vision towards reality.

2.4 A Continuous Actor–Critic Deep Q-Learning-Enabled Deployment of UAV Base Stations: Toward 6G Small Cells in the Skies of Smart Cities

Unscrewed ethereal vehicle-mounted base stations (UAV-BSs), too known as ramble base stations, are considered to have promising potential to handle the impediments of ground base stations. They can give cost-effective Web association to clients that are out of framework. They can too take over rapidly as benefit suppliers when ground base stations fall flat in an unforeseen way. UAV-BSs advantage from their versatile nature that empowers them to alter their 3D areas in case the request profile changes quickly. In arrange to viably use the portability of UAV-BSs so as to maximize the execution of the organize, 3D area of UAV-BSs requires ceaseless optimization. In any case, tackling the optimization issue of UAV-BSs is NP-hard with no deterministic arrangement in polynomial time. In this paper, we propose a ceaseless actor-critic profound support learning arrangement in arrange to unravel the area optimization issue of UAV-BSs within the nearness of versatile endpoints. The reenactment comes about appear that the proposed show essentially progresses the organize execution compared to Q-learning, profound Q-learning and ordinary calculations. Whereas the Q-learning and profound Q-learning-based baselines reach the whole information rate of 35 Mbps and 42 Mbps separately, our proposed ACDQL-based procedure maximizes the whole information rate of endpoints to 45 Mbps. Moreover, the proposed ACDQL-based technique decreases the meeting time of the UAV-BS arrangement optimization by 85 percent compared to the Q-learning and profound Q-learning baselines.

2.5 Deep Reinforcement Learning Based Algorithm for Symbiotic Radio IoT Throughput Optimization in 6G Network

Web of Things (IoT) -based 6G is anticipated to revolutionize our world. Different candidate innovations have been proposed to meet IoT framework necessities based on 6G, advantageous radio (SR) is one of these innovations. This paper points to utilize advantageous radio innovation to back the detached Web of things and improve uplink transmission execution. The IoT tag data is sent to the cloud for investigation through a large scale base station (MBS) or a remote get to point (WAP), where the smartphones are utilized as a transfer to transmit this data to the MBS or WAP. In this paper, an optimization issue was defined into two stages to maximize the full throughput of the framework. The primary stage is, the issue of accomplishing the ideal mode choice of the LTE or Wi-Fi Arrange, pointing to maximize the framework throughput. A coordinating amusement calculation is utilized to fathom this issue. Moment stage, the issue of accomplishing ideal clustering of labels, where the labels are partitioned into virtual clusters, and finding which smartphones' LTE/Wi-Fi downlink signals all cluster individuals can ride to maximize the framework throughput. A twofold profound Q-network (DDQN) demonstrate was proposed to solve this issue. Recreation comes about appear that our proposed calculations increment the entire framework information rate by an normal of 90% over the framework utilizing the LTE arrange to begin with without DDQL calculation. Besides, it upgrades the capacity of the framework on normal by 100% over LTE arrange to begin with framework without the DDQL calculation .Web of Things (IoT) has been the subject of critical inquire about consideration in later a long time, the paper too talks about ML approaches as security arrangements against DDoS assaults in IoT situations. Moreover, the paper suggests a number of bearings for future inquire about. This paper is expecting to help the investigate community with the plan and advancement of successful defense frameworks able of overcoming distinctive sorts of DDoS assaults.

2.6 6G Cloud-Native System: Vision, Challenges, Architecture Framework and Enabling Technologies

Every generation of wireless technologies needs to bring a set of new system capabilities to enable future applications and services, the sixth-generation mobile system (6G) is no exception. This paper provides an overview of the technology transformation from the communication-centric the fourth-generation mobile system (4G) and the fth generation mobile system (5G) to the compute-centric 6G with the cloud-native system framework as the foundation of the next generation technologies. We explain what 6G plans to achieve, the fundamental reasons for this technology transformation, the architecture framework and enabling technologies to achieve 6G cloud-native technology objectives. This paper intends to provide a technical deep dive on the 6G cloud-native system to trigger more discussions, innovations and bring the technology transformation from concept to reality.

