

Enhancing aviation CRM security with salesforce data cloud

Ivan Steniakin^{1,*†}, Dmytro Shevchuk^{1,†}, Kostiantyn Cherednichenko^{1,†}, Nazarii Liskovych^{1,†}, Olena Sokolova^{1,†} and Maksym Gryshchenko^{1,†}

¹ National Aviation University, Liubomyra Huzara Ave. 1, Kyiv, 03058, Ukraine

Abstract

As a result of the growing dependency on modern technologies within the scope of aviation, comprehensive measures should be taken to protect customer information, ensure regulatory adherence, and mitigate any cyber threats. This article studies the improvements that Salesforce Data Cloud brings to the security of Customer Relationship Management software security in aviation companies. Data Cloud increases encryption locks and decreases the chances of unauthorized breaches through the use of real time data integration, automated cyber security measures, and strong encryption. The research investigates the fragmentation of data and global compliance with data protection laws and cyber resilience which are principal issues of cybersecurity in aviation CRM. Also, the automating security monitoring and building compliant CRM infrastructure along with zero trust architecture and secure APIs are additional key components afforded by Data Cloud that make active cyber defense further reaching and robust. Reconstruction of Ukraine's aviation industry after the war requires trust scalable CRM systems that are secure and compliant for uninterrupted operations and customers. This study presents an important aspect of the strategic adoption of Salesforce Data Cloud for the protection of aviation CRM systems against security threats and crypto-crime radiation.

Keywords

CRM, Salesforce Data Cloud, dataflow, cybersecurity

1. Introduction

The constant digitization of aviation management has made it crucial to have secure and resilient management systems. With airlines managing a significant quantity of sensitive customer data, the cybersecurity of CRM systems has emerged as one of the most important challenges. This thesis aims to find out how Salesforce Data Cloud improves aviation security by filling major gaps, aiding in compliance, and reducing cyber risk mitigation issues. The implementation of sophisticated security features through the use of data leakage prevention, monitoring, encryption, and access control creates a supportive environment for aviation companies to protect themselves against data breaches and unauthorized access. This paper seeks to evaluate how Salesforce Data Cloud augments CRM security in the aviation industry, why this issue is important for the industry, and what the post-war reconstruction of the industry will look like.

2. Related work

The safety of CRM systems in aviation is one area of concern that has gained attention over the years. Different studies have sought to investigate various cybersecurity frameworks, encryption

CH&CMiGIN'24: Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, January 24–27, 2024, Kyiv, Ukraine

* Corresponding author.

† These authors contributed equally.

✉ ivansteniakin@gmail.com (I. Steniakin); dmitroshevchuk@gmail.com (D. Shevchuk); cherednichenko.kostya@gmail.com (K. Cherednichenko); nazarii.liskovych@npp.nau.edu.ua (N. Liskovych); sokolovaelena89@gmail.com (O. Sokolova); gryshchenko86@gmail.com (M. Gryshchenko)

ORCID 0000-0002-3511-6826 (I. Steniakin); 0000-0001-9911-7214 (D. Shevchuk); 0000-0002-9388-3521 (K. Cherednichenko); 0000-0002-0636-9648 (N. Liskovych); 0000-0001-6341-0195 (O. Sokolova); 0009-0000-3103-3524 (M. Gryshchenko)



© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

methods, and access control aspects [1–5]. Sources show how legacy CRM platforms are vulnerable to data breaches and insider threats and how CRM proprietary software frameworks are less secure. A number of researchers have written about the advantages of cloud computing, such as scalability and real time monitoring of security features in cloud-based CRM systems [6–8]. Existing literature has also considered compliance concerns like GDPR and other applicable rules streams emphasizing the need for stronger CRM aviation security [9].

One of the most significant barriers to effective aviation CRM security is the integration of unique data sources from various airlines, airports, and even other service providers. There are researches focused on how cloud platforms can offer data management services while securing role based access control and encryption. Also, the unsolicited use of artificial intelligence to do proactive worrying in CRM platforms has helped mitigate cybersecurity issues. They have also looked at cloud-based CRM security issues from a cost benefit perspective and identified them as operational risk on international security standards.

Up to October 2022, there have been advancements, but little research has been done on the role of Salesforce Data Cloud in aviation cybersecurity. Earlier research has looked into cloud-based security mechanisms, however, in depth assessment of the real-time compliance monitoring feature, security policies administrative processes, and AI based anomaly detection of Salesforce Data Cloud's security are not documented. The goal of this thesis is to analyze and integrate existing data by describing the way Salesforce Data Cloud improves aviation CRM security within the context of cyber defenses.

3. Problem statement

The cybersecurity posture of the aviation sector has been more critical than ever before due to increasing threats such as data breaches, insider attacks, and hacking activities on infrastructure. Such systems are difficult to achieve because of the architecture and organizational scope of conventional CRMs, which also often lack effective real-time monitoring. Moreover, the merging of multi-dimensional data sets like passenger information, flight operations, and services from external agencies further intensifies the security challenge. This level of fragmentation and scarcity of governance often results in ineffective and dispersed security measures, substandard encryption, and even non-compliance with regulations, exposing critical aviation information to serious threats.

