Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 2, pp. 770–781, DOI 10.12694/scpe.v25i2.2629

SECURITY AND PRIVACY OF 6G WIRELESS COMMUNICATION USING FOG COMPUTING AND MULTI-ACCESS EDGE COMPUTING

TING XU*, NING WANG †, QIAN PANG‡, AND XIQING ZHAO§

Abstract. The challenges surrounding the confidentiality of data transmission in the context of the upcoming sixth-generation (6G) wireless networks are proposed in this research. The study explores the potential role of blockchain systems in enhancing data security. It examines the integration of machine learning (ML) techniques to address the growing complexities of handling massive data volumes within the 6G environment. This research involves a comprehensive survey of existing strategies for maintaining data confidentiality in automotive communication systems. It further investigates an analysis of confidentiality approaches inspired by the 6G network architecture. The study examines the potential security implications of the Internet of Everything (IoE). It evaluates current research issues related to safeguarding data confidentiality within the framework of 6G communication among vehicles. The exploration involves reviewing ML techniques and their applicability in resolving the data processing challenges inherent in the 6G wireless network environment. The proposed work reveals the increasing complexity and variability of the 6G wireless network environment, leading to potential challenges in protecting private and confidential data during communication. It highlights the promising role of blockchain systems in addressing data security concerns within the 6G network context. Additionally, the study underscores the transformative potential of integrating ML techniques to handle the massive data volumes generated within the 6G ecosystem. The research highlights the importance of these technologies in mitigating data security risks and ensuring the confidentiality of information exchanged within the 6G communication framework.

Key words: Multi-access Edge Technology, Safety and Security, Internet of Everything (IoE), Wireless Communications, Cloud Computing Environment

1. Introduction. The extensive availability of wireless communication devices has had a profound impact on individuals' daily lives and has accelerated the expansion of the manufacturing sector. Businesses engaged in online communication and entertainment have particularly gained the rewards of the current fourth-generation (4G) infrastructure. The upcoming fifth-generation (5G) communication networks will order the Internet of Things (IoT), autonomous vehicles, and both virtual and augmented reality (AR/VR) applications. However, the absence of a personal touch in 5G communications has urged researchers and companies to anticipate the forthcoming phase of wireless communication. Despite its numerous benefits, 5G technology lacks a human element [1, 2].

The connectivity framework of the 6G generation transforms "linked objects" into "associated intelligence." Substantial investments in research and development for the 6G communication system are primarily directed towards the press, the product, and the fundamental building blocks. The emergence of advanced Intelligent Computing, the capability to gather, transmit, and assess information, and the facilitation of a diverse array of applications and intelligent services are all anticipated advancements with the introduction of 6G technologies. Human advancement will be ordered in the 6G paradigm above information, technology, and services. It is anticipated that the 6G communication infrastructure will strengthen confidentiality and security by eliminating any vulnerabilities associated with these issues, thus enhancing the overall reliability of the network. However, if conventional approaches to machine learning are used, the central server structure could be susceptible to privacy and security risks originating from various internal nodes, potentially resulting in a single point of failure [3].

Traditional artificial intelligence methods are inadequate for processing vast amounts of accumulated data.

*Hebei North University, College of Information Science and Engineering, Zhangjiakou, Hebei, 075000, China
†Zhangjiakou Branch of China Mobile Communications Group Hebei Co. Ltd, Zhangjiakou, Hebei, 075000, China
‡Hebei North University, College of Information Science and Engineering, Zhangjiakou, Hebei, 075000, China
§Hebei North University, College of Information Science and Engineering, Zhangjiakou, Hebei, 075000, China (Corresponding author, xiqingzhao63@163.com)

Consequently, the sole solution presented by 6G involves the implementation of distributed artificial intelligence, with all customer-sensitive data stored within a set of instructional equipment close to the vehicle. The upcoming "sixth generation (6G)" of mobile phone networks, the successor to 5G mobile communications, represents a significant departure from the current technological landscape. 6G is anticipated to introduce cost efficiency, heightened security, and enhanced privacy to the system. Achieving this objective necessitates the integration of advanced technologies within the wireless network infrastructure. The ongoing deployment of automated, self-driving vehicles equipped with navigation systems, voice recognition structures, multiplayer games or movies, shopping capabilities, advertising functions, surveillance systems, and weather forecasting systems aims to reduce accidents, fatalities, and property damage. In today's increasingly automated environments, machine learning, often combined with artificial intelligence (AI), is a recent innovation in this domain [4].

Deep training is a form of artificial intelligence capable of discerning patterns and characteristics using vast datasets generated by lens detectors, ultrasonic detectors, and other devices. Automated driving, facilitated by autonomous vehicles (AVs), enables real-time adjustments of an automobile's acceleration and braking capabilities based on road conditions. The accuracy of judgments relies on both the input information and the capabilities of the deep learning (DL) model. Over the past few years, the focus on interconnected vehicles within the internet-of-vehicle (IoV) program has shifted towards integrated cognition. Data exchange and communication between mobile nodes will soon incorporate a hybrid approach, combining vehicle-to-anything (V2X) and designated limited-range transmission. Wireless access in vehicular environments (WAVE) relies on the 802.11p IEEE protocol, which will require updates to manage the substantial data flows across the internet. Anticipated advancements in 6G technology are expected to enhance V2X capabilities, highlighting privacy-protective features in these scenarios [5].