2.7 Blockchain-Based Lightweight Multifactor Authentication for Cell-Free in Ultra-Dense 6G-Based (6-CMAS) Cellular Network

Cell-Free mMIMO could be a portion of innovation that will be coordinates with future 6G ultradense cellular systems to guarantee boundless remote network and ubiquitous latency-sensitive administrations. Cell-Free picked up researchers' intrigued because it offers omnipresent communication with expansive transfer speed, tall throughput, tall information transmission, and more noteworthy flag pick up. Cell-Free disposes of the thought of cell boundary in cellular communication that diminishes visit handover and inter-cell impedances issues. In any case, the adequacy of the current confirmation convention may ended up a genuine issue due to the energetic nature of Cell-Free in thickly dispersed, tall number of clients, tall versatility, and visit information trade. Besides, secure communication may be accomplished in such a energetic environment at the cost of tall verification overhead, tall communication and computational costs. To address the over security challenges, we proposed a lightweight multifactor shared verification convention for Cell-Free communication utilizing ECC-based Deffie Hellman (ECDH). This plot utilizes timestamping, one-way hash work, Blind-Fold Challenge plot with open key framework. The proposed cryptosystem coordinating with blockchain innovation utilizing verification of staked (POS) as a agreement instrument to guarantee judgment, nonrepudiation and traceability. The proposed conspire can implement the relief of a few major security assaults on communication joins such as spoofing assaults, listening stealthily, client area security issues, replay assaults, dissent of benefit assaults, and man-in-the-middle (MITM) assaults, which is one of the noteworthy highlights of the conspire. Besides, this plot contributes to decreasing confirmation, communication, and computational overheads with an normal of 32.8%, 52.4% and 53.2% way better execution separately as compared pattern verification conventions.

2.8 Wireless and Optical Convergent Access Technologies Toward 6G

The 6th era of versatile communication (6G) frameworks is as of late rising a part of intrigued, presenting modern cutting edge and challenging utilize cases that will request much more than fair communications to gotten to be a reality. Higher throughput, lower latencies, higher number of associations will thrust the necessity of long-term versatile systems to a new level, but too detecting, situating and imaging will play an imperative part within the unused predicted utilize cases. The integration of strategies created for remote communications with those conceived for optical joins will be fundamental to supply the foundation for the 6G systems. In this setting, this paper presents a audit on remote and optical merged get to arrangements towards the 6G frameworks. The composition brings the utilize cases, necessities and enablers for 6G systems counting a discourse around the state-of-the-art on THz and sub-THz communications, remote and optical convergence, unmistakable light communication, coordinates and free-space optics, new antenna plans, powerover - fiber deployments and the utilize of machine learning within the physical layer of future systems. By looking into the foremost important commitments accessible within the writing for remote and optical communications and displaying their fundamental commitments, this paper clearly appears that, more than a innovative slant, the meeting of remote and optical advances may be a crucial step towards the improvement of the 6 organize framework.

2.9 Designing a 6G Testbed for Location: Use Cases, Challenges, Enablers and Requirements

Area will have a central part in Investigate and Improvement (R&D) towards 6G systems, both as a benefit advertised by the organize (making strides the current advertising of 5G) and as an input to progressively location-aware administrations and arrange capacities. To coordinated area into 6G guidelines, it'll be exceptionally vital to plan approval frameworks such as testbeds, indeed when the actual innovation isn't however commercially accessible. This paper performs a survey of the utilize cases and their necessities, empowering advances in 6G, and challenges; and proposes a adaptable testbed engineering for performing arrange area related R&D. This engineering will allow to deploy an advancing foundation which is able permit early approval of 6G innovations.

