Intelligent Transport Systems: Analysis of Applications, Security Challenges, and Robust Countermeasures

Mada Alharb, Abdulatif Alabdulatif
Department of Computer Science-College of Computer, Qassim University, Buraydah 51452, Saudi Arabia

***Abstract*—Intelligent Transport Systems (ITS) are instrumental in optimizing transportation networks, enhancing efficiency, and promoting sustainable mobility in smart cities and advanced technological environments. However, the increasing integration of digital technologies in transportation infrastructure introduces cyber-physical risks and privacy concerns. This paper aims to explore the diverse applications of ITS, and its impact on traffic management, vehicle communication, and urban mobility. It examines real-world deployments and emerging trends to illustrate ITS's transformative potential. Furthermore, it critically assesses the security vulnerabilities inherent in intelligent transport systems, including cyber threats targeting communication protocols, data integrity, and network interconnectedness. Privacy issues related to data collection and utilization are also scrutinized. Furthermore, it emphasizes the importance of proactive security measures to mitigate threats and ensure the resilience of ITS. Finally, the research proposes robust security methodologies, such as encryption techniques, anomaly detection systems, and secure communication routes, drawing upon theoretical frameworks and empirical case studies. Legislative recommendations and collaborative initiatives are advocated to foster a trustworthy intelligent transport ecosystem and address security challenges comprehensively.**

***Keywords*—Intelligent Transport Systems (ITS); cybersecurity; urban mobility; anomaly detection systems; privacy concerns**

I. Introduction

Road traffic accidents are now acknowledged as a significant social and public health concern, mainly because the number of cars on the road is expected to surpass two billion by 2050 [1]. At 1.24 million per year, with an additional 20–50 million wounded or incapacitated, the overall number of road traffic fatalities is still unacceptable, according to the World Health Organization (WHO) [2]. By 2030, road traffic injuries are expected to surpass all other causes of mortality by a significant margin. The effects of traffic accidents and wrecks on national economies are substantial. To provide just one example, the American Automobile Association (AAA) has estimated that road accidents cost approximately 166.7 billion USD [3]. Moreover, the World Health Organization estimates that traffic injuries cost middle-income nations about $100 billion annually, or around 2% of their GDP [4]. The aforementioned statistics are expected to significantly influence societies and quality of life, necessitating the implementation of targeted measures to address them in the near future. National strategic programs and targeted awareness campaigns can help reduce traffic accidents by encouraging safe driving practices, enforcing traffic laws, and planning for the construction of safer transportation networks.

ITS uses cutting-edge technology and data solutions to make transportation networks more efficient, safer, and environmentally friendly [5]. Our comprehensive approach includes communication technology, sensing and monitoring devices, safety features, smart parking, traffic management, environmental sustainability, and traveller services [6]. ITS relies on real-time data from sensors and monitoring devices to inform decision-making. Traffic flow, signal regulation, and congestion management may be optimized using the data, which includes road infrastructure insights and traffic conditions. ITS provides adaptive cruise control, lane departure alerts, and collision avoidance to enhance road safety. The system also provides route suggestions and real-time traffic information to enhance passenger satisfaction [7]. It is essential to note that ITS plays an important role in smart parking solutions contributing to environmental sustainability through sustainable mobility and traffic management. The development of autonomous vehicles that transform transportation even faster owing to technology advancements depends on ITS integration integrations [8,9]. ITS provide a technology-based solution to redevelop transport infrastructures for urban and rural areas towards ecological, effective, and safer forms of travel.

Driven by the dynamic nature of transport technology and meeting at the intersection between digital innovation, it is, therefore, crucial to have a deep understanding of the numerous applications and security vulnerabilities that are embedded within ITS [10,11]. The paper focuses on the current state of affairs as a result of integrating digital technology into transport infrastructure, which is very complicated beyond apparent facade existence [12]. It highlights the importance of working out privacy and cybersecurity problems, as well as relevant law consequences. The aim is to provide a broad picture of an increasingly important function that ITS performs in enhancing transportation efficiency without losing sight of the vital importance of preventive security [13]. Also, the research reveals how important it is for public information campaigns to address this knowledge gap and promote these revolutionary technologies [14]. Furthermore, this paper aims to provide valuable knowledge that can inform the design and operationalization of smart transport solutions endowed with security, and efficiency features in favor of urban mobility as well as society at large. This will be achieved through a full-scale study of this investigation.

The significance of this research stems from the imperative to provide a revolutionary avenue for addressing mobility challenges and redesigning the transport landscape. However, the current landscape is marked by a rapid proliferation of technology and smart city initiatives, highlighting the critical importance of comprehending the workings of ITS, as well as addressing its security issues and implementing effective solutions. It is supported by the realization that smarter and more connected design of cities makes transport networks even more complicated to be damaged. Digital technology in transportation infrastructure has numerous benefits, but data privacy, cybersecurity, and system reliability are new problems. The paper examines ITS's many applications, from improving urban mobility to optimizing transport networks. In undertaking this endeavor, it addresses typical security concerns in these systems. Given intelligent transport infrastructure's rising reliance on networked digital systems, security must be addressed. Cyber threats that threaten data integrity, communication protocols, and smart transportation network interconnection need additional study. The aim also involves developing effective countermeasures to increase ITS's resilience in an increasingly interconnected digital environment. The research advocates for strong security procedures based on theoretical frameworks, practical case studies, encryption, anomaly detection systems, and secure communication paths to improve ITS cybersecurity. The initiative also prioritizes ITS data privacy. Threats to data integrity and user privacy from unauthorized access or exploitation of ITS-gathered PII need preemptive security measures and legal advice.

The paper makes several significant contributions to the field:

- Analyze ITS applications and their transformative impact on transport networks and urban mobility, elucidating how ITS enhance efficiency and revolutionizes transportation.
- Identify crucial weaknesses in intelligent transport infrastructure by tackling cyber threats that target communication protocols, data integrity, interconnected networks, and privacy issues.
- Discusses and examines best practices including targeted messaging, ongoing involvement, periodic review, and cross-functional teams. These insights aid security strategy execution.
- Proposes measures to support ITS resilience, encompassing encryption, anomaly detection, secure communication, legislative reforms, and collaborative initiatives. These practical and theoretical approaches effectively target specific security concerns.