The beginning of self-driving vehicles represents an increasing technology that, upon full integration, promises customers a seamless and stress-free travel experience courtesy of machine learning and multi-access edge computing (MEC). By feeding back collected data to edge structures, MEC facilitates the automation of vehicles through edge intelligence (EI), enabling them to anticipate and respond appropriately. The implementation of EI technology has the potential to strengthen the network's dependability and generally reduce latency. However, despite the manifold benefits outlined, the pursuit of establishing an automated 6G ecosystem faces various challenges. Ensuring the reliability of wireless networks, preserving the privacy of individual nodes, safeguarding sensitive data, and other related factors necessitate careful consideration [6].

A relatively young AI technology has swiftly emerged as one of the most powerful tools in its domain. Its adaptability has led to its widespread use in diverse fields, such as wireless network security, traffic monitoring, and dynamic topology alert systems, as well as for ensuring data reliability and privacy. These applications represent only a fraction of AI's potential. While initially intended for monitoring geographically dispersed networks, AI is now commonly employed to improve networks' overall efficiency and functionality. The network's initial structure was deliberately kept simple to enable upgrades at any node, anytime. Since integrating AI, the network has been continuously monitored and fortified against potential threats. Encryption methods are frequently employed to detect and prevent suspicious activities within wireless networks, including monitoring network load and traffic volume to identify and counteract denial of service (DoS) attacks. AI-based technology can complement existing network security strategies, ultimately reducing wireless security risks [7].

Artificial intelligence, machine learning, and deep learning algorithms, previously unattainable services, have become feasible. These innovative techniques have enhanced our understanding of wireless environments and enabled accurate predictions across various activities. Tasks such as capacity classification, resource management, and data security stand to benefit significantly from the application of such technology. Implementing these methodologies can positively impact the quality of experience (QoE) and enhance network reliability. Furthermore, advancements in machine learning have automated the creation of communication models, facilitating the development of increasingly sophisticated methods for connectivity. Additionally, users can now request internet access, prompting the system to identify relevant devices and service-oriented applications and provide them to the user in an orderly fashion. Previously, users had to expend significant time and effort conveying their requirements to network technicians for tailored system maintenance [8].

The aim of achieving greater adaptability and swiftness in this sphere is realized by implementing a Software-Defined Networking architecture. By enabling easier access to complete permissions, access providers

can better cater to the needs of clients with stringent requirements, which stands as the primary objective of this initiative. By integrating multiple encryption mechanisms, SDN and AI can streamline various operations, including load distribution, process management, and network security against potential threats. Some estimates suggest that over 55 per cent of access providers plan to incorporate AI into their infrastructures to streamline current processes. The recent spread of AI-powered devices with embedded connectivity has sparked notable advancements in in-vehicle connectivity. This modern technology has significantly enhanced the performance of various blockchain-powered devices, including IoVs and software-defined networks (SDNs). While the current 5G technology adequately supports existing devices, it may face challenges accommodating future technologies such as 3D video chats. The convergence of AI and IoT has led to a wider array of interconnected devices capable of participating in and benefiting from online communication [9].

Hence, in the future, 5G will only be able to support a limited data volume or a large customer base. Under the current 5G standard, administrators can manually configure and optimize their networks. Consequently, manually managing a sprawling, dynamic, and widely dispersed network poses significant challenges. In a scenario beyond 5G (B5G) or with the advent of 6G, the integration of AI technology is anticipated to render these vulnerabilities obsolete.

2. Related works. In vehicle networks, numerous drivers can engage in real-time information exchange while providing a diverse range of conveniences to fellow motorists. These services include GPS navigation, ridesharing, valet parking, real-time traffic updates, and digital vehicle diagnostics. The fifth generation (5G) of radio communication technologies introduces significant enhancements in security, accessibility, and network capacity. Educational and corporate institutions have displayed considerable interest in 5G-supported vehicular networks (5GVNs), expecting them to have a transformative impact on the transportation landscape and foster various novel connectivity options. Simultaneously, advancements in sensor technology and the expansion of regional data collection systems have made gathering extensive information from vehicle users, including identity verification, status updates, and location tracking, an unavoidable reality. Regrettably, 5GVN still grapples with diverse privacy threats, leaving users' information, viewpoints, locations, and movements susceptible to potential breaches. The latest research findings examine 5GVN's architecture, features, and capabilities. It subsequently delves into the privacy objectives of 5GVN and the associated security risks, providing an in-depth analysis of existing solutions to preserve user privacy. Finally, potential avenues for further research are outlined to stimulate greater interest in this innovative design and its privacy concerns while encouraging grassroots initiatives to address these issues effectively [10].

The 5GVN represents a groundbreaking framework poised to revolutionize the scale of service deployment and vehicle communication. As 5G networks expand and electric vehicles become increasingly commonplace, 5G will become more deeply ingrained in our daily lives. Nevertheless, privacy risks continue to raise a spectrum of concerns for automotive users. This research extensively evaluates numerous privacy-preserving options for 5GVN, encompassing an exploration of its architecture, features, and capabilities. The study emphasizes the imperative of protecting user privacy, assessing the threats within 5GVN, and examining the problems and solutions ensuring user anonymity within the 5GVN context. Ultimately, the study highlights the need for continued attention and effort to address 5GVN and its associated security challenges [11].

The 6G represents cutting-edge technology with promising capabilities for addressing the demanding communication requirements of autonomous vehicles. Its potential benefits include minimized latency, reduced communication costs, and a strong focus on safeguarding user data in the dynamic 6G ecosystem. Various technologies, such as machine learning, deep learning, artificial intelligence, and blockchain, can be used to address these challenges. However, the increasing number of vehicles on the road and interconnected IoT devices has made ensuring a reliable flow of information over the Internet increasingly complex, particularly with the application of conventional ML techniques.