2.10 Autonomous Vehicles With a 6G-Based Intelligent Cybersecurity Model

Sixth-generation (6G)-based communications have numerous applications and are developing as a unused framework to utilize existing vehicles and communication gadgets in independent vehicles (AVs). Electric vehicles and AVs not supporting the integration of brilliantly cybersecurity will ended up helpless, and their inside capacities, highlights, and gadgets giving administrations will be harmed. This paper presents an shrewdly cybersecurity demonstrate coordination shrewdly highlights concurring to the rising 6G-based innovation based on advancing cyberattacks. The model's novel plan was created utilizing the vital calculations to supply speedy and proactive choices with cleverly cybersecurity based on 6G (IC6G) arrangements when AVs confront cyberattacks. In this show, organize security calculations consolidating brilliantly methods are created utilizing connected cryptography. Cash exchange taking care of administrations actualized in an AV are considered an case to decide the security and insights level depending on the IC6G arrangements. Insights, complexity, and vitality effectiveness (EE) are evaluated. At long last, we conclude that the demonstrate comes about are viable for scholarly people recognizing and anticipating cyberattacks on AVs.

2.11 Satellite Swarm-Based Antenna Arrays for 6G Direct-to-Cell Connectivity

Coordinate network in L/S recurrence groups between satellites and common versatile earthbound client gear (UE), such as smartphones, is an basic include for future 6G non-terrestrial systems. The specialized slant in closing the connect between the communication endpoints is to create huge staged recieving wire clusters to be propelled in LEO circle. Toady swarms speak to an inventive and promising approach. Swarms are composed of a few little and lightweight satellites organized in a free-flying arrangement (i.e., remote associated) or a fastened arrangement (i.e., wired associated) making a disseminated staged radio wire cluster. It has the potential to supply an improved pick up, smaller pillar width and lower launch/build costs compared to customary single toady frameworks with large phased recieving wire clusters. The primary objective of this work is the plan of swarm-based radio wire clusters, in which the affect of key parameters such as the number of satellites within the swarm, their corresponding separate and the cluster geometry, is altogether analyzed. It is appeared that the undesired marvel of grinding projections can be relieved by means of optimized cluster geometries and a unused geometry named the upgraded logarithmic winding cluster (ELSA) is presented. The moment objective of this work is the recognizable proof of the foremost critical inquire about headings and framework plan angles for the swarm framework. In specific, it is appeared that fastened swarms with ELSA geometries, imaginative deployable structures and exceptionally little satellites can cultivate the arrangement of swarms in future adherent frameworks.

2.12 6G Networks Physical Layer Security Using RGB Visible Light Communications

Unmistakable Light Communication (VLC) could be a key innovation for the sixth-generation (6G) remote communication much obliged to the plausibility of utilizing acritical natural lights as a information exchange channel. In spite of the fact that VLC frameworks are more safe against impedances and less vulnerable to security vulnerabilities like most remote systems, VLC is indeed intrinsically helpless to listening stealthily assaults. Besides, since VLC is considered an empowering innovation for 6G, specific instruments are required to uphold information security. This paper considers making strides the security of the following era of remote communications by utilizing the Watermark Blind Physical Layer Security (WBPLSec) in VLCs. The most instinct is that RGB LEDs offer the plausibility for Wavelength Division Multiplexing (WDM) as a valuable bolster for the Spread-Spectrum (SS) watermarking. In this paper, we propose an approach that points at getting VLC Physical Layer Security (PLS) by combining watermarking with an RGB Driven sticking. We offer a execution examination of the proposed security engineering based on the mystery capacity in terms of its existence and blackout likelihood. We demonstrate that WBPLSec can be utilized to altogether progress privacy within the following era of remote communications. The comes about offer the plausibility of making a secure locale around the genuine recipient by leveraging the sticking optical control.

