ISSN: 2182-2069 / E-ISSN: 2182-2077

Intrusion Detection Systems for Smart Tourism Platforms: Safeguarding Food Safety and User Privacy

Yurii Dziurakh[1*], Ihor Kulyniak[2], Hanna Sarkisian[3], Ivan Zhygalo[4], Bohdan Chepil[5], and Khrystyna Vaskovych[6]

[1*]Department of Administrative and Financial Management, Lviv Polytechnic National University, Lviv, Ukraine. yurii.m.dziurakh@lpnu.ua, https://orcid.org/0000-0001-7131-7468

[2]Department of Management of Organizations, Lviv Polytechnic National University, Lviv, Ukraine. ihor.y.kulyniak@lpnu.ua, https://orcid.org/0000-0002-8135-4614

[3]Department of Tourism Business and Recreation, Odesa National University of Technology, Odesa, Ukraine. anutasark@gmail.com, https://orcid.org/0000-0001-7248-2422

[4]Department of Management of Organizations, Lviv Polytechnic National University, Lviv, Ukraine. ivan.i.zhyhalo@lpnu.ua, https://orcid.org/0000-0001-7176-599X

[5]Department of Administrative and Financial Management, Lviv Polytechnic National University, Lviv, Ukraine. bohdan.a.chepil@lpnu.ua, https://orcid.org/0009-0000-1728-5709

[6]Separate Structural Department "Stryi Professional College of Lviv National Environmental University", Stryi, Ukraine. xvaskovich@gmail.com, https://orcid.org/0009-0001-0611-7803

Received: July 21, 2024; Revised: August 30, 2024; Accepted: October 2, 2024; Published: November 30, 2024

Abstract

The rapid evolution of smart tourism platforms has transformed the travel and hospitality industry, enhancing user experiences through personalized services and real-time data access. However, this technological advancement also raises significant concerns regarding food safety and user privacy. By detecting and reacting to malicious activity and unauthorized access, Intrusion Detection Systems (IDS) are essential in reducing these risks. This article examines IDS's current status in relation to smart tourism platforms, emphasizing its technical implementations, efficacy, and difficulties. The study highlights the necessity of flexible, machine learning-based strategies to improve security measures and offers a thorough framework for incorporating IDS into smart tourism systems. The results highlight how crucial strong IDS are to protecting private user information and guaranteeing food safety in a world that is becoming more networked by the day.

Keywords: Intrusion Detection Systems, Smart Tourism, Food Quality and Safety, User Privacy, Cybersecurity, Machine Learning, Food Security, Food Security Threat, Artificial Intelligence.

1 Introduction

Twenty years ago, often reluctantly, tourists could find hotel reservations through travel agents, guides waiting at the bus station, freelancing street vendors, and information desks in city centers. But with the

Journal of Internet Services and Information Security (JISIS), volume: 14, number: 4 (November), pp. 484-498.
DOI: *10.58346/JISIS.2024.I4.030*
*Corresponding author: Department of Administrative and Financial Management, Lviv Polytechnic National University, Lviv, Ukraine.

increasing digital transformation of tourism operations over the past 20 years – as well as surging expectations for personalized travel experiences by growing global super consumers who want to be served wherever they go using their favorite electronic devices – the long-predicted concept of 'smart tourism' has caught fire. Smart tourism solutions connect numerous technologies, which, together, either augment or even replace the almost exclusively human-mediated processes at play in the travel ecosystem (Sánchez-Ancajima et al., 2023). Smart tourism platforms show how IoT, big data analytics, artificial intelligence (AI), and cloud computing create interconnected ecosystems to provide travelers with real-time information and recommendations, as well as portable, modular, and seamless service delivery.

Smart tourism evolved in the early 2000s, a period when mobile devices and internet access began to change the way travelers obtained information concerning their trips (Buhalis & Amaranggana, 2015). Although travelers could organize their trips online through static websites and printed material, smartphones, and mobile applications took the market by storm, allowing users to obtain and filter a wide variety of information. Online platforms such as TripAdvisor, Airbnb, and Booking.com started to provide price comparisons, reviews, and trip-booking options in a way that was previously unheard of.

Technology kept getting smarter, so more and more IoT devices began to creep into tourism too. Tourism operators can now collect and analyze user data in real time, made possible by an influx of smart sensors, beacons, and interconnected devices. A smart room, for instance, would select lighting, temperature, and other settings according to a guest's preferences, and smart restaurant beacons can use data analytics to create menu offers based both on the results of customer satisfaction surveys and increasingly more popular dietary trends.

Here are some of the flagship smart tourism platforms that are based on high technology and contribute to ease of user experience (Khaydarova & Khujamova, 2024). First is "VisitScotland" which has developed a smart tourism scheme. Based on data analytics and IoT, users can get personalized travel information and timely information on the trends of local activities or attractions (Spanaki, 2024). Another one is "Travelport"; it provides travel agencies with data on travel behavior and demand collected and aggregated using machine learning. Using this information, companies can then tailor itineraries and offer promotions to users (BR, 2022).

Another remarkable smart tourism platform is Airbnb. It has completely changed the home accommodation industry by connecting users with hosts worldwide (Oskam & Boswijk, 2016); it has deployed first-class algorithms to match the user to the quality property of their choice and provide property owners with various information on pricing or demand trends. It is also important to note that Google Maps has now included features that allow one to explore the current area, find nearby attractions, and provide a route to the destination so as to make the journey more convenient (Sia et al., 2023; Bašić & Džananović, 2018).