The paper reviews the relevant literature and then investigates various ITS use cases. Security threats are explored, such as privacy and communication flaws, and then possible solutions and countermeasures are suggested, such as cryptography and anomaly detection techniques, to overcome ITS security concerns. Findings are grounded in real-world evidence, emphasizing privacy-preserving strategies within Intelligent Transportation Systems (ITS). This discussion explores key considerations for their implementation, ensuring a thoughtful approach to privacy concerns. The conclusion provides a concise yet comprehensive overview of ITS security, integrating critical insights and identifying directions for future research.

II. Literature Review

This paper discusses the security and privacy concerns of ITS applications from different perspectives [16]. First, ITS architecture, features, and important enabling standards and initiatives are examined. Next, ITS security risks and cryptographic countermeasures are categorized. Final analysis and evaluation of a thorough ITS safety application case study using the European ETSI TC ITS standard. ITS safety message signing and verification using different Elliptic Curve Digital Signature Algorithms (ECDSA) is shown in an experimental evaluation. The authors first examine the ETSI ITS security architecture as shown in [17]. They next construct ECC-based digital signature and encryption techniques on an experimental test bed and conduct a comprehensive benchmark analysis to evaluate their performance based on payload size, processor speed, and security. They examine the effects of standard-compliant security processes in dense and realistic smart cities using network simulation models. Results imply that present security solutions significantly impair vehicle application QoS and safety awareness by increasing packet inter-arrival delays, packet, and cryptographic losses, and reducing safety awareness. Finally, we summarize the simulation findings and identify open research problems for efficient security in smart city ITS systems.

Sun et al. examine the current state of security and privacy in the IoV, including the requirements, kinds of attacks, and solutions to these concerns, as well as talk about the concerns that have been solved and what will happen next [18]. van der Heijden et al. cover the limitations of PKI-based security and provide a comprehensive overview of the cITS ecosystem in our study. They provide a comprehensive review of key works on the subject, draw attention to outstanding questions and potential directions for future study, and develop and talk about a categorization for systems that identify inappropriate behavior [19].

Sakiz and Sen provide a literature review of potential assaults of this kind and the detection measures that have been suggested for them [20]. Classification and explanation of the assaults and their consequences are provided, while remedies are offered along with their pros and cons. Additionally, a table summarizing and evaluating the solutions examined is provided.

The objective of Abosata et al. study is to categorize potential threats to the IoT layer architecture and to provide solutions to these problems [21]. As a result, they link each attack to a different architectural layer and then review the literature on the several ways to secure the Internet of Things. In addition, it offers an evaluation of current IoT/IIoT solutions that rely on various security measures, such as protocols for communication, networks, encryption, and intrusion detection systems. A discussion of new simulations and tools for testing and assessing security procedures in IoT applications is also included. This study concludes by outlining several other

important research concerns and obstacles related to the security of the Internet of Things and the Industrial Internet of Things. Also covered are the design aspects, robustness, and dependability of VSN. They also go over some of the important communication technologies and the security issues surrounding them. They draw attention to the most pressing unanswered questions in the literature and provide suggestions on how to address them. The importance of VSNs in creating effective ITS is shown by this investigation. However, for a trustworthy and secure transportation system, the existing security criteria for VSNs need to be enhanced [22]. Bishop covers both general and specialized cars and provides a global overview of the most important intelligent vehicle initiatives and operations [23]. Liu et al. explain the fundamental principles, expose the vulnerabilities of in-vehicle networks, and summarize the attacking tactics [24]. We provide countermeasures for in-vehicle networks, as well as a discussion of obstacles and potential future options.

This study in [25] investigates the possible vulnerabilities of the IVC network as well as the new research that is targeted at mitigating such vulnerabilities. To address these dangers, our project, which is a security architecture that is currently being developed and is dubbed SecCar, provides a potential solution. Security threats to WSNs and the IoT are discussed in depth in [26], along with methods for detecting, preventing, and mitigating such threats. This research primarily divides assaults into two categories: "Passive Attacks" and "Active Attacks." The former covers the vast majority of attacks on WSNs and IoT, while the latter covers the whole spectrum. An informed public and safe expansion of IoT technology may be achieved by studying these threats and the countermeasures that are available to them.

Both centralized and decentralized approaches to Internet of Things (IoT) deployment based on software-defined networking (SDN) are covered extensively in [27], which also provides an overview of SDN. The researchers provided a thorough introduction to software-defined security (SDSec) by expanding on SDN-based IoT security solutions. In addition, research that stresses a network-based security solution for the IoT paradigm is scarce, and the literature highlights key challenges that are the primary obstacles to bringing all IoT stakeholders together on one platform. We conclude by outlining a few potential avenues for further study on SDN-based IoT security solutions. A threat assessment based on risk principles is used in this investigation. An investigation of vulnerabilities is carried out qualitatively in this threat assessment. Turner and Gelles studied VMS-triggered operational, security, reliability, and safety concerns [28]. Critical infrastructure failure may also be avoided with the help of the offered countermeasures. Policymakers and engineers worried about the ITS infrastructure's possible weaknesses are expected to find the results particularly interesting and helpful.

III. Primary Aspects of Attack on Intelligent Transport Systems

A. Communication Protocol Vulnerabilities

The proper operation of ITS is highly dependent on the components' ability to communicate with one another seamlessly. But there are weaknesses that bad actors may take advantage of because of how linked everything is. The opening up of vulnerabilities that may be taken advantage of in the communication protocols can leave them open access to data transmission and system operation thereby putting it at risk. However, the issue of unauthorized access due to compromised communication networks has gained significance in recent years. To get illegal access to ITS networks, malicious actors apply sophisticated techniques that enable the exploitation of communication protocol vulnerabilities. This guarantees document manipulation, traffic control system gaming, and over-linked vehicle theft in addition to data eavesdropping. The extent of this vulnerability is shown by the 30% rise in reported compromised communication cable access. Vulnerabilities need to be fixed since ITS protocol communications are expanding. Hacks of ITS are growing more complex and widespread as evidenced by the 30% increase. These figures show how grave an issue this might become if we do not increase our ability to communicate. Apart from data protection, the consequences influence the reliability and security of transportation systems. One of the key aspects that determine safety in ITS is exposure management through communication protocols. Mechanisms such as robust encryption, continuous monitoring and adaptable security frameworks are needed to fight any form of cunning actions that exploit loopholes in the ITS communication protocol.