The authors examine the potential privacy implications of IoE within the context of 6G automotive interactions, highlighting ongoing research concerns in privacy preservation. Safeguarding consumers' privacy and security remains a principal consideration in wireless networks. While introducing 5G technology brought new threats to user safety and privacy, the advent of 6G network technology is expected to mitigate these issues. As a result, advancing an efficient and reliable identification mechanism becomes imperative in 6G-powered transportation communication [12].

The IoV introduces a novel computing model offering several advantages to drivers and users, including route suggestions, reduced traffic delays, and enhanced driving experiences. However, sharing IoV participants' data with external entities exposes them to potential privacy breaches. This article conducts a comprehensive analysis of the privacy risks associated with IoV. It proposes strategies for addressing these concerns, examining the privacy challenges of IoV's architecture. In this exploration of the IoV, the authors focus on ensuring the security of sensitive information. Initially, researchers investigate the structural intricacies of IoV, highlighting the inherent privacy challenges. The authors established a cohesive framework for safeguarding personal data, encompassing encryption, anonymity, and perturbation as essential privacy measures. Additionally, potential avenues are thoroughly examined for research, emphasizing IoV applications and advanced methodologies while prioritizing individual privacy requirements [13].

The paper addresses the privacy challenges associated with V2X communication in the cloud by introducing the security evaluation methodology with understanding considerations. Leveraging artificial intelligence on previously collected data enables the assessment of cloud-based uncertainties based on prior evaluations. Moreover, PAU accounts for privacy-preserving capabilities derived from moment-to-moment vehicle interactions. It presents a security aggregation technique that combines online and offline perspectives to enhance the precision of the security assessment. In these models, a method is established for generating the mixed zone by selecting nodes with a heightened awareness of confidentiality. The outcomes of our research validate the efficacy of our approach on various fronts, particularly in stimulating the system against malicious behaviour and slander-based attacks using historical data stored on the public Internet.

The rapid advancement of technology and modern vehicles underscores the critical need to ensure the security and reliability of the IoV. This environment inherently faces ongoing security challenges due to the vulnerability of wireless networks, leading to concerns about personal safety, protection, and anonymity on roadways. Over the years, various privacy- and security-preserving techniques have been proposed to mitigate destructive player attacks, complex computations, and high communication costs, aiming to overcome the limitations of existing solutions [14].

Several approaches have been suggested by computer security experts, authors, and practitioners to address the security and privacy concerns [15]:

(i) The proposed system integrates a structure akin to fog cloud vehicular ad hoc systems.

(ii) The solution incorporates an identity protection mechanism based on public key cryptography for securing user information.

(iii) To assess and rank four distinct algorithms for dynamic routing using a simulator, tracking the findings for each protocol and conducting a graphical analysis of the collected data throughout the simulation. The combined impact of ECC deployment and the optimal routing protocol on VANET performance are evaluated in this context.

The VANETs safeguarding many prior initiatives have merely repurposed conventional security methods that have proven effective without accommodating the network's specific nature. Several solutions advocated by security specialists rely on trusted platform modules (TPMs), perceived as single points of failure, or involve intricate computations impacting VANET efficiency. In response to our examination of VANET architecture and its associated security challenges, an approach is formulated that fulfils the requirements for confidentiality while ensuring the protection of individual user privacy [16, 17].

A novel system, called the fog cloud, has been introduced to incorporate fog computing. This was accomplished through experiments, inspections, and evaluations in Network Simulator 3 to identify the optimal routing protocol, addressing the intricacies of security solutions. The dynamic source routing (DSR) algorithm was determined to be the most effective approach when implementing ECC within the system. Leveraging encryption to uphold user confidentiality and ensure anonymity is based on insights from the study on each of the employed methodologies [18].

3. Proposed Methodology.

3.1. Internet-of-everything (IOE) Security Concerns in the Fifth Industrial Revolution. Industry 4.0 has seen a surge in standards owing to technological advancements such as artificial intelligence (AI), the IoT, and cloud-based computing. Its core aim is to make various businesses "smarter," overseeing an array of tools and technologies throughout their life cycles. Automation is the key to reducing the need for human

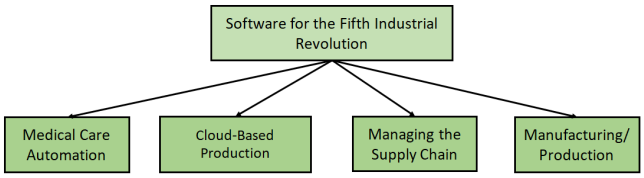

Fig. 3.1: Applications of Industry 5.0

involvement in labour-intensive processes. The goal is to leverage AI to bridge the performance gap between computers and machine learning (ML) devices, ultimately achieving higher overall efficiency. Looking ahead to Industry 5.0, the focus is on integrating human and artificial intelligence. Many experts anticipate that human interaction will be pivotal in this next industrial revolution. Industry 5.0 is self-assured to boost production, catering to human and robotic adaptability. This will facilitate seamless information and feedback exchange between humans and machines, ultimately enhancing productivity. Within the Industry 5.0 framework, emphasis is placed on optimizing the quality of final products by differentiating tasks that require research and innovation from mundane, time-consuming activities. Skilled labour is encouraged, as people will be responsible for coding instructions for robots, promoting mass customization in manufacturing. Unlike the previous phase, Industry 4.0, which focused on mass production, Industry 5.0 significantly focuses on personalized and individualized end products, as depicted in Figure 3.1.