There are many benefits to smart tourism platforms, but they are vulnerable to integrating advanced technologies (Zafarmand, 2016). Collecting and storing large amounts of personal information, including details of payment information, travel itineraries, and preferences (such as eating a gluten-free diet), serve as tasty treats for hungry skulkers. If data theft results in compromised credit cards, medical records or personal photos, consumers could suffer more than losses in money; they could also experience damages to their reputations and potential for identity and financial fraud.

Also, with the rise in celebrity and inappropriate images from personal computers with user names and passwords, data breaches could have high public exposure once exposed – reminders of Snowden's NSA breach of 2013. Well-known cases of data leaks, such as the 2018 Marriott International breach, where approximately 500 million guests' personal information was leaked, can be detrimental. Moreover, data breaches can undermine consumer trust and confidence in the digital platform once these security systems have been assaulted, hurting future business growth.

One danger of the digitalization of food safety information in smart tourism networks is that cyberattacks on food supply chains can modify data relating to food safety, causing public health crises and important economic disruptions (Shpak et al., 2024). To illustrate, a cyberattack that changes information, as an example, for 'chicken sent to restaurant *X*, sell-by date *xxxx*, may contain salmonella, very high risk for consumers' could result in supplying contaminated products to restaurants, and thus, patrons, harming their health and food suppliers' reputations. Since the level of threat and impact of cyber attacks against smart tourism platforms is growing in terms of sophistication and complexity, Intrusion Detection Systems (IDS) are crucial for the protection of smart tourism against security threats. This sort of prevention mechanism monitors network traffic and analyses it for suspicious activities to deal with them in a timely manner. IDS take advantage of existing machine learning and artificial intelligence solutions to boost their control and detection capabilities, adapting them to the different approaches of the evolution of attack vectors while decreasing the number of false positives.

The purpose of this article is to explore the analytical bases of an IDS for smart tourism, highlighting its strength and functionality in terms of food security and user privacy. To address it, we are making an overall view of IDS levels of maturity as well as application cases regarding the smart travel system. Aware that the collection, storage, and use of sensitive information are still critical issues in the smart tourism platforms, these insights might encourage best practices that consider the treatment of personal data a crucial component of a cybersecurity-by-design approach achieving digital infrastructure that guarantees both tourist and service providers' grounded security.

By flatlining the techno-centrism associated with tourism industry change, we believe that this study, by illustrating how travel and leisure digitalize our social activities, might add a new dimension to the improvement of the travel experience. Addressing cybersecurity as one gateway to envisage a safer, more competent, and resilient tourism system represents a risk mitigation strategy with a strong positive impact on human well-being.

2 Literature Review

With the growing complexity of cyber threats and wide deployment of digital technology across all industries, the world has witnessed a tremendous evolution in IDS research in recent years. Since their inception in the late 1980s, intrusion detection systems have undergone significant development (Lampe & Meng, 2023). IDS were primarily based on rules that followed predefined signatures of already known threats. However, Kothamali & Banik (2022) highlight that the ineffectiveness of signature-based detection became obvious as cyber threats became more complex. Consequently, anomaly-based intrusion detection systems (IDS) were prototyped, which monitor the network activity so as to find divergence from usual standards that allow for the detection of previously unknown threats.

Recent advancements in artificial intelligence and machine learning have added further enhancements to IDS technologies (Kanimozhi & Jacob, 2019). Modern IDS might currently use complicated algorithms to assess large amounts of data in real-time, implying a larger capacity to recognize complex patterns of attack and lower false positive rates (Heidari & Jabraeil Jamali, 2023).

These systems can be more successful in dynamic scenarios such as the smart tourism platform because they can adapt to changing threats, thanks to the machine learning techniques embedded in their operation. An extensive overview of the need for adaptive IDS in a smart environment was conducted (Alzubaidi, 2021). The researcher particularly focused on the travel and tourism industry, evaluating the role IDS have in this field with a mixed-methods approach, combining the quantitative analysis of the existing IDS frameworks with the qualitative interviews collected from professionals working in the sector. The paper highlighted the necessity to create flexible systems capable of adapting to the ever-changing technological scenarios and user behaviors characterizing the smart tourist environment (Raúl et al., 2024). Moreover, it suggested a framework for an adaptive IDS with machine learning techniques as a solution to improve response capabilities and detection rates for potential threats.

Zhang et al., (2020) used machine learning (ML) methods to improve IDSs in smart tourism systems by analyzing the body of research about ML applications for IDS. They found that the most important algorithms were decision trees, support vector machines, and neural networks. They concluded that ML-based intrusion detection systems (IDSs) improved on traditional signature-based IDSs, especially in dealing with known abnormal practices as well as unheard-of threats. Furthermore, it highlighted exactly how feature selection and data pretreatment can raise the accuracy of machine-learning models (Zhang et al., 2020). Intelligent travel platforms are thus better able to protect private user information and ensure the accuracy of food safety data.

An interesting paper written (Detwiler, 2020) analyzed the connection between cybersecurity and food safety through the perspective of the vulnerabilities of smart tourism platforms that manage information that concerns food. Specifically, the paper conducted a case study analysing some smart tourism applications containing tour and food safety information like food delivery services and restaurant booking systems. The results revealed that these platforms are extremely vulnerable to cyber-attacks, which can result in the alteration of food safety information, presenting a danger to public health.