2.13 Channel Estimation Using CNN-LSTM in RIS-NOMA Assisted 6G Network

The combination of non-orthogonal numerous get to (NOMA) and reconfigurable cleverly surface (RIS) innovations is proposed to meet the requests of information rate, idleness, and network in 6th era (6G) systems. The two methods can bolster each other to extend the execution of the 6G framework. In a RIS-aided system, channel estimation could be a challenging issue, particularly when applying inactive RIS which has no flag processing. This paper proposes a profound learning (DL)-based channel estimation strategy employing a convolutional long-short term memory (CNN-LSTM) show for RIS-NOMA remote communication frameworks that coordinated RIS and NOMA strategies. CNN-LSTM leverages both the benefits of convolutional neural organize (CNN) as well as long-short term memory (LSTM), in which CNN can capture uncommon highlights whereas LSTM can capture transient highlights of time-series information. The recreation comes about demonstrate that the proposed CNN-LSTM show appears its vigor toward the variety of the RIS-NOMA framework parameters, i.e., transmit signal-to-noise proportion (SNR), control allotment calculate, and the number of RIS components. The impacts of the RIS-NOMA framework parameters on the forecast exactness of the proposed DL-based channel estimation strategies are assessed through diverse execution measurements. The comes about uncover that the execution precision in terms of normalized root cruel square blunder (NRMSE), coefficient of assurance R-squared score (R2 score), cruel outright scaled blunder (MASE), and mean absolute rate mistake (MAPE) increments with an expanded transmit SNR, control allotment calculate of the primary client and the number of RIS components. Moreover, the CNN-LSTM expectation execution appears its prevalence as compared to those of the four benchmark models counting the CNN1D-LSTM demonstrate utilizing one-dimensional convolution layer (conv1D), CNN1D-BiLSTM demonstrate utilizing bidirectional long-short term memory, CNN demonstrate and LSTM show.

2.14 What Physical Layer Security Can Do for 6G Security

Whereas existing security conventions were planned with a center on the center organize, the upgrade of the security of the B5G get to organize gets to be of basic significance. In spite of the reinforcing of 5G security conventions with regard to LTE, there are still open issues that have not been completely tended to. This work is enunciated around the introduce that reexamining the security plan foot up, beginning at the physical layer, isn't as it were reasonable in 6G but imperatively, emerges as an productive way to overcome security obstacles in novel utilize cases, eminently gigantic machine sort communications (mMTC), ultra-reliable moo idleness communications (URLLC) and independent cyber physical frameworks. Not at all like existing survey papers that treat physical layer security orthogonally to cryptography, we'll attempt to supply many experiences of basic associations. Examining numerous down to earth issues, we'll display a comprehensive audit of the state-of the-art in i) mystery key era from shared haphazardness, ii) the wiretap channels and essential limits, iii) confirmation of gadgets utilizing physical unclonable functions (PUFs), localization and multi-factor confirmation, and, iv) sticking assaults at the physical layer. We at last conclude with the proposers' desires for the 6G security scene, within the hyper-connectivity and semantic communications period.

2.15 The Evolution of Networks and Management in a 6G World: An Inventor's View

The onset of the 6G time in broadcast communications, touted to dispatch in 2030, is trusted to serve numerous experts and convey an unparalleled enhancement in capabilities, applications, insights, and undoubtedly free human potential. The vision of 6G consolidates unused radio frequencies and innovations, the integration of detecting, cognitive strategies characterizing both organize capacities and their administration, and unused organizing approaches for a broader scope of applications and conveyance. The challenges for innovators lies in both physical gadgets and a substantive advancement within the advancement of capacities actualized by, and overseen, with program. The calculations (counting energetic arrangements based on Fake Insights and Machine Learning), conventions, and engineering evolutions will bring together the foremost progressed computer program frameworks ever envisioned for broadcast communications. However, the commerce of companies building and working these another era stages requires a tremendous venture, and 6G will surpass all others with its breadth and complexity. This paper diagrams one conceivable timeline of innovative affect based on the pace of innovation, speculation, worldwide setting, and the wide objectives of 6G. From this, takes after a vision of the basic strategies in computerization, security and organizing that we accept will be central to bringing the dream of 6G to a reality.