Machine learning (ML) is an increasingly reliable and prevalent innovation in the medical field. ML-based models are now used to diagnose patients, leading to faster and more accurate assessments. However, achieving a fully automated environment requires more than just these models. The concept of Industry 5.0 opens the possibility of automated processes, including patient examination and medication administration, based on the findings. In recent years, high-tech devices equipped with sensors have been developed to monitor patients' conditions, such as smartwatches and fitness trackers. These devices provide valuable data that aids physicians in conducting thorough examinations. In critical situations, these devices can communicate with each other and alert the medical team. According to Industry 5.0, robots could independently perform crucial surgical procedures, enabling human physicians to focus on innovation and research.

Internet manufacturing is a new technology that integrates IoT devices and cloud-based approaches to provide an automated virtualization experience to end-users. This collaboration among international stakeholders aims to reduce production costs and increase overall productivity. Cloud computing in content creation offers various advantages, including improved quality, reduced production expenses, enhanced security, and reliability. It also helps minimize environmental impact by preventing the mass production of defective items. Moreover, integrating human insights into IoT and artificial intelligence development can help address issues associated with unexpected mishaps. By combining human intelligence with machine intelligence, many unforeseen disasters, including earthquakes, tsunamis, and other natural calamities, can be efficiently mitigated.

3.2. New 6G methods for protecting security. The extensive wireless connections within future 6G environments, particularly in various vehicles, will raise the bar for ensuring privacy and security. The forthcoming 6G networks will require specific features to address potential security breaches. While several advanced techniques have demonstrated their capabilities within the 6G context, their ability to uphold security and privacy remains uncertain. Conversely, technologies such as cloud computing and system software are under scrutiny concerning the privacy aspects of 5G.

In summary, the potential solution for mitigating the reliability challenge in the upcoming 6G environment involves addressing key concerns, including reducing privacy risks by implementing available and contemporary solutions. Figure 3.2 provides insights into how certain common technologies could minimize privacy and security risks.

The Blockchain approach has experienced significant growth in distributed database technology, gaining traction in the mobile phone industry through various publicly available DLTs. Leveraging blockchain to

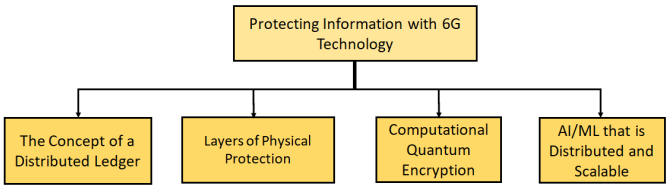

Fig. 3.2: Secrecy Tools for the 6th Generation

integrate multiple services into a 6G network ecosystem while maintaining security offers numerous advantages. However, incorporating machine learning (ML) or additional data analysis techniques might lead to potential vulnerabilities in 6G networks despite the benefits of integrating AI approaches. Several machine learning methods are susceptible to various forms of attack during both the training and testing phases. Consequently, verifying the authenticity and source of data before subjecting it to various artificial intelligence methods is crucial. The use of immutable data in DLT can help ensure data integrity, with this assurance being shared among the numerous parties involved in establishing the trustworthiness of AI robots in a dynamic environment. Drawbacks arise from users' exposure to a wide spectrum of security issues when employing DLT in a 6G context, potentially impacting the efficiency of the 6G ecosystem. Vulnerabilities in programs, limitations in programming languages, and numerous security and privacy ambiguities in internet connections are primary sources of these attacks. Such confusion can lead to compromised trust, financial losses in cryptocurrency transactions, or the unavailability of an internet connection or website.

Integrating digital currency within the 6G network architecture framework offers solutions for specific challenges and new opportunities. Public ledgers are more relevant than private ones regarding security routing concerns. For example, validating whether smart contracts have been updated becomes highly challenging since every node in a blockchain-based network is responsible for their validation. Smart contracts are an integral part of blockchain infrastructure, crucial for enabling automation and ensuring the legitimacy of transactions. Various reliability testing methods are used to search semantic faults to ensure the correctness of a smart contract. Moreover, rigorous monitoring of artificial intelligence (AI) blockchain nodes or malicious software with strict control over access and verification is essential. These solutions can withstand a wide array of attacks. Blockchain innovation enables the implementation of several security measures, including privacy by design and trusted execution environment (TEE), making it possible to construct more resilient networks. Below are some examples of networking types that a distributed ledger can accommodate.

There are various blockchain types, including open, closed, connection, and mixed networks. Utilizing different types of internet infrastructure gives rise to different privacy concerns. If, for instance, more than 50% of attacks against a particular 6G enterprise are executed through publicly accessible blockchains, proactive measures may become necessary. The subsequent step involves establishing either a consortium blockchain or a private ledger, which can enhance efficiency, reduce vulnerability to attacks, and better safeguard the confidentiality of a given dynamic node. Hence, introducing any blockchain system impacts specific risks and the diverse services offered in a 6G environment.

The emergence of quantum computing technology is anticipated to eventually replace all existing computational methods and cryptographic systems. It is suggested that vulnerabilities in 6G wireless networks could be detected, mitigated, and prevented using this approach. Networks leveraging 6G are proposed to achieve unprecedented dependability with quantum technology, enabling the transition from silent communication modes to cognitive-communication pathways. Several qualitative methods have been proposed to address the continual exponential issue in public key cryptography. Moreover, quantum computers are expected to strengthen their security infrastructure shortly. Based on its foundation in the atomic structure of information, quantum computing is widely expected to significantly anticipate novelty and security, enhancing the dissemination capabilities of 6G communication, which rests on quantum data.