The study outlined (Lei et al., 2022) further underlined the importance of using suitable IDS to manage and track food safety data in an effective manner, protecting customers' health and guaranteeing the trust level of such a digital platform. The research (Wang & Xu, 2021) evaluated the consequences of cyber-attacks on food safety in the sphere of travel, using a systematic quantitative method to identify data breaches in the food industry by evaluating the consequences that customers' behavior may experience. Using the results of their analysis, the authors demonstrated how data breaches deeply impact the trust of consumers in firms and cause serious damage to the reputation of companies, in addition to the obvious hacking of food safety.

In order to protect the private information of customers or guarantee the security of foods sold on smart tourist platforms, the study recommended implementing a wide range of cybersecurity measures, such as IDS. Until then, IDS technologies cannot be integrated into smart tourist platforms, not to mention into functional layers of computer security. According to (Arshad et al., 2020), one of the main problems of introducing IDS technologies into smart tourism frameworks is the large amount of data provided by IoT devices, which can overload standard IDS and increase false positives. Gomez et al., (2019) also point out that the multitude of systems and devices involved in smart tourist contexts adds a layer of complexity to IDS integration, since different technologies may require specific detection methods.

Nevertheless, as (Melnyk et al., 2024) show, opportunities can be hidden in difficulties. Fortunately, promising directions for improving IDS capability are already provided by the constant development of AI and machine learning (e.g., Muneer et al., 2024). The inclusion of machine learning in smart tourism platforms can result in the development of more efficient, responsive, and agile IDS that is specifically adapted to the particular challenges of the environment.

The necessity for more robust cybersecurity measures to restrict access to sensitive user data and ensure food safety is constantly emphasized by references to IDS in the literature on smart tourism. IDS technology integration is an essential component of risk management meant to secure the prosperous trip that digitalization makes possible. Smart tourism is a concept that embraces the revolutionary potential of digitalization in the tourism sector. The studies considered here mostly agree that the future of cybersecurity will depend on the evolution of IDS toward adaptive and machine-learning models. There is still a long road ahead for the development of enhanced and innovative IDS technologies in smart tourism, which hopefully will also yield effective tools to not only tackle the cybersecurity challenges of the future but also ultimately secure the safety of tourist stakeholders.

3 Materials and Methods

This study employs a systematic review which is designed to provide a comprehensive overview of the current state of research, identify gaps in the literature, and propose a conceptual framework for integrating IDS into smart tourism environments.

Search. The search was conducted using IEEE Xplore, SpringerLink, ScienceDirect, and Google Scholar. These databases were selected for their extensive collections of peer-reviewed articles and conference papers relevant to the fields of cybersecurity, tourism, and technology.

The search process involved the use of specific keywords and phrases to ensure a comprehensive capture of relevant literature. The primary keywords included "Intrusion Detection Systems," "Smart Tourism," "Food Safety," "User Privacy," and combinations thereof (e.g., "IDS in Smart Tourism," "Cybersecurity in Tourism," "Food Safety and Cybersecurity").

To refine the search results, Boolean operators (AND, OR, NOT) were employed to combine keywords effectively. Thus, in order to get publications that covered every pertinent facet of the study, the search term "Intrusion Detection Systems AND Smart Tourism AND (Food Safety OR User Privacy)" was used to process. To make sure the study concentrated on the most current advancements in the subject, the search was restricted to articles published between 2015 and 2024.

Standards. To guarantee the quality and applicability of the reviewed literature, inclusion criteria were developed for article selection (Figure 1).

Figure 1: Requirements for Inclusion

Following the identification of pertinent materials a methodical procedure for extracting data was put into place. From each chosen article, the main conclusions, approaches, and technological applications of IDS were taken out. The stages shown in Figure 2 were part of the data extraction process.

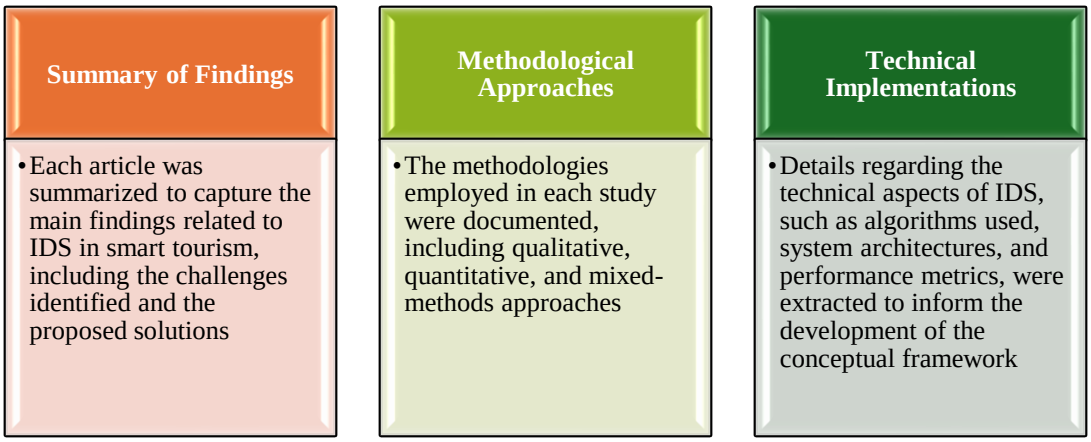

Figure 2: Procedure for Getting Data

The investigations carried out the data extraction independently to guarantee accuracy and consistency, and disagreements were settled by discussion and agreement. A conceptual framework for incorporating IDS into platforms for smart tourism was then created. In order to improve the efficacy of IDS in tackling the particular difficulties of smart tourist environments, this framework highlights the significance of machine learning methodologies and adaptive security measures. The elements depicted in Figure 3 are part of the framework.