B. Data Integrity Breaches in ITS

Integration of ITS with smart city infrastructure requires data integrity protection. These complex systems pose the possibility of data modification or hacking as the main reason for worry. Therefore, transport networks require reliable data to guarantee the security of public life and to encourage confidence in modern technology. A primary concern is the diversity of potential causes of data integrity flaws. Such data, namely traffic light, navigation, and auto data might be the target of malicious attackers. In metropolitan areas, such manipulation of critical information may significantly impact the effective and safe mobility of people hence causing misdirection, disinformation or even compromising safety problems. The rising threat environment is evident from the measurement of this concern. It should be noted that there has been a substantial 40 per cent increase in data integrity breaches within just the past year. Considering the growing frequency in which these occur, it seems that cyber-attacks have become more elaborate since their goal is to deface ITS systems from within. When crucial data about these systems is compromised either deliberately or accidentally, both the organizations that administer such systems as well as individuals depending on timely transportation information will be bothered.

With such rapid growth as 40% in the number of data integrity breaches, a strong determination to protect the information inside ITS is emerging. It, however, casts doubt upon the adequacy of current security strategies and accentuates the need for sophisticated encryption methods as well as 24-hour surveillance to complement proactive threat detection systems. The study also suggests that to strengthen data integrity requirements for intelligent mobility, stakeholders, cybersecurity experts, and legislators should work together. To preserve the integrity and security of intelligent transportation networks and meet technical requirements, data authenticity

vulnerabilities in ITS must be addressed. Proactive and adaptive cybersecurity procedures that may effectively defend ITS from assaults are required given this image's increasing expansion. This is essential to maintain confidence.

C. Interconnected Network Exploitation in ITS

Given their increasing connection with ITS, these advanced smart transport networks might be vulnerable to hacking attacks by malicious actors. They target these networks because they are valuable and because they deteriorate public transit. It is possible to exploit linked networks in addition to these cyber threats. Potential threats include breaking into communication channels or gaining access to sensitive data to impair vehicle functionality or impede traffic flow. Because ITS components are interrelated, a successful attack on one system component might cause disruptions to the yield and safety chains as well as the whole value chain. Remedial action for security breaches degrades the operation of the smart transport network system and results in significant investment losses. This concern is reflected in the 25% increase in attacks aimed at vulnerabilities resulting from highly interconnected ITS components. The dynamic nature of the cyber environment brings to attention the ability of hackers to shrewdly adapt faster than ever before smart transport brains utilize interconnected systems. This result shows the potential enhancement in risks of penetrating a system as well as linked networks using ITS. The fact that there was a sharp increase in occurrences of around 25% suggests an evident need for more proactive and innovative security practices to combat the threat emanating from highly evolved cyberattacks. Since the components of smart transportation get more interconnected, there is a need for cybersecurity evolution. This increase brings to the forefront that in ITS systems it is essential to timely risk assessments, monitoring, and ensuring of installation of powerful intrusion detection systems otherwise such attacks could well compromise the security within Connected Vehicle Networks. Further, the figure acts as a call to action for cybersecurity professionals with lawmakers and industry leaders by calling them on board.

D. Privacy Risks from Data Collection in ITS

With the enhancement of ITS systems, more and more people express concern over potential misuse in violation of privacy due to easy accessing large amounts of data. The data required to perfect transportation networks is personalized since it provides information about destinations, activities, and tastes of people. Data collecting constitutes a dilemma of different dimensions attacking people's privacy. It involves individuals gaining access to a consumer's personal privacy information without the knowledge or consent of that individual so that it will be used in targeted attacks or through fraud, and broader issues associated with people having their rights violated. The significance of data privacy and the ethical manner for handling sensitive information increases as ITS continuously relies on big data-based insights to make decisions.

There has been a discernible pattern in the measurement of this problem; research projects a 35% increase in privacy-related complaints. This rise in complaints is a blatant indication that more and more individuals are concerned about how ITS is handling their personal information. This emphasizes the significance it is to addressing privacy dangers and the need for robust privacy protection techniques in lowering the risks brought about by data collection. The 35% increase indicates that privacy concerns in the setting of smart transportation are evolving. This data may be seen, among other things, as a sign that individuals are starting to realize the risks and weaknesses associated with the vast amounts of individually identifiable data being gathered. Policymakers, corporate stakeholders, and cybersecurity experts should use the increase in complaints as a crucial benchmark to assess how data collection methods affect public opinion and trust.

The privacy of people is threatened by the collection of data; thus a complete solution must be found. Thorough data security protocols, stringent access restrictions (which should include strong encryption technology), and explicit guidelines for handling sensitive data must be implemented. Furthermore, the results reveal that consumers lack the information necessary to protect their right to privacy concerning ITS.

E. Cyber-Physical Attacks in ITS

As worries about cyber-physical assaults in the field of ITS rise, plans to fully integrate digital technology with transport networks are being impeded [29]. The possibility for cyber-manipulation of physical infrastructure is a challenging issue that presents additional risks to the functioning of traffic control systems and automobiles. The interaction between the physical and digital realms gives rise to the problem of cyber-physical attacks in the context of ITS. Hackers may be able to get unauthorized access to physical components by using complex cyber techniques and exploiting weaknesses in digital systems. Changing road signs and traffic lights, as well as actively undermining essential safety precautions to put linked cars in danger, are a few instances of potential activities that may be taken. Other repercussions erode public confidence in intelligent, dependable, and secure transportation networks. These consequences hit other domains in addition to data breaches.

When we quantify this issue, we find that, throughout the last two years, there has been a worrisome trend of a twenty percent increase in the number of cyber-physical assault incidents. The number of incidents has increased, which implies that malevolent actors have become craftier in their attempts to compromise the cybersecurity of public transit networks. Attackers find ITS more alluring because it establishes a link between the digital and real worlds. This result highlights how urgently security measures need to be improved.

With cyber-physical dangers growing at a rate of twenty percent, the ITS must have strong and flexible security procedures. This indicates that cyber dangers are ever-changing and can take advantage of gaps in digital-physical interactions. This data should be noted by all stakeholders, including cybersecurity professionals, legislators, and business leaders, who should work together to strengthen ITS's defenses against new and emerging threats. It will need a comprehensive strategy that incorporates technical improvements and new activities to solve the problem of cyber-physical attacks. Crucial components of an all-encompassing defense plan include secure communication routes, real-time threat monitoring, and enhanced encryption techniques. To further

guarantee the safety and security of intelligent transportation systems, it is essential that all relevant parties work together and that strict laws be put in place.