While Salesforce Data Cloud suggests some remarkable features that could potentially solve these issues, aviation CRM has yet to be studied deeply in order to determine the practicality of these features. Specifically, can Salesforce Data Cloud mitigate the unique security challenges within the aviation sector during critical periods of post-war reconstruction? Without thorough examination of its capabilities, adoption methods, and restrictions, all stakeholders in the aviation industry could remain in the dark on how best to use this technology for customer data protection, ensuring comp.

4. Proposed solution

Salesforce Data Cloud is equipped with advanced data management functionalities as well as Bring Your Own Model (BYOM) feature which offers a solution to this problem. As shown in Figure 1, it permits organizations to incorporate bespoke machine learning algorithms that help in the processing and analysis of data streams in real-time to provide relevant outcomes. Having the capability of enabling predictive maintenance through data analytics, Salesforce Data Cloud has the capability of facilitating the airline industry in reducing unscheduled maintenance, improving safety measures, and optimizing other operations.

The next sub-sections present deals with the CRM application in the aviation area and give mathematically precise models that outline various data streams. These models demonstrate how data integration, security overhead, risk assessment, and anomaly detection can be formulated towards real-time protection.

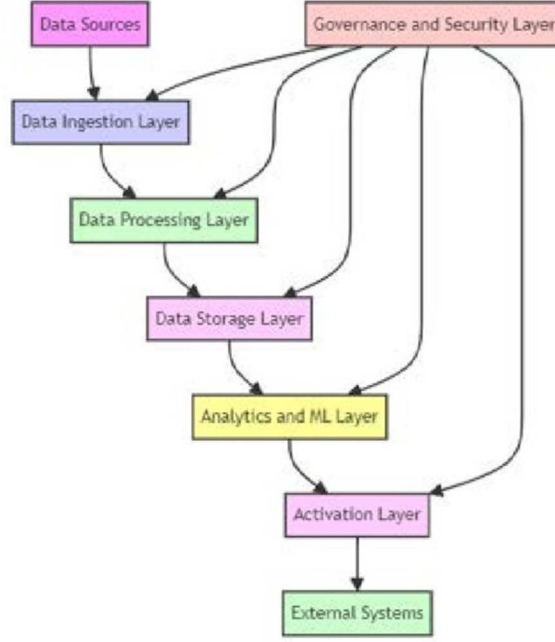


Figure 1: Salesforce data cloud architecture [7].

4.1. Data streams and aggregation

Let n be the number of data streams feeding into the CRM from different sources (e.g., airlines, airports, third-party providers). We can define each data stream as a function of time:

$$X_i(t) : R \rightarrow R, i = 1, 2, \dots, n, \quad (1)$$

where $X_i(t)$ represents the data rate (or data volume) from the i -th source at time t . The total data ingested by the CRM at time t is:

$$T(t) = \sum_{i=1}^n X_i(t). \quad (2)$$

4.2. Real-time security overhead

To maintain confidentiality and integrity, each data stream may undergo encryption or security checks. Let $C_i(t)$ denote the computational overhead needed to secure the i -th data stream, which may depend on both the volume of data and the complexity of encryption:

$$C_i(t) = f(X_i(t), E_i), \quad (3)$$

where E_i represents the encryption method or security protocol applied to stream i . The total security overhead at time t is:

$$C_{total}(t) = \sum_{i=1}^n C_i(t). \quad (4)$$

4.3. Risk function for data streams

Define a risk function $R_i(t)$ for each stream that reflects the probability of a breach or compromise, considering factors such as encryption strength and threat level:

$$R_i(t) = g(X_i(t), \partial_i, E_i), \quad (5)$$

where ∂_i is a parameter capturing the threat profile for stream i . A simple aggregated risk measure might sum or average these:

$$R_{aggregate}(t) = h(R_1(t), R_2(t), \dots, R_n(t)). \quad (6)$$

4.4. Anomaly detection

Anomaly detection algorithms can be employed to identify suspicious patterns in real time. Suppose $A_i(t)$ is an anomaly score for stream i :

$$A_i(t) = \delta(X_i(t), \mu_i(t), \sigma_i(t)), \quad (7)$$

where $\mu_i(t)$ and $\sigma_i(t)$ are, respectively, the expected mean and standard deviation of the data stream under normal conditions. The function δ measures deviations from the expected pattern. A combined anomaly index can be:

$$A_{combined}(t) = \sum_{i=1}^n \omega_i A_i(t). \quad (8)$$

where ω_i are weights reflecting the relative importance or criticality of each data source.

4.5. Multi-objective optimization

In a secure CRM design, we balance performance (i.e., minimizing latency, maximizing throughput) with security (i.e., minimizing the risk of breach and overhead). A simplified multi-objective optimization problem might be formulated as:

$$\min_{E_i, \omega_i} [\lambda_1 C_{total}(t) + \lambda_2 R_{aggregate}(t) - \lambda_3 T(t)] \quad (9)$$

subject to compliance and operational constraints. The parameters λ_1 , λ_2 and λ_3 indicate the relative weighting of security overhead, risk, and data throughput, respectively.