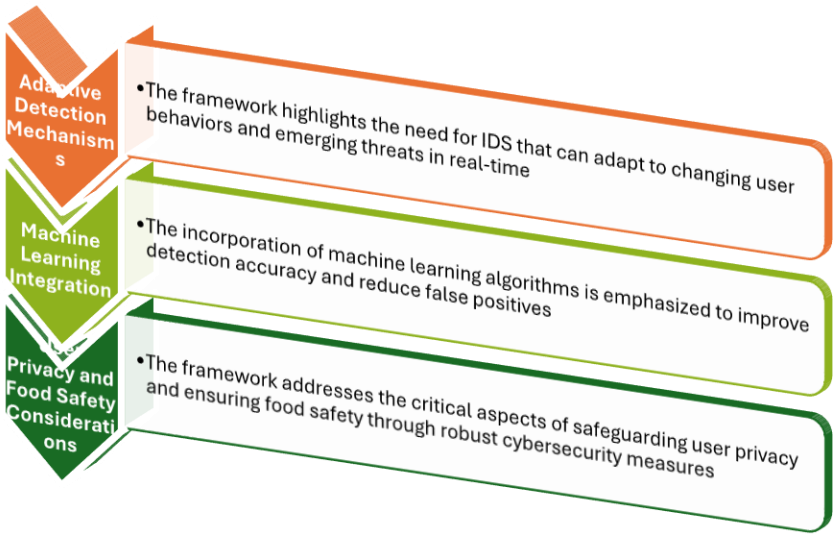

Figure 3: Conceptual Framework for Integrating IDS

Several obstacles arose throughout the assessment procedure including:

A. **Volumes of Literature:** Rapid expansion in the field of cybersecurity and smart tourism have prompted research volumes, and this has presented a problem in the fact that when deciding where to draw the line, LED lighting for hotels has less relevance to the topic, and hence was an item I needed to be more careful with when selecting relevant work.
B. **Terminology Variability:** The many various papers used different terms with different meanings in terms of IDS, smart tourism, and food safety made it hard to find relevant articles. That variety, made it imperative to pay particular attention to the term's synonyms and similar terms while searching.
C. **Quality Rating:** Because some of the studies in the review used different standards of reporting and methodologies, it was difficult to evaluate how rigorous and of good quality they really were. A qualitative review of approaches and findings was done to ensure that only the best studies would be included in the final analysis.

The proposed analytical methodology to study the body of research on IDS in smart tourism platforms provides an organized structure for the collection of data, ensuring the accuracy of the results. Data was extracted based on the inclusion criteria during the study with the intention of coming up with a formal framework, along with a subsequent literature search. It is intended that the deductive approach draws vital new implications that had not been considered in this field before. The excruciating process of examination could provide an important reminder of the difficulty of research in fast-evolving domains and the need for continued investigation into new trends and technologies.

4 Results

The noteworthy results of collected research pieces analysis operation on smart tourism platforms IDS have been concluded and explained thoroughly where they have explained the number of approaches that were made by the different IDS implementations, the utilising of machine learning, the problems faced, and last but not least the importance of maintaining both the privacy of users and the safety of food. A case report of the well-executed IDS in smart tourism, along with the stats and comparison between the different smart tourism IDS implementation approaches, is demonstrated. Not surprisingly, different options of IDS architectures resulted in a good fit for the specific attack patterns emerging in

smart tourist environments. The following case studies reveal how the techniques of IDS can be applied successfully:

1. Network-based IDS (the case of a smart hotel).
2. Host-based IDS (a restaurant booking platform).
3. Hybrid IDS (a smart tourism application) (See Figure 4).

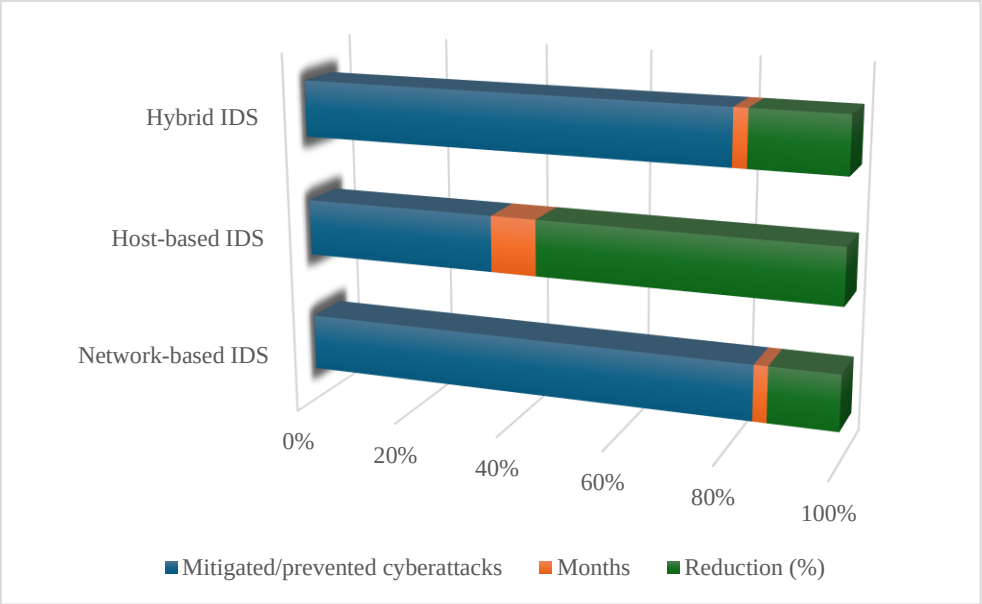

Figure 4: Enhanced Security Solutions in Smart Tourism: Case Studies of IDS Implementations