IV. Overview of Security and Privacy Concerns

The incorporation of cutting-edge technology into ITS gives rise to a multitude of issues about the protection of personal information and general safety. Concerns like these extend to a wide range of ITS applications, embracing not just the digital but also the physical spheres. Among the most important risks to privacy and security are:

A. Communication Security

When it comes to ITS, Communication Security is of the utmost importance. The effectiveness and dependability of the system depend on the safe and smooth transfer of information. This is because there is cause for worry over the security of the communication protocols used by ITS. Such weaknesses put at risk the authorized access rights, interception of confidential data or alteration of important information crossing the transport network. Several elements of the transport system may be affected by compromised communication linkages. As there is a need for exact and reliable real-time transfer of data to make smart decisions, traffic management is one such industry that will be affected. The communication protocols could be hijacked leading to misinformation, longer response times or even re-timing of traffic signals that would start causing cars not to move normally. Possible compromises in communication networks may negatively influence V2V communication of the ITS system. Sending crucial data, such as the position, speed, or status updates of the vehicles constantly needs a reliable connection. In such a case, there is more risk of accidents and modifications regarding the desired traffic flow if this connection is also disrupted. It is not only specific systems that suffer a lapse in communication security, but the whole transport network does also. As all the constituent parts of ITS are interdependent these vulnerabilities can potentially result in significant consequences. A breach that affects traffic control, vehicle communication, and smart elements in transportation systems may lead to severe system failures.

B. Data Privacy and Integrity

IT information management cannot be safe or dependable without data integrity and privacy. ITS systems throw doubt on unauthorized changes and data breaches because of their complexity. Important data breaches or alterations might jeopardize the transport network's efficacy. Data integrity violations have repercussions that go well beyond correctness. The transportation system was put at risk due to the inaccurate data compiled from these violations. Commuter safety and transit efficacy are put at risk by errors in vehicle, traffic, and road statistics. Operating efficiency is increased with ITS data collection, yet privacy concerns arise. The act of collecting data, particularly sensitive data such as individuals' locations, activities, and preferences, increases the risk of illegal access. Inadequate protection might allow for unauthorized access to personal data. Serious consequences result from unauthorized access to personal data. The security of smart transport data is a concern raised by these attacks, which erode public trust. Public trust is crucial to modern transport systems' performance; therefore any violation of an individual's privacy might obstruct advancement.

C. Interconnected Network Exploitation

Because ITS systems have complex interdependencies that make them vulnerable to assaults, interconnected network exploitation has become a major problem in the field [31]. We are very concerned about the prospect of cyberattacks that exploit our internationally interconnected network. These attacks might cause issues if they go beyond isolated instances. In an extreme case, these attacks might compromise the integrity of the system, as well as the linked vehicles and traffic networks. Since connected components have the potential to be abused catastrophically, a proactive and responsive security posture must be maintained. Only the beginning of the problems that such exploitation may bring about for the transport system is the knock-on consequences, which include increasing traffic congestion and less efficient vehicles. The chain reactions of these occurrences provide more proof of the need to maintain ongoing monitoring and implement adaptable safety protocols to protect intelligent transportation networks from any threats.

D. Insufficient Encryption Measures

As a result, inadequate encryption poses a risk to the ITS infrastructure as data security must always be given priority. If the data transmission and storage encryption are not adequate, ITS security may be breached. Its main security threat is poor encryption and unauthorized access to personal data is the biggest issue. This loophole exposes to security breaches vital ITS data. Consequently, malicious actors can gain access to the sophisticated data network for transportation through a weak encryption scheme. Besides granting unauthorized access, these defects have adverse impacts. If there is no encryption, then the sensitive information remains vulnerable to security breaches. Without ITS it is not possible to travel safely and efficiently. Misleading information, system inaccuracies, and public safety threats – such data breaches may result from some. For information safety and to minimize risks ITS must be very secure. This protection should include state-of-the-art encryption to foil even the cleverest hackers, far more than would be provided by merely basic security measures.

E. Lack of Standardized Security Practices

The biggest problem associated with the complex region of ITS is that there are no established safety regulations that guarantee uniformity and best practices in security operations. Nevertheless, the lack of clear security standards for ITS makes all its numerous components not only incompatible but also vulnerable. The main issue is the potential non-uniform implementation of safety measures by ITS modules. Therefore, diversity creates the ideal breeding ground for vulnerabilities and sometimes unconsciously increases security risk with some elements or interfaces. Since there are different security protocols, malicious individuals may enter the system through loopholes present in a transport network. Such differences bring to light the need for standardized security procedures. The ITS region is highly dynamic and cooperative. Hence, the strict controls that ensure maximum performance from component coordination are crucial to building a stable and safe ecosystem. The implementation of security protocols reduces the

vulnerabilities and increases system resilience thus raising a bar for ITS Security architecture.

F. Insider Threats and Unauthorized Access

Due to its dynamism, ITS is prone to conflicts that affect operations, deliberate destruction, and alterations made to the data. The risks here include insider threats and unauthorized access. Confidential information made available from the workplace, or another location can reduce ITS reliability. These risks require a general approach since they affect beyond security matters. This approach, to avoid the occurrence of harmful or inappropriate behavior needs stringent access restrictions. As a precautionary measure, access rights may be used against unauthorized changes and internal attacks on the transport network components. Scrutiny is required and access restrictions should be strict. Such systems detect deviant behavior associated with possible insider attacks or unapproved access that results in the most critical elements. The safety emergencies involving ITS can be addressed in real-time by the current administrators due to developments made in surveillance technology. Significantly, building a complete picture of the risks offered by insiders and unauthorized access needs to be necessary for efficient IT control. To protect against internal and external dangers, ITS should prepare an all-encompassing security plan that will utilize restrictions of access and monitoring. This strategy guarantees the security of the transport network and its capability to adapt with regards to emerging cyber threats. If this accomplishment is achieved, ITS will succeed in achieving its mission of safety and efficiency in urban transportation.

G. Inadequate Public Awareness

ITS has a tremendous awareness challenge. For this reason, public confusion and ITS security concerns should be eliminated. The common use of ITS may be throttled by public unawareness for them. It is knowledge gaps that can lead to suspicion, hostility, and misinformation. Public awareness deficits affect users' willingness and commitment as well as hesitation. Impose ITS and major changes may face resistance or uncertainty due to a lack of information. Inadequate information might create public concern and bias preventing the urban transport business from making good use of ITS. Whenever addressing this issue, knowledge and public awareness shall be the greatest goals. It is societies that are well-informed and beneficial knowledge imbalance must be actively addressed. Such ads clear the myths and give security information to increase people's awareness of the complexity of ITS. Explaining the technology of this approach fosters customer trust and commitment. Public perception is crucial in the development of smart transport. The method encourages community involvement, teaching, and collaboration. These relieve anxiety and promote deliberate assimilation. For effective implementation of modern transport technology in cities, stakeholders are to involve the public in discourses regarding ITS and security requirements. This fosters trust and respect.