2.16 Designing an Enhanced User Authenticated Key Management Scheme for 6G-Based Industrial Applications

Within the 6th Era (6G) versatile framework, the significance of security increases even more within the communication framework. One of the potential innovations of 6G is the Network in a Box (NIB). The 6G-enabled NIB may be a multi-generational, effortlessly and quickly installable innovation utilized for communication. It is based on both equipment and program. The most highlights of a 6G-enabled NIB incorporate moo idleness and a tall level of exibility. In addition, it gives network administrations to the applications utilized in unusual circumstances such as fight elds or normal calamities within the industry. Be that as it may, most of the applications utilized within the 6G-enabled NIB are not suitably secured. There are chances of a few dynamic and inactive assaults due to the unreliable channel. Hence, a novel farther client verification and key administration plot is displayed in this paper. This plot is the modi ed and progressed adaptation ofUAKMS-NIB and is renamed as the made strides Client Verification and Administration Conspire to secure the 6G-enabled NIB (iUAKMS -NIB) that can be utilized in mechanical applications. Thus, the proposed conspire gives the leading security arrangement against the conceivable assaults on the 6G communication framework. The expository comes about appear that the proposed conspire performs superior compared to the existing plans.

2.17 Physical-Layer Security in 6G Networks

The sixth generation (6G) of mobile network will be composed by different nodes, from macro-devices (satellite) to nano-devices (sensors inside the human body), providing a full connectivity fabric all around us. These heterogeneous nodes constitute an ultra-dense network managing tons of information, often very sensitive. To trust the services provided by such network, security is a mandatory feature by design. In this scenario, physical-layer security (PLS) can act as a first line of defense, providing security even to low-resourced nodes in different environments. This paper discusses challenges, solutions and visions of PLS in beyond-5G networks.

2.18 Security and Trust in the 6G Era

A comprehensive set of security innovation enablers will be basically required for communication frameworks for the 6G period of the 2030s. Dependability must be guaranteed over IoT, heterogeneous cloud and systems, gadgets, sub-networks, and applications. The 6G danger vector will be denied by 6G engineering disaggregation, open interfacing and an environment with different partners. Broadly decayed into spaces of cyber-resilience, protection and believe and their particular crossing point, we investigate important security innovation enablers counting computerized program creation and mechanized closed-loop security operation, protection protecting advances, equipment and cloud implanted stays of believe, quantum-safe security, sticking security and physical layer security as well as conveyed record advances. Article insights and machine learning (AI/ML) as a key innovation enabler will be unavoidable and of essential significance over the security innovation stack and engineering. A novel vision for a reliable Secure Telecom Operation Outline is created as portion of the computerized closed circle operations worldview.

2.19 An Ultralow-Loss and Lightweight Cellulose-Coated Silica Foam for Planar Fresnel Zone Plate Lens Applications in Future 6G Devices

A comprehensive set of security innovation enablers will be basically required for communication frameworks for the 6G period of the 2030s. Dependability must be guaranteed over IoT, heterogeneous cloud and systems, gadgets, sub-networks, and applications. The 6G danger vector will be denied by 6G engineering disaggregation, open interfacing and an environment with different partners. Broadly decayed into spaces of cyber-resilience, protection and believe and their particular crossing point, we investigate important security innovation enablers counting computerized program creation and mechanized closed-loop security operation, protection protecting advances, equipment and cloud implanted stays of believe, quantum-safe security, sticking security and physical layer security as well as conveyed record advances. Article insights and machine learning (AI/ML) as a key innovation enabler will be unavoidable and of essential significance over the security innovation stack and engineering. A novel vision for a reliable Secure Telecom Operation Outline is created as portion of the computerized closed circle operations worldview