Oblivious transfer is a conventional information dissemination method wherein the sender is unaware of the

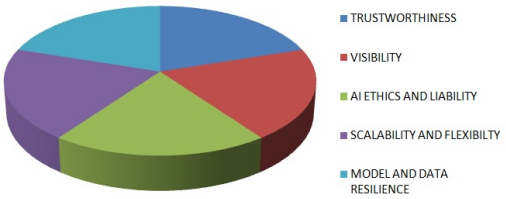

Fig. 3.3: Difficulties in applying ML/AI to 6G

specific information being transmitted. Yet, such information exchanges are not feasible in quantum computing, as any information leakage may disrupt a two-way connection. According to the quantum principle, systems lack a replicating property, rendering the precise replication of their states physically impossible. Thus, to successfully tamper with the data, an adversary must first extract its random quantum state and then replicate it into a duplicate without altering the original state of the data. A quantum collision could also occur if different values fed into a hash function yield the same result.

Numerous industries and academic institutions are investigating and creating Quantum attack solutions to address the increasing challenges of upcoming 6G communications. Several diverse quantum-proof algorithms are founded on lattice-based structures, hash values, or multiple variables. The issue related to computing on a lattice can be resolved by leveraging IoT devices, which offer enhanced performance, connectivity, and more. Since traditional random oracle models will not suffice with quantum-proof algorithms, it is crucial to authenticate security at multiple levels within a quantum-obtainable random oracle framework. This prevents adversaries from potentially querying the random oracle in non-relativistic time if the framework is unprotected.

The forthcoming 6G ecosystem will enable a wide array of automated tasks to be executed without human intervention, encompassing monitoring, computation, recovery, and optimization. Zero-touch infrastructure & services management (ZSM) is an emerging architecture that establishes fully autonomous wireless connectivity emphasizing cybersecurity through artificial intelligence and machine learning. As extensive sixth-generation mobile networks will generate massive volumes of data, wireless networks must incorporate artificial intelligence and machine learning to handle the resulting data overflow. The authentication checks in 6G connections can be enhanced using a diverse array of distributed cryptographic techniques based on artificial intelligence and machine learning. The primary benefits of this deployment approach are the precision and foresight of machine learning and artificial intelligence algorithms for cryptography within a 6G context.

There are challenges to overcome and rewards to gain when bringing AI and ML into a 6G setting. Some of the difficulties are described in applying AI/ML in 6G is shown in Figure 3.3.

The most demanding question that must be answered before using AI and ML in a 6G setting is whether or not we can have faith in these innovations to reliably and securely run a susceptible network.

3.3. Analysis of privacy-protecting methods for 6G-powered automobile communication. The global demand for cutting-edge autonomous vehicles equipped with advanced features has increased. The rapid advancement of virtual reality technology has raised concerns regarding security and privacy, thereby underscoring the importance of safeguarding both drivers' safety and privacy within a fully automated wireless environment. The extensive data collection from multiple devices to provide diverse consumer services necessitates implementing various security approaches that effectively protect this information without compromising user privacy. In the context of 6G networks, the transmission and management of voluminous data become significantly more complex, given the exponential increase in the number of end nodes compared to 5G networks. Balancing the delicate data security and privacy concerns within the 6G landscape while maintaining the current encryption techniques' privacy standards requires careful consideration of the data processing costs and the need for privacy.

Monitoring each device within the 6G wireless network poses a substantial challenge, potentially diminishing the efficacy and transparency of the data acquisition process. Consequently, adopting big data technologies

across distributed networks with a focus on ensuring privacy and security could increase the system's overall computation and transmission costs. Key obstacles to maintaining user security and privacy in a 6G network include the introduction of security vulnerabilities that may lead to the theft of users' personal information during extensive wireless communications. Additionally, the significant data accumulation facilitated by 6G technology could potentially compromise the privacy of individual nodes within the network as 6G ushers in a new era of AI-powered, high-tech devices, the deployment of various applications across the network's framework necessitates the development of innovative lightweight security measures at the network edge. Achieving this balance will require a stable environment prioritizing exceptional service provision while ensuring user safety and data privacy.

The careful management and restriction of access to data collected by various service-based applications is crucial for ensuring that these applications function as intended, especially concerning information related to the user's identity and immediate surroundings. In a 6G environment, blockchain technology presents a novel solution to address customer privacy concerns. While integrating blockchain technology into 6G networks offers numerous benefits, there are also potential drawbacks. Blockchain can potentially serve as a safeguard in maintaining data security within a 6G landscape. Blockchain enables users to maintain security without compromising their physical location or identity by functioning as a unified messaging system across the network.

It is important to note that blockchain, a form of distributed ledger technology (DLT), operates on a publicly accessible platform. Consequently, all user data collected within this framework may become publicly available. While 6G technology strives to establish a more secure architecture that enables reliable service-based and network-based activities, there remains a significant risk to the security and privacy of the data collected and the relationships established between dynamic nodes. Despite the potential for digital currencies to facilitate privacy objectives among distributed service-oriented devices, potential security and privacy concerns persist.

Digital certificates, CoinJoin, and similar techniques can effectively alleviate privacy concerns for consumers. One crucial area where privacy issues have significant implications is ML approaches, supported by cutting-edge and rapidly expanding AI techniques in the 6G environment. When utilizing a flexible 6G system, it becomes possible to securely store the user's personal information in specific devices distributed through AL/ML methods. However, there remains a risk that AI and ML-based methods might be susceptible to attacks from other AI and ML methods, resulting in data loss, alteration, or other unintended consequences. Various forms of artificial intelligence can be employed to safeguard users' private data, including messages, geolocation information, and other sensitive data. Within an AI/ML-driven framework, an attacker typically seeks to predict the next unpredictable outcome generated by the knowledgeable model during the training or testing phases.