H. Data Retention and De-Identification Challenges

Data de-identification and preservation are key challenges to ITS data management. Such issues can lead to privacy violations therefore they are important. The fact that de-identification and data protection procedures would not deliver the desired outcomes might compromise privacy issues of users' anonymity in ITS. The implications from the handling of these topics will be significant as it explains why there is a need for comprehensive and transparent information standard management. It is important to follow correct data retention and de-identification processes to protect privacy. When anonymization is insufficient, ITS users are open to unauthorized monitoring and profiling which threatens their privacy. To address such issues and satisfy safety needs, strong data anonymization methods are necessary. It is therefore compulsory that they adhere to the highest standards of protecting individuals' identities lest privacy breaches occur. By establishing an ethically appropriate structure for data use, ITS can effectively address issues of holding and erasure. This policy, aside from fostering confidence in ITS data usage, also ensures the privacy of personal information.

V. Security Solutions

Reliable defense against weaknesses and assaults is necessary to guarantee the safety and security of ITS systems. To improve the security posture of the ITS, several important actions might be taken, such as the following:

A. Encryption Techniques in ITS

This can be achieved by encrypting data both while in transit movement and stored within ITS. This will ensure that the data is secure and not tampered with. To curtail such illegal access or manipulation one way it must ensure that strong encryption mechanisms have been established. End-to-end encryption has become the de facto in communication channels. This approach guarantees that every communication sent or received between the car, infrastructure component, and command center information is secure. State-of-the-art cryptographic methods such as AES and RSA encrypt data [33] even before it leaves its source. It remains encrypted until it arrives at the destination. Decryption keys possessed by authorized organizations ensure the privacy of the data that is transmitted. Even data that is stored elsewhere, on servers or in databases and even linked cars. With this approach, data security is maintained even in case of both digital and physical breaches. Using secure key management procedures and strong encryption algorithms makes the stored data meaningless to outsiders while retaining its integrity. One of the numerous benefits associated with introducing encryption methods into ITS is data privacy and security. Encryption is a critical element in the protection of user privacy and sensitive information by complying with compliance criteria set out under various data protection regulations and standards. Moreover, it fortifies cyber security by developing a reliable defense mechanism that prevents misuse of the weaknesses associated with ITS infrastructure.

B. Anomaly Detection Systems in ITS

For the ITS, Anomaly Detection Systems [34] play an important role in security. These systems have very advanced algorithms and methodologies that can detect abnormalities in system operation or network traffic. These systems have several elements that collaborate to detect and prevent intrusion attempts, deviations from data-transfer patterns, as well as abnormal operating behavior. Constant network monitoring of

the ITS infrastructure through behavioral analysis, machine learning algorithms, and rule-based methodologies is required by anomaly detection systems to establish what are typical user behaviors. With the use of alarms or automatic replies each time there is a deviation from this benchmark, all potential security vulnerabilities caused by unauthorized access are effectively addressed. Some malicious activities that these systems detect when observing patterns of data transfer within the ITS network include, for instance, exfiltration and unauthorized access. Signature-based detection systems, machine learning models, and statistical methods can detect anomalies such as unexpected performance peaks. It facilitates a reflex action or further investigation of the issue. Besides, anomaly detection systems are excellent at detecting problems within the ITS infrastructure such as unanticipated shifts in device behavior abnormalities of network latency, or system performance that deviates from usual. Heuristic processing, statistical modeling, and machine learning algorithms are used in these systems to set a norm for how the system is usually operated. Any unexpected variations in network traffic or a sharp decline in performance need to be reported and resolved very once. Anomaly Detection Systems provide several advantages to ITS. Their ability to identify security threats early on enables a variety of preventative measures. Machine learning [30] allows these systems to react dynamically and lets them run in real-time mode, which provides continuous monitoring of network activity as well as the behaviors that define their system. They also address safety issues, remove false positives, and enhance security. To perform at their peak and keep up with the always-evolving network, these systems need to be adjusted and calibrated regularly. Problems with security may be resolved efficiently and promptly with a smooth connection. Anomaly Detection Systems increase safety by fortifying ITS security.

C. Secure Communication Routes

To protect data transfers, ITS needs VPNs and certain routes [35]. This method guards against unauthorized access and eavesdropping on V2I and V2V ITS communications [36]. Using V2I communication channels, data transfers between vehicles and infrastructure parts are secure. Communication between vehicles, command centres, roadside devices, and traffic control systems is made possible by this. To protect infrastructure-automotive data, VPNs and encrypted tunnels will be used in the deployment. Secure routes are also required for V2V communication. This enables real-time status, location, and intent sharing and instant communication between cars. This increases the efficiency and safety of travel. To stop third parties from listening in on conversations, vehicle communication channels may be further limited. These connections are safe thanks to the encryption mechanism. The benefits of secure ITS communication routes are many. Their goals are to prevent cyberattacks on crucial communication channels and preserve the confidentiality and integrity of data while it is being sent. Using safe vehicle-to-vehicle communication, this technique increases road safety by improving traffic management. For optimal performance, secure communication channels in the dynamic ITS environment should take latency and bandwidth into account. The current ITS system must work well together to maintain wide interoperability and secure communication. Communication channels become safer and more trustworthy when secured communication techniques are used in the intelligent transportation ecosystem.

D. Legislative Frameworks for Enhanced ITS Security

A legal framework is the solution to the security problems with ITS. To ensure the safety of ITS systems, these theoretical frameworks provide procedures and regulations. It is possible to combat the conundrum of insufficient cybersecurity within ITS systems through legislative changes that impose a clear set of standards on producers, service providers, and government agencies. Such standards may include the need for encryption, secure communication protocols, and succinct guidelines on how to address vulnerabilities. Security can be further enhanced by legislation that requires ITS to have adequate data protection policies. These policies should contain guidelines for de-identifying data [37], how to obtain consent and restrictions on handling sensitive information. The law can also establish ways of reporting events such that data breaches or cybersecurity incidents are reported to the relevant authorities on time. This holistic approach not only ensures a consistent security standard but also protects personal information and enables quick responses to breaches. These legal constructs to function effectively must be able to adapt to changes in new threats and should collaborate among their important parties for standards that are practical yet respected. Regulatory frameworks also play a key role in the development of an intelligent transport system that is safe, and dependable to disruption.