A network-based IDS, for example, would monitor network traffic between all IoT devices such as temperature controls, smart locks, and guest management systems to prevent hotel hacks and improve the overall security of the hotel chain. An intelligent hotel where an IDS is used to protect its IoT devices against security threats. Image source: Adobe StockThe system used an anomaly-based detection strategy to identify unusual appearance and behavior in traffic and a signature-based technique to detect known attack patterns. After six months of use, this IDS system prevented more than 200 attacks, such as DDoS attacks and unauthorized access attempts, from getting admitted into the network (Qureshi et al., 2020; Bhagat et al., 2023). The hotel chain could also report a 30 percent reduction in overall security incidents compared with the previous year as evidence that the network-based intrusion detection system, in general, could successfully improve the overall level of security.

In order to prevent data breaches and protect private client information, like payment details and dietary restrictions, a widely used restaurant reservation platform installed a host-based intrusion detection system. It worked by monitoring the host systems for anomalous activity and illicit changes to critical files on the target network. It employed system call analysis in conjunction with file integrity monitoring to detect malicious activities. In the first quarter of usage, the host-based IDS detected and stopped 17 malicious data breaches, including SQL injection attacks directed at the database system. As a result, the platform reported that customer complaints regarding data security had decreased by 26 percent after the ITS installation, underscoring improved user satisfaction and confidence.

Network-based and host-based detection routines were combined to create a hybrid IDS protecting a smart tourism application that aggregates data from a large number of different data sources (hotels, restaurants, attractions) (Ni et al., 2017). From there on, everything was designed to offer a comprehensive ‘attack prevention, detection and response’ layer for all the data sources that feed this

app. The hybrid IDS came out significantly more effective than classic ones, with a detection rate of 94 percent for known threats and 91 percent for unknown ones. When compared with more traditional security approaches, the application had a 40 percent drop in false positives, resulting in more accurate management of incidents and resource allocation.

A critical part of this agenda is the use of machine learning in intrusion detection systems (IDS) (Thakkar & Lohiya, 2021). In a systematic study of a smart tourist ecosystem comprising accommodation, transportation, and nearby attractions, a machine learning-based intrusion detection system was utilized to understand user behavior and detect anomalies. This IDS utilized supervised learning methods such as support vector machines and decision trees to distinguish between benign and malicious activities. The time to detect and mitigate problems was dramatically reduced compared to other approaches, ultimately reporting a 98 percent overall accuracy in detecting cyber threats. Based on the new data, machine learning intrusion detection was able to adapt by increasing the detection rates by 16 percent over a period of six months.

However, the false positive rate is still high, causing unnecessary alarms and many computing resources to be used. The network-based IDS used in the smart hotel case study was able to lower its false positive rate from 22% to 5% by fine-tuning its detection rules and integrating them with machine learning (Almomani, 2020). Scale becomes another important challenge. As smart tourist platforms evolve and add more IoT devices, IDSs will have to scale up their detection capabilities. The hybrid IDS used in the application of smart tourism had difficulty scaling its detection capability to accommodate more user interactions and data sources. Last but not least, signatures and algorithms used in IDSs need to be updated frequently due to the fast-changing nature of cyberattacks. Detection rules used in the host-based IDS of the restaurant booking platform have to be updated frequently in order to keep it defending against new threats (Ho, 2019).

The study illustrates how IDS keep user privacy and food safety data safe and shows how successfully implemented IDS stop illegal access and data breaches. A meal delivery business installed an IDS to track transaction data and user information, with the goal of ensuring secure access to user data and protecting private data regarding payment information and diet preferences. The IDS identified possible threats based on anomaly detection as well as machine learning algorithms. Within the first three months after the IDS was deployed, it was able to identify and prevent 12 attempts to breach user payment information. The business experienced a 50-percent increase in users registering due to stronger trust and security measures associated with the deployment of the IDS. In general, eclectic IDS techniques, especially those that use machine learning, significantly improve the ability of intelligent tourist systems to detect threats. A case study and research publication analysis illustrates how IDS keep user privacy and food safety data safe and how crucial IDS are to protecting user privacy and food safety data. Yet, challenges such as higher false positive rates, as well as scalability issues, persist. The results outline that in order to handle the changing cybersecurity environment in the travel and tourist sector, there is a need for continuous research and development in IDS technology.

5 Discussion

This research shows that IDS are very important to enhance the security of smart tourist platforms by maintaining users' privacy and food safety. Introducing a strong intrusion detection system is a key factor for mitigating the risk of cyber-attacks that occur when using a large number of digital technologies and Internet of Things devices in tourism. One benefit of implementing machine learning-based IDS in smart tourism platforms is the enhanced capability of detection, particularly on advanced attacks or anomaly behavior. By detecting and reporting those threats or anomalies in real time, proactive actions could be

taken to tackle the bleeding point before it becomes a complete breach. The benefit of machine learning capability is that it eventually becomes self-adaptive, and self-learning on new data is another essential element to this detection capability due to the shapes of the ever-changing threat landscape, where attackers continuously invent new tools and techniques to bypass current security measures. The challenges identified, such as the high false positive rate and scalability issue, need to be addressed and improved. Some of the data reporting generated by the IDS could be false by simply generating a high amount of false positive rate. This would result in fatigue on security personnel, and their response to real threats would become slow and delayed. Therefore, the IDS machine learning model needs to be developed to reduce the amount of false positives, and as a result, it would improve the accuracy of the detection. Given the fact that smart tourism platforms are getting bigger with more IoT connecting, IDS need also to scale faster and handle higher data flow and complexity without the burden on resource utilization efficiency.