2.20 A D2D-Aided Federated Learning Scheme with Incentive Mechanism in 6G Networks

Inescapable unused time applications are anticipated to include enormous sum of information to execute brilliantly disseminated systems based on machine learning, upheld by 6th era (6G) systems innovation to offer quick and solid communications. Unified Learning (FL) is quickly developing as promising privacy-preserving arrangement to prepare machine learning models in a conveyed design. In any case, clients are frequently not as well slanted to require portion within the learning handle without accepting emolument. Thus, to overcome this downside, the utilitarian integration of a legitimate gadgets motivating force instrument with an proficient approach for the gadgets choice in a same FL system gets to be fundamental. In this respect, this paper proposes a FL framework involving a one-side coordinating theory-based incentive instrument to choose and energize clients to require portion of the method with the point at minimizing the FL handle merging time and maximizing the clients harbour. Besides, this paper faces with the plausibility to overcome terrible communication interface conditions by turning to device-to-device communications among clients in arrange to lower the vitality squandered and progress the joining time of the FL handle. In specific, an reverberate state- arrange, running in nearby at each client location, has been considered to estimate channel conditions in a solid way. Execution assessment has highlighted the changes in joining time and vitality utilization of the proposed FL system in comparison with routine approaches, consequently, highlighting its reasonableness for applications within the up and coming 6G systems.associated with IoT networks make smart city infrastructure vulnerable to cyber-attacks. For example, Distributed Denial of Service (DDoS) attack violates the authorization conditions in smart city infrastructure; whereas replay attack violates the authentication conditions in smart city infrastructure. Both attacks lead to physical disruption to smart city infrastructure, which may even lead to financial loss and/or loss of human lives. In this paper, a hybrid deep learning model is developed for detecting replay and DDoS attacks in a real-life smart city platform. The performance of the proposed hybrid model is evaluated using real life smart city datasets (environmental, smart river and smart soil), where DDoS and replay attacks were simulated. The proposed model reported high accuracy rates: 98.37% for the environmental dataset, 98.13% for the smart river dataset, and 99.51% for the smart soil dataset. The results demonstrated an improved performance of the proposed model over other machine learning and deep learning models from the literature.

3. COMPARATIVE ANALYSIS

S. No	Title	Techniques & Mechanisms	Parameter Analysis	Tools	Future Work
1.	Towards 6G-Enabled Internet of Vehicles: Security and Privacy	Decentralized learning algorithm.	privacy-guarantee as model	federated learning (FL)	Focusing on the security and privacy aspects of the 6G enabled IoV
2.	Proactively Predicting Dynamic 6G Link Blockages Using LiDAR and In-Band Signatures	DBSCAN clustering algorithm	Baseline method and the ML method	LiDAR	mmWave and LiDAR sensory data to proactively predict dynamic blockages in mmWave systems.
3.	The Roadmap to 6G Security and Privacy	AI/ML	APIs by continuing the trend develop	using security check tools	6G security towards a reality has already initiated from the research level.
4.	A Continuous Actor–Critic Deep Q-Learning-Enabled Deployment of UAV Base Stations: Toward 6G Small Cells in the Skies of Smart Cities	RL algorithm	UAV-BS depends on the current state of the environment	UAV-BS	UAV-BSs have recently gained increasing attention as a solution to provide Internet connectivity to endpoints in various scenarios.
5.	Deep Reinforcement Learning Based Algorithm for Symbiotic Radio IoT Throughput Optimization in 6G Network	DDQL, matching game	DQL algorithm was proposed to solve problem	AI	Selection of (LTE or Wi-Fi) network that acts as a relay for the backscattered information received from IoT tags.
6.	6G Cloud-Native System: Vision, Challenges, Architecture Framework and Enabling Technologies	Workload Algorithm	performance metrics, simulation scenarios, trafic models	Communication service providers (CoSPs)	The cloud-native system establishes a platform foundation to integrate communication, computing and data services into a 6G wide-area cloud and to support AI-native workloads.