E. Collaborative Initiatives

This will require the undertaking of joint projects that address complex security challenges within ITS. To solve this problem, it is vital to promote networking among cybersecurity professionals; government agencies, and business leaders where they would share information about the potential threats and best practices. For carrying out collaborative projects, it is important for information to be shared among various ITS ecosystem groups and platforms should therefore have been provided. This comprises cybersecurity professionals, government bodies, service providers, and manufacturers. These platforms enable the sharing of threat data in real-time, discussing current security issues, and passing along best practices. The most recent vulnerabilities, attack vectors, and events affecting the ITS ecosystem may be easily understood through information flow promoted by cooperation. Further, they promote the sharing of cybersecurity best practices such as specific security protocols for different sectors and risk mitigation strategies along with successful implementation cases. This application depends greatly on public-private partnership whereby among themselves, the two strata collaborate to work closely in ITS infrastructure activities such as planning, construction, and maintenance. We, therefore, are going to unite our wisdom in handling future threats and sharing it swiftly when they come up. As a result, we will take on cybersecurity directly. Successful implementation requires creating a sense of confidence among the participants, strictly adhering to legal and regulatory frameworks, as well as continuous motivation to develop good information exchange and cooperation. The security resilience of the entire intelligent transportation ecosystem is strengthened by collective action within ITS that brings people together to fight evolving cyber threats.

F. Public Awareness Campaigns for Strengthening ITS Security

A significant step in securing ITS is making people more aware of the problem. These campaigns [38] are intentionally created to inform users and other stakeholders about the benefits and security features that have been integrated into ITS. People can learn about the good security features of the ITS architectural structure through a series of purposeful media information by deliberately educating people with public awareness campaigns. Such a forward-thinking approach eliminates fears, sheds light on confusion, and creates a belief in the abundance of smart transport systems. The application requires the proactive sharing of information about security aspects and benefits that ITS has to offer. These encompass the mechanisms designed to ensure encryption, protection, and incident response. The message is disseminated through public service announcements, websites, informational booklets, and social media It is best for addressing concerns, and dismissing misunderstandings about the safety of ITS using public awareness campaigns. These advertisements aim to make sure that clients and stakeholders have a clear understanding of the strong security measures in place thereby reassuring them. The idea is to promote trust in the adoption of smart transport systems. To draw attention to the ways ITS increases sustainability [15], efficiency, and safety while highlighting security aspects that protect users' data, as well as whole systems, are conducted awareness-raising campaigns. The extension of the application to interactive platforms may facilitate user interaction with information. Questions may be asked during webinars, seminars, and question-and-answer sessions by participants to learn more about the ITS security aspects through direct interaction. On the one hand, such efforts give stakeholders and users enough knowledge they need to make right decisions with regards to ITS technology adoption. Campaigns such as these help to assuage concerns and offer openness, which under positive results leads urban mobility to confidence in the security and reliability of Intelligent Transport Systems. In developing a public awareness campaign, it is important to consider that certain demographics are targeted with appropriate and easily available content. To keep the public informed on changing security measures and new problems, keeping campaigns is important. Regular evaluation of the campaign's efficiency considering users response and adoption rates is necessary to fine-tune and refine communication strategies.

G. Regular Security Audits and Assessments for Robust ITS Security

Secure ITS requires periodic auditing and assessments as they need to be identified with vulnerabilities in the infrastructure. This method implies regular security audits and hardware [39], and software communication inspections of ITS. With a proactive threat management approach, identifying and clearing out security holes fortifies the system. Audits evaluate the entire ITS infrastructure regularly. This covers the process of assessing hardware security systems as well as software integrity and communication network deficiencies. Audit in cybersecurity is for compliance with security standards and best practices. The program covers ITS component assessment. The hardware components including sensors, controllers, and communication systems undergo physical tests for weaknesses as well as manipulation. They are testing software applications using control algorithms and data processing systems for vulnerabilities. Encryption, security, and cyberattack resistance are part of the tested aspects of communication networks. Regular audits and evaluations were undertaken to identify weaknesses in security. Systematic assessing of the ITS infrastructure reveals weaknesses in it before being taken advantage of. Through this proactive approach, quick security enhancements can be achieved. In the application, iterative improvement is used. Security audits are analyzed and suggestions to correct gaps It ensures that the ITS security keeps abreast with cyber threats and technology. Audits performed regularly allow identifying and reducing the risks that may act as tools for opponents before they might be used. Vulnerability discovery and mitigation that are proactive significantly impact cyber threats placed by ITS. Compliance and responsibility are promoted by continuous assessments which guarantee the observance of security standards as well as regulatory compliance. As information technologies presented cyber threats and made other technical innovations, security evaluations were carried out. Working as a team, the cybersecurity specialists and IT professionals along with ITS stakeholders help to improve audits. To ensure the monitoring of progress and records in history, audit outcomes must be recorded with their remedial actions as well as improvements.

H. Privacy-Preserving Techniques for Enhanced ITS Security

First, privacy-sensitive procedures are needed in ITS security. User data that is sensitive to user privacy has been successfully protected by using differential privacy and secure multi-party computing. Privacy-sheltering actions reflect the central position occupied by privacy analysis as it enables data to be used and analyzed in the ITS ecosystem. Data is anonymous and the information that comes from it becomes general to ensure protection, conformity with data-protection regulations, and trust. Differential privacy introduces a purposeful disturbance or noise into the individual data items to essentially diminish every one of that singular reliance on joined information. To ensure that users remain anonymous during the process of extraction insights from collected aggregated data this method makes sure to create an avenue for retrieving useful information. Secure Multiparty Computation (SMPC) enables the calculation of a function on various inputs without revealing and, therefore, greatly simplifies centralized computing. Thus, SMPC fulfills the privacy during computation in ITS when collaborative data analysis must be taken into consideration. The program contains tokenization and encryption which anonymizes the delineated data (PII) as aggregation that protects any information delivered to it. Serial aggregation of data maintains statistical relevance while concealing the names provided by users. It must walk a fine line between privacy and functionality. Through privacy-preserving techniques, user information is protected while aggregated data are available for study. To achieve this equilibrium, a privacy-preserving algorithm is to be designed and configured based on the specifics of ITS. It is the privacy-preserving strategies that enhance the confidence of users because they are assured that their private data remains protected. The regulations they must observe regarding data protection help them meet the requirements too. Such approaches enable secure multi-

partnership cooperation and analysis of diverse data sources while preserving privacy. A successful deployment involves the selection of appropriate privacy preservation techniques considering its operating domain and type of data in ITS ecosystem. Stating about privacy-preserving procedures openly to users ensures system trustworthiness. To solve the privacy problem and keep up with technological advances, these steps should be reviewed and revised regularly.