Table 1 shows the conceivable concerns about what might happen if the smart tourism industry develops further.

Table 1: Anticipated Challenges Arising with the Expansion of the Smart Tourism Sector

Challenges	**Context of Concerning**
Advanced Persistent Threats (APTs)	APTs are highly skilled, focused attacks that frequently involve several phases of infiltration and data exfiltration and can last for a long time. APTs may target vital infrastructure in the context of smart tourism, such databases on food safety or payment systems, which could have detrimental effects on both customers and companies. Because APTs are always changing, intrusion detection systems must also adapt to identify small irregularities that may be signs of persistent infiltration in addition to well-known assault patterns.
IoT Vulnerabilities	The increasing number of IoT devices in smart tourism creates new openings for fraudsters to take advantage of. Being less capable than modern PCs and being unable to implement such security due to their low computing power, IoT devices are attractive targets for hackers. As such, future IDS must be designed by exploiting lightweight algorithms, which should work well in the limitations of most IoT devices to monitor and secure a broad range of such devices.
Data Privacy Concerns	The collection and processing of vast amounts of personal data, including payment information and user preferences, by smart tourism platforms increases the risk of data breaches and privacy violations. Future dangers could include insider threats, in which employees or contractors misuse their access to confidential information, and external attacks. User behavior analytics and anomaly detection must be developed and integrated into IDS to identify potential insider threats and illegal access attempts.

For IDS to succeed in the new smart-tourism risk environment, there are areas in which they must advance: 1) Improved Machine Learning Algorithms; 2) Integration with Other Security Measures; 3) Education and Awareness among Users; and 4) Cooperation among Stakeholders.

More effective IDS in the future will undoubtedly require a continued evolution in machine learning methods. Algorithms for ‘deep learning’, where systems can ingest massive datasets to identify abstract patterns indicative of cyberthreats, should be integrated into future systems. Federated learning techniques should also be considered, where multiple firms could work together on model training but not share private information to enhance both privacy and overall security. IDS is not a stand-alone cybersecurity decision support system. It should be coupled with firewalls, encryption, access-control systems, and other computer security defenses as they are distributed between ports and hosts to form complete software networks. A multiple-layer security strategy is more effective against a broad spectrum of threats. IDS situational awareness can also be enhanced by implementing threat information feeds to achieve better response efficiency against novel attacks. The other aspect of the ‘human factor’

in cybersecurity is how well-equipped a given organization or the travel sector is in terms of cyber defense. To develop a culture of security in the travel sector, extensive user-awareness programs are an absolute necessity. The chances of a successful attack can be reduced significantly if the staff members and other relevant stakeholders are familiar with the various risks and the importance of cybersecurity.

To build an effective IDS, the cooperation of various stakeholders, from government agencies to travel booking agents and tech companies, becomes essential. Karyy et al., (2021) analysis supports the idea that stakeholders could collaborate to strengthen the smart tourism security posture by sharing knowledge on risks, vulnerabilities, and good practices. Public-private partnerships could also support the maturation of industry standards and recommendations for the use of IDS. Hence, IDS integration with smart tourist systems is important, and the issues of food security and user privacy are key challenges. So, is the sector sufficiently armed to handle these dynamic cyber threats that will, no doubt, persist? Yes, but continuous innovation in IDS technology is necessary. Even the most hallowed tourist sector can adapt by creating a resilient security landscape that can protect companies and customers in an increasingly digital world – through improving machine learning capabilities, integration with other security measures, stakeholder education, and collaborations. The future security and dependability of smart tourism platforms will depend on the proactive development of intrusion detection systems.

6 Conclusion

IDS plays an important role in ensuring security for smart tourism platforms. This article concentrates on the technicalities of IDS, as well as the importance of relatively new approaches in invading detection. It is proposed that IDS need to be adapted to new methodologies based on machine learning, which will no doubt improve the IDS technology. With the rapid development and digital transformation of the tourism industry, future research may focus on IDS adaptation and explore related solutions to overcome the issues in this study. With IDS functioning in smart tourism platforms, it may alleviate users' trust concerns regarding food safety and user privacy issues, which all form a part of the industry's overall cybersecurity.

The study explains several ways of designing in-depth defense systems, including the architecture of network-based, host-based, and hybrid IDS systems, and discusses which of these would be better for a specific challenge based on the constraints faced by smart tourism platforms. The study also explains how machine learning increases IDS responsiveness and significantly improves how it can detect sophisticated attacks and anomalies in real time, covering a wider range of security issues. It's also highly important to establish strong cybersecurity policies that clearly outline best practices for data security, incident response, and users' privacy. These policies must be reviewed and updated regularly according to the changing security landscape.

Overall, regular training and awareness sessions are necessary for employees and users – training stakeholders to understand what threats look like and the importance of cybersecurity can help them better appreciate and support the security model on which tourism should be developed and delivered.

Partnerships can be formed between, for instance, technology providers, tourism operators and regulatory bodies to share information about threats, vulnerabilities and best practices that might lead to industry-wide standards and guidelines on how to build effective IDS. IDS should complement other cybersecurity measures such as firewalls, encryption, and access control systems for a multilayered approach against a broad range of threats. Performance should be assessed at regular intervals and strategies modified based on results, as determined by key stakeholders with regard to performance metrics. The tourism industry can rebuild the confidence of users by bolstering cybersecurity and by

implementing the recommendations above. Join forces to create safer and more resilient tourism systems through IDS. Integrating IDS into smart tourism is the right way forward. Smart and innovativeIDStourism will undoubtedly transform the world. Regardless, cyber-criminals will always be watching in order to harm this great connected industry. The future of this industry depends on our capacity – the tourism industry, academia, governments, and standards bodies alike – to innovate and cooperate to ensure the security of the data and systems that support vital activities and services for the public.