The concept of quantum computing can be personalised to enhance reliability and increase efficiency in a 6G setting. As researchers explore better and more robust ways to protect users' privacy, these diverse and heterogeneous approaches can help maintain 6G wireless networks over time. However, the anticipation of integral applications and vast scenarios within 6G communication networks has amplified the significance of privacy protection and highlighted notable privacy-related issues, such as anonymity, node connections, and the lack of reports on the visibility of changing nodes within the wireless infrastructure. As a result, many individuals remain cautious about providing their personal information online. Consequently, employing randomized patterns to provide consent for sensitive data sharing has become a common approach to privacy protection. Several proposed approaches address confidentiality-related issues to mitigate the potential of adversaries studying private information.

4. Experimentation & Results.

4.1. Recommended model for asymmetrical privacy protection. In this ecosystem, we present DPSmartCity, an SDN-based technology that protects user confidentiality and provides network administrators more flexibility. Below are some code snippets to illustrate the core concept of our proposed solution. To address the limitations of current research, we introduce the DPSmartCity approach, designed to establish a thriving and efficient smart city leveraging the Internet of Things (IoT). The IoT infrastructure within a smart city ensures the security of individuals' personal information. The DPSmartCity framework comprises two main components:

1) A software-defined networking (SDN) enabled IoT-based smart city.

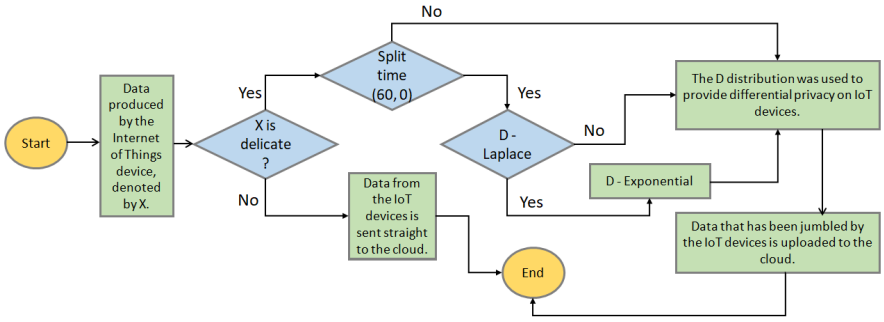

Fig. 4.1: Dynamics of Privacy-Preserving Mechanisms in Smart City IoT Infrastructure

2) A strategy for safeguarding individual privacy within the wired smart city, particularly when utilizing IoT devices with varying levels of confidentiality.

In the provided example, all IoT nodes are interconnected through an OpenFlow bridge, which is then linked to a central hub known as an SDN administrator. The software-defined networking (SDN) controller communicates with the cloud computing environment. IoT devices are interconnected in our smart city scenario, and their data is routed to OpenFlow switches through SDN. The SDN controller oversees and regulates these switches via wireless or wired connections. The correlation, highlighting the benefits of SDN infrastructure, can be connected within this innovative city concept, illustrated in Figure 4.1.

These advantages include enhanced mobility, remote administration, and centralized control while ensuring data remains confidential. The SDN controller maintains constant connectivity with both Cloud links, enabling it to receive instructions from the cloud and relay them to IoT devices, facilitating bidirectional data flow. First, the IoT-based smart city is integrated with the SDN paradigm, followed by the embedded approach that upholds user privacy, as depicted in the confidentiality technology flowchart presented in Figure 4.1. Upon the control system receiving modified data, it is directed to the SDN, eventually making its way to the cloud for further analysis by the SDN controller. Conversely, if the data isn't highly sensitive, the IoT device transmits it directly to the Internet.

When an IoT device generates private data, it employs differential privacy (DP) to safeguard this information. Within a connected urban environment, each IoT device has two options to choose from to protect user privacy:

1) A differentially private approach utilizing the Laplace probability principle.

2) A differentially private technique employs the inverse exponential probability.

The SDN controller updates the dissemination of the currently active differential privacy approach every hour. As a result, the distribution pattern of the utilized approach in vulnerable IoT devices fluctuates between Laplace and exponential probabilities on a minute-to-minute basis. Following applying one of these DP techniques, the device transmits the data directly to the Internet. Due to the continuous updates to the designated privacy protocol across all connected devices, the dynamic environment's fluctuations and intentional differential privacy intrusion are more effective in preventing the leakage of sensitive information. The detailed procedure can be expressed as follows.

Let us consider a scenario where information is transmitted between IoT devices and recipients as quickly as possible, but there are instances where information transmission may require several minutes. If data transfer exceeds a certain time threshold, the protocol switches to the alternative method during data transmission. Therefore, if the required time for communication delivery is denoted as $\tau_i = minp_i, M$, where it represents the time needed for successful communication delivery, notably, the value of p_i is directly linked to M, indicating that as the value of M increases, the probability of the approach being unsuccessful rises. Consequently, the value of p_i approaches one as the value of M approaches its maximum. Additionally, we interpret the symbol T as signifying an extended period during which any protocols are vulnerable to breach, further increasing the complexity of theft attempts. The initial decision regarding the protocol at the onset of the attack diminishes