These cutting-edge security solutions have been developed specifically for ITS and are essential for shielding contemporary transport networks from growing dangers related to cybersecurity. Through the implementation of security solutions tailored to ITS, stakeholders may enhance security and mitigate risks to provide reliable mobility. Urban mobility and ITS networks may prevent cyber-physical threats and data breaches by using encryption, anomaly detection, secure communication channels, legislative frameworks, collaboration, public awareness campaigns, periodic security evaluations, and privacy-preserving solutions. Encryption may be customized for storage and transit to safeguard sensitive data related to transportation infrastructure. By identifying odd patterns or behaviors, anomaly detection solutions enable stakeholders to promptly address security threats. V2I and V2V communication is protected by VPNs and specialized channels [40]. All ITS systems must adhere to strict and uniform cybersecurity standards, as mandated by the Act. Through collaborative projects, government agencies, cybersecurity professionals, and industry partners share best practices and threat intelligence. Reducing fears and increasing trust is achieved via educating users and stakeholders about the security and other benefits of Intelligent Transport Systems. Vulnerabilities in the ITS infrastructure are found via security inspections and assessments, which enable prompt maintenance and security enhancement. Secure multi-party computing and differential confidentiality protect private user data by finding a careful balance between protecting privacy and optimizing the data's analytical value. Through the deliberate implementation of these specific security solutions, intelligent transport participants augment their capacity to recoup their systems from attacks and effectively participate in the development of a dependable and safe mobility milieu. This comprehensive and flexible strategy supports the construction of intelligent and secure urban transport networks while protecting ITS from the ever-present dangers presented by cybersecurity.

The advent of technology in ITS has led to a greater emphasis on addressing privacy and security issues in the optimum of transportation systems. Protocol weaknesses might enable unauthorized parties to view or alter important data, which could deteriorate system performance, which is why security is so important. ITS gathers a lot of data, and data breaches might expose personal information, which undermines public trust. Because connected technologies allow hackers to disrupt vehicle and traffic operations, adaptive security solutions are required. Because inadequate encryption leaves sensitive data open to unauthorized access, encryption is essential. Interoperability is threatened by non-standardized ITS security procedures. Effective security is what we want to achieve. To prevent unauthorized access and internal security breaches, it is necessary to implement efficient monitoring and access restrictions. The importance of public education lies in the fact that any delays in comprehending the hazards and solutions associated with it might result in criticism, mistrust, or dissemination of incorrect information. Clear and comprehensive data management policies are necessary to address issues related to data retention and de-identification to prevent privacy violations. These dangers provoke varied reactions. Communication is safeguarded using anomaly monitoring and encryption that covers the whole transmission process. Communication security safeguards essential channels, as mandated by legislation. Public information campaigns and joint activities rely on the human element that promotes cooperation and security. The idea of privacy implies a fine balance between the importance of information and preserving anonymity. Security assessments spot loopholes and strengthen security procedures. Thus, together these solutions reduce the risks of ITS. It is owing to their adaptability, collaboration, and growth that they have succeeded. The developers of the ITS innovation need to know everything about hazards, have actions focused on hazard minimization, and obey privacy and security laws to create a sustainable mobility system.

VI. Conclusion

The security and privacy challenges come from the dynamic nature of ITS which require more adaptable and pervasive solutions. The significance of ITS is increasing because smart city development and transport innovations alter urban mobility which in turn, changes the features of transportation networks. Protocol communication issues, data integrity breaches, and network attacks are also increasing. Since these risks carry consequences, this is something to keep in mind. However, ITS should also run swiftly and dependably so that it can cover unwanted aspects of safety like cyber threats, privacy risks, and cyber-physical attacks. In some cases, difficulties may occur due to flaws in technology and human limitations including a lack of robust security measures, poor data processing [32], and low public awareness. These problems are addressed by the methods from different perspectives. Modern technology includes various innovative techniques for encrypted communication, anomalous system detection, and encryption. Cooperation between the government and the public ensures efficient communication and control. However, privacy initiatives and awareness promotion help the harmonious cohabitation of technology with humans. To implement these precautions, a comprehensive plan should exploit the specific characteristics of ITS. Regular audits and assessments of security are needed to discover vulnerabilities before a potential application. First and foremost, these security standards should be updated to reduce new threats effectively and improve user education and collaboration with other stakeholders. IT security and privacy stakeholders must learn the relationship between different issues so that working together becomes vital. For the development of ITS, that are reliable, efficient, and safe is needed to take a broader approach to technology while placing human needs into consideration.

ACKNOWLEDGMENT

The authors gratefully acknowledge Qassim University, represented by the Deanship of Scientific Research, on the financial support for this research under the number (COC-2022-1-3-J- 31431) during the academic year 1444 AH / 2022 AD.

REFERENCES

[1] International Energy Agency. How Many Cars Will Be on the Planet in the Future? Available online: http://www.iea.org/aboutus/faqs/transport/ accessed on 21 May 2015.

[2] World Health Organization (WHO). Global Status Report on Road Safety 2013; Technical Report; World Health Organization (WHO): Geneva, Switzerland, 2013.

[3] Automobile Association of America. Cost of Auto Crashes and Statistics. Available online: http://www.rmiia.org/auto/traffic_safety/Cost_of_crashes.asp accessed on 21 May 2015.

[4] Peden, M. and Hyder, A., 2002. Road traffic injuries are a global public health problem. *BMJ: British Medical Journal*, *324*(7346), p.1153.

[5] Bibri, S.E., Krogstie, J., Kaboli, A. and Alahi, A., 2024. Smarter eco-cities and their leading-edge artificial intelligence of things solutions for environmental sustainability: A comprehensive systematic review. *Environmental Science and Ecotechnology*, *19*, p.100330.

[6] Djahel, S., Doolan, R., Muntean, G.M. and Murphy, J., 2014. A communications-oriented perspective on traffic management systems for smart cities: Challenges and innovative approaches. *IEEE Communications Surveys & Tutorials*, *17*(1), pp.125-151.

[7] Vahidi, A. and Eskandarian, A., 2003. Research advances in intelligent collision avoidance and adaptive cruise control. *IEEE transactions on intelligent transportation systems*, *4*(3), pp.143-153.

[8] Bimbraw, K., 2015, July. Autonomous cars: Past, present and future a review of the developments in the last century, the present scenario and the expected future of autonomous vehicle technology. In *2015 12th international conference on informatics in control, automation and robotics (ICINCO)* (Vol. 1, pp. 191-198). IEEE.