References

[1] Almomani, O. (2020). A feature selection model for network intrusion detection system based on PSO, GWO, FFA and GA algorithms. *Symmetry*, *12*(6), 1046. https://doi.org/10.3390/sym12061046

[2] Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, *7*(1), e06016. https://doi.org/10.1016/j.heliyon.2021.e06016

[3] Arshad, J., Azad, M. A., Amad, R., Salah, K., Alazab, M., & Iqbal, R. (2020). A review of performance, energy and privacy of intrusion detection systems for IoT. *Electronics*, *9*(4), 629.

[4] Bašić, Z., & Džananović, A. (2018). Route Tourist Railway Banovići – Zlaĉa. *Archives for Technical Sciences, 1*(18), 49–54. https://doi.org/10.7251/afts.2018.1018.049B

[5] Bhagat, A., Kaushal, S., Anand, A., & Mary, S. P. (2023, October). Decentralized Hotel Rooms Booking System Using Pragama Solidity and Blockchain Technology. In *Proceedings of the 6th International Conference on Intelligent Computing (ICIC-6 2023)* (Vol. 107, p. 119). Springer Nature. https://doi.org/10.2991/978-94-6463-250-7_22

[6] BR, S. R. (2022). Information and communication technology application in the Indian tourism industry. *Technology Application in Tourism in Asia*, 327-347. https://doi.org/10.1007/978-981-16-5461-9_20

[7] Buhalis, D., & Amaranggana, A. (2015). Smart tourism destinations enhancing tourism experience through personalisation of services. In *Information and Communication Technologies in Tourism 2015: Proceedings of the International Conference in Lugano, Switzerland, February 3-6, 2015* (pp. 377-389). Springer International Publishing. https://doi.org/10.1007/978-3-319-14343-9_28

[8] Detwiler, D. (2020). *Building the future of food safety technology: blockchain and beyond.* Academic Press.

[9] Gomez, C., Chessa, S., Fleury, A., Roussos, G., & Preuveneers, D. (2019). Internet of Things for enabling smart environments: A technology-centric perspective. *Journal of Ambient Intelligence and Smart Environments*, *11*(1), 23-43. https://doi.org/10.3233/AIS-180509

[10] Heidari, A., & Jabraeil Jamali, M. A. (2023). Internet of Things intrusion detection systems: a comprehensive review and future directions. *Cluster Computing*, *26*(6), 3753-3780. https://doi.org/10.1007/s10586-022-03776-z

[11] Ho, H. P. (2019). *Auto Scaling Infrastructure for Fit Restaurant with Nginx and Docker*. Technology and Communication: Helsinki, Finland.

[12] Kanimozhi, V., & Jacob, T. P. (2019, April). Artificial intelligence based network intrusion detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. In *2019 international conference on communication and signal processing (ICCSP)* (pp. 0033-0036). IEEE. https://doi.org/10.1109/ICCSP.2019.8698029

[13] Karyy, O., Kulyniak, I., Struchok, N., Halkiv, L., & Ohinok, S. (2021). Evaluation of the Tourist Attractiveness of Ukraine's Regions in the Conditions of Uncertainty Using Game Theory. *Proceedings – International Conference on Advanced Computer Information Technologies, ACIT*, 351–355. https://doi.org/10.1109/ACIT52158.2021.9548360

[14] Khaydarova, S., & Khujamova, S. (2024). The Vital Role of Libraries in Enriching Tourism Experiences. *Indian Journal of Information Sources and Services*, *14*(2), 11-16. https://doi.org/10.51983/ijiss-2024.14.2.02

[15] Kothamali, P. R., & Banik, S. (2022). Limitations of Signature-Based Threat Detection. *Revista de Inteligencia Artificial en Medicina*, *13*(1), 381-391.

[16] Lampe, B., & Meng, W. (2023). A survey of deep learning-based intrusion detection in automotive applications. *Expert Systems with Applications*, *221*, 119771. https://doi.org/10.1016/j.eswa.2023.119771

[17] Lei, M., Xu, L., Liu, T., Liu, S., & Sun, C. (2022). Integration of privacy protection and blockchain-based food safety traceability: Potential and challenges. *Foods*, *11*(15), 2262. https://doi.org/10.3390/foods11152262

[18] Melnyk, M., Leshchukh, I., Prytula, K., Ivaniuk, U., & Ohinok, S. (2024). Logistics potential to ensure the resilience of the Ukrainian economic system facing global challenges. *Problems and Perspectives in Management*, 22(2), 399–418. https://doi.org/10.21511/ppm.22(2).2024.31

[19] Muneer, S., Farooq, U., Athar, A., Ahsan Raza, M., Ghazal, T. M., & Sakib, S. (2024). A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection: A Comprehensive Analysis. *Journal of Engineering*, *2024*(1), 3909173. https://doi.org/10.1155/2024/3909173

[20] Ni, J., Zhang, K., Lin, X., & Shen, X. (2017). Securing fog computing for internet of things applications: Challenges and solutions. *IEEE Communications Surveys & Tutorials*, *20*(1), 601-628. https://doi.org/10.1109/COMST.2017.2762345