7.	Security issues in cell free 6G environment by integrating blockchain with lightweight multifactor point (AP) consist of multiple antennas	Particle swam optimizat ion technique	Control station shares location strategy parameters	Back propagation (BP)algorithm	Cell-Free mMIMO is a part of the technology that will be Integrated into future ultra-dense wireless networks.
8.	Wireless and Optical Convergent Access Technologies Toward 6G	Cloud computing technology	Radiocommunicatio ns Reference Center (CRR)	Platform as a service (PaaS)	Investigate the overhead caused by traffic schedule and PON framing in edge computing enabled TWDN- PON, addition the implementation of control plane enabling traffic scheduling to investigate.
9.	Designing a 6G Testbed for Location: Use Cases, Challenges, Enablers and Requirements	WIFI using Received Signal Strength Indicator (RSSI)	RAN and core network functions	Python-based data analytics	To develop and test these location techniques and location aware applications of the future, the R&D community needs a testbed that is purposefully built for location in 6G.
10.	Autonomous Vehicles With a 6G-Based Intelligent Cybersecurity Model	deep-learning algorithms	Devices used in the AVs	Autonomous Vehicles (AVs)	cyberattacks on AVs and intelligent cybersecurity solutions that maintain secure services from all vulnerabilities created by attackers, faulty devices, or fake messages.
11.	Satellite Swarm-Based Antenna Arrays for 6G Direct-to-Cell Connectivity	The complexity of the algorithm	satellite orbit parameters	Enhanced logarithmic array (ELSA)	Use of satellite swarms for the direct to cell connectivity use case
12.	6G Networks Physical Layer Security Using RGB Visible Light Communications	WBPLSec for VLC Networks and Jamming Receiver (Bob)	The scaling parameter	jamming as a security tool	VLC is considered a key enabler technology for fast wireless Communications.
13.	Channel Estimation Using CNN-LSTM in RIS-NOMA Assisted 6G Network	DL model with an orthogonal matching pursuit algorithm	RIS-NOMA system model	OMA technique	The CNNLSTM shows its robustness to the variation of the RISNOMA system parameters.

14.	What Physical Layer Security Can Do for 6G Security	symmetric encryption algorithm and message authentication code (MAC) algorithm	Bob and Eve is the fading parameter	Addressed with standard cryptographic tools	PLS could play in 6G, in view of the evolution in terms of security.
15.	The Evolution of Networks and Management in a 6G World: An Inventor's View	Artificial Intelligence and Machine Learning	Risk Analysis	virtualized RAN (vRAN)	Intent-based networking from the UE, network assisted service creation
16.	Designing an Enhanced User Authenticated Key Management Scheme for 6G-Based Industrial Applications	collision-resistant one-way cryptographic hash algorithm	Bo_x related secret key and reproduction parameter	Monitoring and controlling industrial equipment, intelligent industrial tools	An authentication scheme is proposed in Wazid et al.
17.	Physical-Layer Security in 6G Networks	artificial intelligence algorithms	higher-layer cryptographic techniques	Massive Cell-Free MIMO	PLS can help in facing the significant security challenges raised by ubiquitous ultra-dense heterogeneous networks.
18.	Security and Trust in the 6G Era	symmetric encryption algorithms	quantum safe security by adaptation of parameters	AI/ML	proof-of-concept and case study work in the domains of key technology.
19.	An Ultralow-Loss and Lightweight Cellulose-Coated Silica Foam for Planar Fresnel Zone Plate Lens Applications in Future 6G Devices	FZP lens antenna.	Scattering parameter	FZP lens	The FZP lens was connected to a waveguide and has been shown to be capable of increasing.
20.	A D2D-Aided Federated Learning Scheme with Incentive Mechanism in 6G Networks	cross-silo horizontal technology	Interface to submit the corresponding parameter	Echo state network	D2D-aided FL scheme for applications in 6G based networks.

4. CONCLUSION

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 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.

5. REFERENCES

[1] Z. Qadir, K. N. Le, N. Saeed, and H. S. Munawar, ‘‘Towards 6G Internet of Things: Recent advances, use cases, and open challenges,’’ ICT Exp., vol. 30, pp. 1–17, Jun. 2022.

[2] P. Mach and Z. Becvar, ``Device-to-device relaying: Optimization, performance perspectives, and open challenges towards 6G networks," IEEE Commun. Surveys Tuts., vol. 24, no. 3, pp. 13361393, 3rd Quart., 2022.