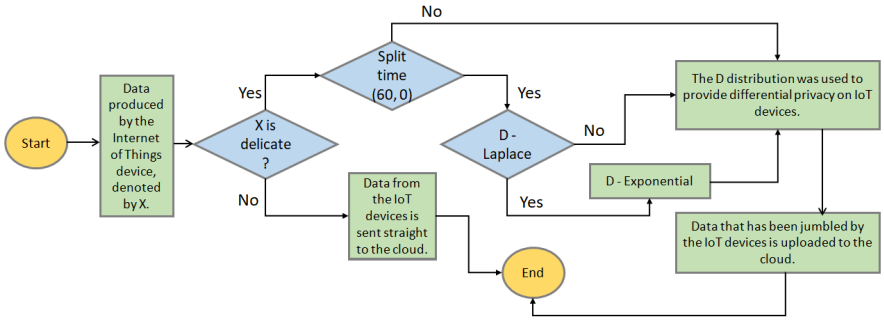

Fig. 4.2: Calculational effort and T's relationship

Table 4.1: CPU Usage Trends for Different Device Configurations

Time (s)	Number of Devices	CPU Usage (%)
1	500	22
4	500	20
14	500	28
1	165	16.5
4	165	16.5
16	165	16.5

the chance of success to one-quarter. Therefore, if denotes the likelihood of success at any given time (regardless of the technique employed), the probability of success is a quarter of the anticipated value of each of the remaining four techniques. The escalation in processing costs directly results from the mounting operational load. Moreover, interpreting as the probability of the entire process failing, will oscillate between its minimum value for lower values of M and its maximum value of 1.0 when M equals the value of T. Employing the method across multiple modes will help determine the optimal scenario, balancing computational expense criteria and the risk of total operation failure, yielding the most favourable outcome.

4.2. Simulation and Evaluation . The limited computational capability of IoT devices is a widely recognized fact. The current predominant concern revolves around the associated costs, which can only be comprehensively understood through practical application. In this section, we investigate the evaluation of the impact of our approach on IoT devices by examining its overhead. Upon implementing the DP smart city method, there is a discernible increase in the workload, which can be measured as a proportion of the devices' aggregate median augmented CPU utilization. The fundamental attributes of the simulation and the corresponding expenses will be explained below.

The SDN concept in a cutting-edge urban environment is introduced, capitalizing on the highly dynamic nature of the smart city's setting. The proposed process is simulated in C# using Visual Studio 2019. Expanding the total count of IoT devices, we observed a resultant increase in throughput, as depicted in Figure 4.2.

The relationship between the overall probability and the value T and the associated overhead is illustrated in Figure 6. The average CPU usage across the entire network is displayed in Figure 4.3.

To maintain conciseness, Table 4.1 presents the data on CPU usage in just four different states, although the general trend remains consistent across multiple scenarios. Notably, the proportion of CPU time utilized during processing tends to vary slightly across different runs. For instance, during the first, fourth, and fourteenth seconds, 22%, 20%, and 28% of CPU time were consumed by 500 devices, respectively. The current operational costs for 165 devices are as follows: there was a 16.5% increase in periods 1, 4, and 16 (s), respectively. Both the pre-execution surge related to data retrieval and the post-execution surge related to recording are transient,

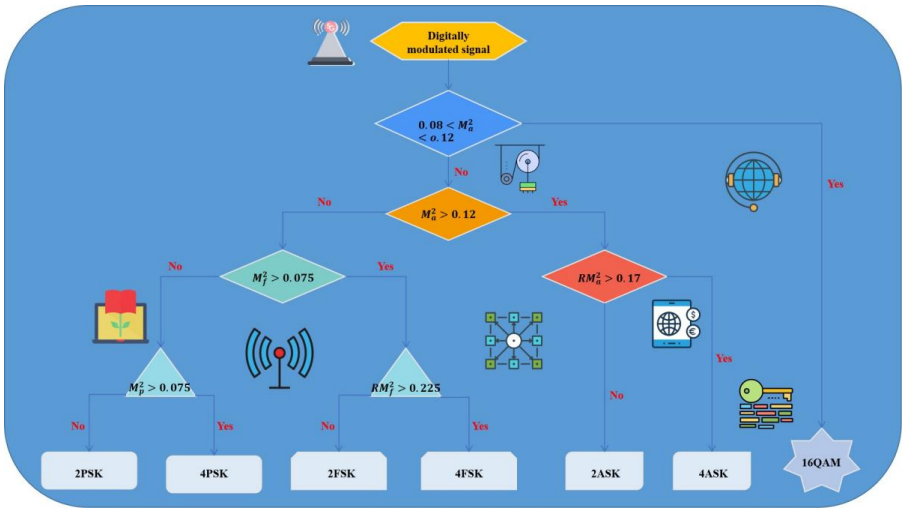

Fig. 4.3: Overall probability's relationship to the value T

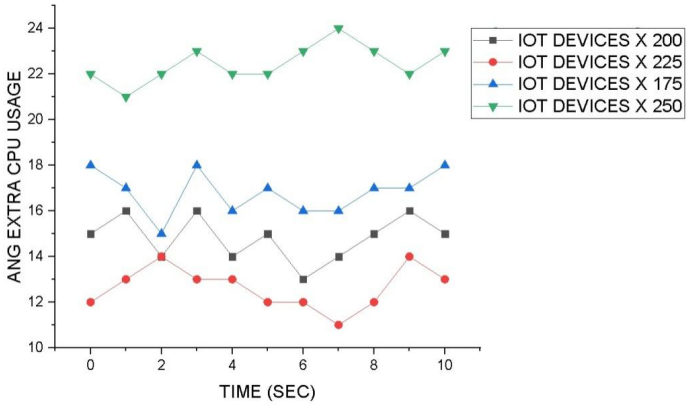

Fig. 4.4: Overhead analysis

with a slight potential capacity boost during this time. Our findings underscore the substantial cost implications for IoT devices.