[21] Oskam, J., & Boswijk, A. (2016). Airbnb: the future of networked hospitality businesses. *Journal of tourism futures*, *2*(1), 22-42. https://doi.org/10.1108/JTF-11-2015-0048

[22] Qureshi, A., Afaqui, M. S., & Salas, J. (2020, August). IoTFC: A Secure and Privacy Preserving Architecture for Smart Buildings. In *International Conference on Security and Privacy in New Computing Environments* (pp. 102-119). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-66922-5_7

[23] Raúl, A. S., Miguel, J., Flabio, G., Adriel, O. H. A., Edwar, L., & Jordan, A. G. B. (2024). Intelligent System for Tourist Guidance in Tumbes-Perú. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 15*(3), 325-353. https://doi.org/10.58346/JOWUA.2024.I3.022

[24] Sánchez-Ancajima, R. A., Jiménez-Carrión, M., Gutierrez, F., Hermenegildo-Alfaro, A. O., Saavedra-López, M. A., Hernández, R. M., & Exebio Moya, L. R. (2023). Applications of Intelligent Systems in Tourism: Relevant Methods. *Journal of Internet Services and Information Security, 13*(1), 54-63. https://doi.org/10.58346/JISIS.2023.I1.006

[25] Shpak, N., Matviyishyn, Y., Dziurakh, Y., & Gvozd, M. (2024). Simulation of the impact of changes in the volume of production and export of products on the food security of the country: on the example of Ukraine. *Frontiers in Sustainable Food Systems*, *8*, 1361625. https://doi.org/10.3389/fsufs.2024.1361625

[26] Sia, P. Y. H., Saidin, S. S., & Iskandar, Y. H. P. (2023). Systematic review of mobile travel apps and their smart features and challenges. *Journal of Hospitality and Tourism Insights*, *6*(5), 2115-2138. https://doi.org/10.1108/JHTI-02-2022-0087

[27] Spanaki, M. Z. (2024). Management of new procedures' implementations risks in the hotel industry: A case study from Crete, Greece. In *The INC 2024 Technology-Enabled Competitiveness and Experiences in Tourism, Hospitality, and Events, 05-07 June 2024*, Amsterdam, The Netherlands.

[28] Thakkar, A., & Lohiya, R. (2021). A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges. *Archives of Computational Methods in Engineering*, *28*(4), 3211-3243. https://doi.org/10.1007/s11831-020-09496-0

[29] Wang, X., & Xu, J. (2021). Deterrence and leadership factors: Which are important for information security policy compliance in the hotel industry. *Tourism Management*, *84*, 104282. https://doi.org/10.1016/j.tourman.2021.104282

[30] Zafarmand, O. (2016). The study of the relationship between entertainment and water sport through creating tourism attraction and development (sport tourism) in Bushehr coasts. *International Academic Journal of Innovative Research*, *3*(1), 18–22.
[31] Zhang, S., Wang, C., Zhang, J., Duan, Y., You, X., & Zhang, P. (2020). Network resource allocation strategy based on deep reinforcement learning. *IEEE Open Journal of the Computer Society*, *1*, 86-94. https://doi.org/10.1109/OJCS.2020.3000330

Authors Biography

Yurii Dziurakh, is a Ph.D. in Public Management and Administration, Associate Professor, Associate Professor at the Department of Administrative and Financial Management, Lviv Polytechnic National University. Author of more than 210 scientific works, including 3 textbooks, 15 collective monographs, and more than 70 articles in specialized scientific publications. The author of 5 certificates of copyright registration for the work. Head and executor of a number of scientific and educational projects. Scientific interests: state regulation of investment activities in Ukraine, financial and investment support of economic growth, sustainable development, and food security of the country.

Ihor Kulyniak, is a Ph.D. in Economics, Associate Professor, and Associate Professor at the Department of Management of Organizations, Lviv Polytechnic National University. Author of more than 300 scientific works, including 15 textbooks, 20 collective monographs, and more than 100 articles in specialized scientific publications. His scientific activities are focused on tourism, investment and innovation management, financial and economic security, risk management, and marketing management. Coordinator of the international educational project Erasmus+ Jean Monnet 101085171 – ERASMUS-JMO-2022-HEI-TCH-RSCH «European experience in the promotion of heritage and cultural tourism» (EEPHCT).

Hanna Sarkisian, is a D.Sc. in Economics, Professor, Professor at the Department of Tourism Business and Recreation, Odesa National University of Technology. The direction of scientific research: modernization of mechanisms of regulation and stimulation of innovation activities of regional tourist markets. Work experience as a sommelier-taster.

Ivan Zhygalo, is a Ph.D. in Economics, Associate Professor, and Associate Professor at the Department of Management of Organizations, Lviv Polytechnic National University. Scientific interests: economic tools in enterprise management, management, entrepreneurship.

Bohdan Chepil, a Ph.D. in Economics and Assistant at the Department of Administrative and Financial Management, Lviv Polytechnic National University. His academic journey began in 2000 when he graduated from the Lviv Polytechnic National University, majoring in foreign economic activity management. He then gained practical experience as an economist, accountant, and chief accountant in various structures of Naftogaz of Ukraine. In 2014, he successfully defended his thesis and was awarded the scientific degree of Candidate of Economic Sciences.

Khrystyna Vaskovych, a dedicated teacher of economic disciplines at the Separate Structural Department "Stryi Professional College of Lviv National Environmental University". Her academic journey includes a Master of Laws from Lviv Ivan Franko National University, Lviv 2023, and a master's degree in public management and administration from Lviv Polytechnic National University, Lviv, 2023.