[3] S. A. A. Hakeem, H. H. Hussein, and H. Kim, ‘‘Security requirements and challenges of 6G technologies and applications,’’ Sensors, vol. 22, no. 5, p. 1969, Mar. 2022, doi: 10.3390/s22051969.

[4] J. Yao and J. Capmany, ‘‘Microwave photonics,’’ Sci. China Inf. Sci., vol. 65, no. 12, pp. 1–15, Aug. 2022.

[5] H. Tataria, M. Shafi, M. Dohler, and S. Sun, ‘‘Six critical challenges for 6G wireless systems: A summary and some solutions,’’ IEEE Veh. Technol. Mag., vol. 17, no. 1, pp. 16–26, Mar. 2022.

[6] 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.

[7] SpaceX Starlink Satellites to Beam Service Straight to Smartphones.Accessed: Aug. 26, 2022. [Online]. Available: https://www.space.com/spacex-starlink-direct-service-smartphones-t-mobile.

[8] Y. Liao and V. Friderikos, "Optimal deployment and operation of robotic aerial 6G small cells with grasping end effectors," in Proc.IEEE Int. Conf. Commun., 2022, pp. 1–6.

[9] S. Jiang, G. Charan, and A. Alkhateeb, "LiDAR aided future beam prediction in real-world millimeter wave V2I communications," IEEE Wireless Commun. Lett., early access, Nov. 4, 2022, doi: 10.1109/LWC.2022.3219409.

[10] U. Demirhan and A. Alkhateeb, "Integrated sensing and communication for 6G: Ten key machine learning roles," 2022, arXiv:2208.02157.

[11] J. Chen, Y. Liang, H. V. Cheng, and W. Yu, ‘‘Channel estimation for reconfigurable intelligent surface aided multi-user mmWave MIMO systems,’’ IEEE Trans. Wireless Commun., early access, Feb. 23, 2023, doi: 10.1109/TWC.2023.3246264.

[12] Y. Sun, J. A. Zhang, K. Wu, and R. P. Liu, ‘‘Frequency-domain sensing in time-varying channels,’’ IEEE Wireless Commun. Lett., vol. 12, no. 1, pp. 16–20, Jan. 2023.

[13] M. Mitev, T. M. Pham, A. Chorti, A. N. Barreto, and G. Fettweis,

[14] "Physical layer security - from theory to practice," Nov. 2022. [Online]. Available: https://www.techrxiv.org/articles/preprint/Physical_Layer_Security_from_Theory_to_Practice/21388338.

[15] National Centers for Environmental Information (NCEI) (NOAA,

[16] U.S. Government, Washington, DC, USA). Time Series of Billion Dollar Weather and Climate Disasters. (2022). [Online]. Available: https://www.ncdc.noaa.gov/billions/time-series

[17] H. Yi, ``A secure blockchain system for Internet of Vehicles based on 6G-enabled network in box," Comput. Commun., vol. 186, pp. 45_50, Mar. 2022.

[18] A. Ghavidel, S. Myllymäki, M. Kokkonen, N. Tervo, and H. Jantunen, "Lens antenna adjustment for telecommunication and imaging modes in a sub-THz radio system," Eng. Rep., vol. 4, no. 3, 2022, Art. no. e12474, doi: 10.1002/eng2.12474.

[19] C. Chaccour, M. N. Soorki,W. Saad, M. Bennis, and P. Popovski, ``Can terahertz provide high-rate reliable low-latency communications for wireless VR?'' IEEE Internet Things J., vol. 9, no. 12, pp. 97129729, Jun. 2022.

[20] R. Zhong, X. Liu, Y. Liu, Y. Chen, and Z. Han, ``Mobile reconfigurable intelligent surfaces for noma networks: Federated learning approaches,'' IEEE Trans. Wireless Commun., vol. 21, no. 11, pp. 10020_10034, Nov. 2022.