As depicted in Figure 4.4, the proposed technique imposes only a 9–19% additional cost on IoT devices. Consequently, our approach can be implemented on IoT devices capable of accommodating the extra processing load. Moving forward, we aim to analyze the proposed approach from multiple perspectives, including assessing the proportion of successful hackers attempting to access confidential information. Additionally, we are keen on examining our approach's performance in scenarios where the allocation time may need to be adjusted.

5. Conclusion. Ensuring the security and privacy of consumers has always been integral to maintaining a reliable internet connection. With the advent of 5G networks and the anticipated rollout of 6G networks between 2026 and 2030, global connectivity can expand dramatically, linking various digital and physical systems, including automated vehicles and sophisticated technologies. This expansion escalates the complexity of potential threats, ranging from learning-enabled attacks to significant data breaches. In the context of 5G networks, the primary challenges include facilitating high capacity, strong connectivity, low latency, robust security, minimal energy consumption, extensive knowledge integration, and reliable networking. This study sought to address safeguarding users' privacy in 6G vehicular communication, considering historical perspectives

and future possibilities. It explored various advanced 6G innovations and their potential applications within the framework of Industry 5.0. Furthermore, the study conducted a comparative analysis of several privacy protection methodologies within the context of 6G mobile communication, examining the current state of the art and identifying the most effective approach for securing privacy in 6G-driven automobile communication settings.

REFERENCES

[1] Torres Vega, M., Liaskos, C., Abadal, S., Papapetrou, E., Jain, A., Mouhouche, B., ... & Famaey, J. (2020). Immersive interconnected virtual and augmented reality: A 5G and IoT perspective. Journal of Network and Systems Management, 28, 796-826.

[2] M. Gheisari, G. Wang, M. Z. A. Bhuiyan, and W. Zhang, "MAPP: A modular arithmetic algorithm for privacy preserving in IoT," in Proc. IEEE Int. Symp. Parallel Distrib. Process. Appl. IEEE Int. Conf. Ubiquitous Comput. Commun., 2017, pp. 897–903.

[3] Imoize, A. L., Adedeji, O., Tandiya, N., & Shetty, S. (2021). 6G enabled smart infrastructure for sustainable society: Opportunities, challenges, and research roadmap. Sensors, 21(5), 1709.

[4] Yang, B., Cao, X., Xiong, K., Yuen, C., Guan, Y. L., Leng, S., ... & Han, Z. (2021). Edge intelligence for autonomous driving in 6G wireless system: Design challenges and solutions. IEEE Wireless Communications, 28(2), 40-47.

[5] Nidamanuri, J., Nibhanupudi, C., Assfalg, R., & Venkataraman, H. (2021). A progressive review: Emerging technologies for ADAS driven solutions. IEEE Transactions on Intelligent Vehicles, 7(2), 326-341.

[6] Fragkos, G., Lebien, S., & Tsiropoulou, E. E. (2020). Artificial intelligent multi-access edge computing servers management. IEEE Access, 8, 171292-171304.

[7] Kaur, P., Kumar, M., & Bhandari, A. (2017). A review of detection approaches for distributed denial of service attacks. Systems Science & Control Engineering, 5(1), 301-320.

[8] Ameen, N., Tarhini, A., Reppel, A., & Anand, A. (2021). Customer experiences in the age of artificial intelligence. Computers in Human Behavior, 114, 106548.

[9] Wu, Y. J., Hwang, P. C., Hwang, W. S., & Cheng, M. H. (2020). Artificial intelligence enabled routing in software defined networking. Applied Sciences, 10(18), 6564.

[10] Li, M., Zhu, L., Zhang, Z., Lal, C., Conti, M., & Martinelli, F. (2021). Privacy for 5G-supported vehicular networks. IEEE Open Journal of the Communications Society, 2, 1935-1956.

[11] Talpur, A., & Gurusamy, M. (2021). Machine learning for security in vehicular networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 24(1), 346-379.

[12] Zuo, Y., Guo, J., Gao, N., Zhu, Y., Jin, S., & Li, X. (2023). A survey of blockchain and artificial intelligence for 6G wireless communications. IEEE Communications Surveys & Tutorials.

[13] Priya Kohli, Sachin Sharma, Priya Matta, Secured Authentication Schemes of 6G Driven Vehicular Communication Network in Industry 5.0 Internet-of-Everything (IoE) Applications: Challenges and Opportunities, 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC).

[14] Huang, J., Fang, D., Qian, Y., & Hu, R. Q. (2020). Recent advances and challenges in security and privacy for V2X communications. IEEE Open Journal of Vehicular Technology, 1, 244-266.

[15] Xia Feng, Liangmin Wang, PAU: Privacy Assessment method with Uncertainty consideration for cloud-based vehicular networks, Future Generation Computer Systems 96 (2019) 368–375.

[16] Wagan, A. A., Mughal, B. M., & Hasbullah, H. (2010, February). VANET security framework for trusted grouping using TPM hardware. In 2010 Second International Conference on Communication Software and Networks (pp. 309-312). IEEE.

[17] Sumra, I. A., & Hasbullah, H. B. (2015, February). Using TPM to ensure security, trust and privacy (STP) in VANET. In 2015 5th national symposium on information technology: towards new smart world (NSITNSW) (pp. 1-6). IEEE.

[18] Chatterjee, S., & Das, S. (2015). Ant colony optimization based enhanced dynamic source routing algorithm for mobile Ad-hoc network. Information sciences, 295, 67-90.

Edited by: Venkatesan C
Special issue on: Next Generation Pervasive Reconfigurable Computing for High Performance Real Time Applications
Received: Sep 26, 2023
Accepted: Dec 5, 2023