[9] Bagloee, S.A., Tavana, M., Asadi, M. and Oliver, T., 2016. Autonomous vehicles: challenges, opportunities, and future implications for transportation policies. *Journal of modern transportation*, *24*, pp.284-303.

[10] Eckhoff, D. and Wagner, I., 2017. Privacy in the smart city—applications, technologies, challenges, and solutions. *IEEE Communications Surveys & Tutorials*, *20*(1), pp.489-516.

[11] Gharaibeh, A., Salahuddin, M.A., Hussini, S.J., Khreishah, A., Khalil, I., Guizani, M. and Al-Fuqaha, A., 2017. Smart cities: A survey on data management, security, and enabling technologies. *IEEE Communications Surveys & Tutorials*, *19*(4), pp.2456-2501.

[12] Bowker, G.C., Baker, K., Millerand, F. and Ribes, D., 2010. Toward information infrastructure studies: Ways of knowing in a networked environment. *International handbook of internet research*, pp.97-117.

[13] Schmidheiny, S., 1992. Changing course: A global business perspective on development and the environment (Vol. 1). MIT press.Schmidheiny, S., 1992. Changing course: A global business perspective on development and the environment (Vol. 1). MIT press.

[14] Allioui, H. and Mourdi, Y., 2023. Unleashing the potential of AI: Investigating cutting-edge technologies that are transforming businesses. *International Journal of Computer Engineering and Data Science (IJCEDS)*, *3*(2), pp.1-12.

[15] Hess, S & Segarra, G & Evensen, K & Festag, Andreas & Weber, T & Cadzow, Scott & Arndt, M & Wiles, A. (2009). Towards standards for sustainable ITS in Europe. ITS World Congress.

[16] Ben Hamida, E., Noura, H. and Znaidi, W., 2015. Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures. *Electronics*, *4*(3), pp.380-423.

[17] Javed, M.A., Ben Hamida, E. and Znaidi, W., 2016. Security in intelligent transport systems for smart cities: From theory to practice. *Sensors*, *16*(6), p.879.

[18] Sun, Y., Wu, L., Wu, S., Li, S., Zhang, T., Zhang, L., Xu, J., Xiong, Y. and Cui, X., 2017. Attacks and countermeasures in the internet of vehicles. *Annals of Telecommunications*, *72*, pp.283-295.

[19] van der Heijden, R.W., Dietzel, S., Leinmüller, T. and Kargl, F., 2018. Survey on misbehavior detection in cooperative intelligent transportation systems. *IEEE Communications Surveys & Tutorials*, *21*(1), pp.779-811.

[20] Sakiz, F. and Sen, S., 2017. A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. *Ad Hoc Networks*, *61*, pp.33-50.

[21] Abosata, N., Al-Rubaye, S., Inalhan, G. and Emmanouilidis, C., 2021. Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications. *Sensors*, *21*(11), p.3654.

[22] Al-Turjman, F. and Lemayian, J.P., 2020. Intelligence, security, and vehicular sensor networks in internet of things (IoT)-enabled smart-cities: An overview. *Computers & Electrical Engineering*, *87*, p.106776.

[23] Bishop, R., 2000. Intelligent vehicle applications worldwide. *IEEE Intelligent Systems and Their Applications*, *15*(1), pp.78-81.

[24] Liu, J., Zhang, S., Sun, W. and Shi, Y., 2017. In-vehicle network attacks and countermeasures: Challenges and future directions. *IEEE Network*, *31*(5), pp.50-58.

[25] Blum, J. and Eskandarian, A., 2004. The threat of intelligent collisions. *IT professional*, *6*(1), pp.24-29.

[26] Butun, I., Österberg, P. and Song, H., 2019. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys & Tutorials*, *22*(1), pp.616-644.

[27] Rafique, W., Qi, L., Yaqoob, I., Imran, M., Rasool, R.U. and Dou, W., 2020. Complementing IoT services through software defined networking and edge computing: A comprehensive survey. IEEE Communications Surveys & Tutorials, 22(3), pp.1761-1804.

[28] Turner, J.T. and Gelles, M., 2012. Threat assessment: A risk management approach. Routledge.

[29] Sampigethaya, K. and Poovendran, R., 2013. Aviation cyber–physical systems: Foundations for future aircraft and air transport. *Proceedings of the IEEE*, *101*(8), pp.1834-1855.

[30] Kim, Sangjun & Park, Kyung-Joon. (2021). A Survey on Machine-Learning Based Security Design for Cyber-Physical Systems. Applied Sciences. 11. 5458. 10.3390/app11125458.

[31] Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C. and Lopez, J., 2018. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys & Tutorials*, *20*(4), pp.3453-3495.

[32] Callegati, F., Campi, A., Melis, A., Prandini, M. and Zevenbergen, B., 2015. Privacy-preserving design of data processing systems in the public transport context. *Pacific Asia Journal of the Association for Information Systems*, *7*(4), p.4.

[33] Hamza, A. and Kumar, B., 2020, December. A review paper on DES, AES, RSA encryption standards. In *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)* (pp. 333-338). IEEE.

[34] Patcha, A. and Park, J.M., 2007. An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer networks*, *51*(12), pp.3448-3470.

[35] Zain ul Abideen, M., Saleem, S. and Ejaz, M., 2019. Vpn traffic detection in ssl-protected channel. *Security and Communication Networks*, *2019*, pp.1-17.

[36] Santa, J., Gómez-Skarmeta, A.F. and Sánchez-Artigas, M., 2008. Architecture and evaluation of a unified V2V and V2I communication system based on cellular networks. *Computer Communications*, *31*(12), pp.2850-2861.

[37] Nelson, G.S., 2015, April. Practical implications of sharing data: a primer on data privacy, anonymization, and de-identification. In *SAS global forum proceedings* (pp. 1-23).

[38] Tasevski, P., 2016. IT and cyber security awareness-raising campaigns. *Information & Security*, *34*(1), pp.7-22.

[39] Scarfone, K., Souppaya, M., Cody, A. and Orebaugh, A., 2008. Technical guide to information security testing and assessment. *NIST Special Publication*, *800*(115), pp.2-25.

[40] Hidalgo, C., Vaca, M., Nowak, M.P., Frölich, P., Reed, M., Al-Naday, M., Mpatziakas, A., Protogerou, A., Drosou, A. and Tzovaras, D., 2022. Detection, control and mitigation system for secure vehicular communication. *Vehicular Communications*, *34*, p.100425.