These formulas define how different data streams can be merged, kept safe, and monitored. In the other sections, we will talk about how specific Salesforce Data Cloud features like compliance in real-time, automated policy enforcement, and AI analytics are embedded into or modify these formulas for the specific security needs of aviation CRM.

5. Data extraction and processing

From the beginning, there were numerous data assets that contained flight data. The first information had two volumes, the first one was already in the designated format and stored in the CRM. The second volume was CSV formatted so we uploaded it as a Data Lake – raw data representation. Finally, the third volume was XML formatted and has a completely different structure. Because of this fact, a Python script was developed that first converted the data into CSV format and then used a combination of features of the data to build a number of different models with different classifiers mentioned in [10–16].

Python scripts can extract data from CSV files. This process is commenced by a function that first employs the built in `xml.etree.ElementTree` library to parse the XML structure [17–25]. The script and combines suitable namespace arguments to locate entities that are between the SOAP envelopes pertaining to caseload information such as the number of passengers, flights, etc. During the first portion of data ingestion, a crucial step is made in piecing together the fractured structures that predominate in aviation-related XML documents such as names, passenger types, flight schedules, and all associated names.

The script further transforms certain parts of the XML into well-formed Python objects. Commitment to augment XML elements proceeds to data manipulation after parsing. Passenger data, for example, is stored within dictionaries that feature last names, first names, and type of passengers. In parallel, flight metadata such as carrier codes, flight numbers, and departure dates are captured for future enrichment. This step emphasizes the simplification of unique data components which makes standardization easier during the machine learning procedure [21–23].

The organized raw information depicts how the preliminary raw characteristics for the model training can be effortlessly acquired. Some straightforward statistics include the number of total passengers on board, as well as the ratio of adults to children traveling. These analytics represent the passenger's composition and can be further enhanced or narrowed down to meet certain criteria such as outlier detection or demand predicting by adding new parameters like booking time frames or frequent flyer indicators. In the end results are comprehensive and highly informative for the primary school position of machine learning around the concepts of multi-layered predictive models,

CRM segmentation, and even applying advanced threat detection techniques in aviation CRM systems.

After the parsing and feature extraction process, the data is structured into two primary components:

Passengers List. A list of dictionaries, where each dictionary holds passenger-specific attributes. For example:

```
{
  'surname': 'Test',
  'first_name': 'TETIANA MRS',
  'type': 'ADT'
}
```

This structure allows for easy iteration or filtering based on attributes like type or surname.

Flight Details Dictionary. A single dictionary capturing overall flight information, such as:

```
{
  'passenger_count': 275,
  'flight_info': {
    'carrier': 'PS',
    'flight_number': '1172',
    'flight_year': 2020,
    'flight_month': 3,
    'flight_day': 29
  }
}
```

This encompasses summary statistics (e.g., total passenger count) and metadata needed for contextual analysis.

At the end, the `build_feature_vector` function merges the sources into a dictionary of features that a machine learning model can work with. This final feature dictionary consolidates passenger level insights (e.g. number of adult/child passengers) and flight level metadata (e.g. flight carrier, date) into one coherent data structure. Consequently, analysts or automated pipelines can easily convert real-time XML data into usable features that enable anomaly detection and predictive models as well as targeted customer segmentation in the aviation CRM domain.

6. Implementation and case study

As shown in Figure 2, the integration process includes structured inputs such as aircraft sensor data, maintenance logs, and operational statistics that are sent to a remote service for processing. These external platforms, such as SageMaker or Vertex AI, use this data to train machine learning models.

The integration stage is aimed at incorporating Salesforce Data Cloud into the current aviation CRM frameworks. The various types of data sources, which include passenger reservation systems and flight operations databases, require meticulous planning in order to facilitate data ingestion and implement effective security measures. These steps provide a broad overview:

- **Systems Assessment:** A snapshot of existing CRM systems must be done first, details of various data sources as well as their sensitivity (such as passenger data compared to internal flight information) need to be documented.
- **Salesforce Data Cloud Configuration:** Data flows and pipelines to ingest data from different sources must be designed in Salesforce Data Cloud. In order to meet the requisite IATA security standards, adequate encryption (for example, AES-256) and role-based access

permissions ought to be configured. To achieve the above, Salesforce Data Cloud has to be provisioned, where data from several sources can be ingested effortlessly (Figure 3). Salesforce provides superior tools for data visualization. Information from various systems can be easily fused and is therefore much more usable to customers.

- Compliance with regional data or GDPR requires the implementation of ETL processes or APIs that will extract data streams from various sources and integrate them into Salesforce Data Cloud.
- Security teams are receiving real-time notifications of possible system intrusions by feeding patterns and baseline data into security systems to set anomaly detection modules in real time monitoring and alerts.
- With the assumption of correct data usage and with the principle of least privilege incorporated into user roles and permissions, targeted training sessions were assigned to users with minimal insider threats.

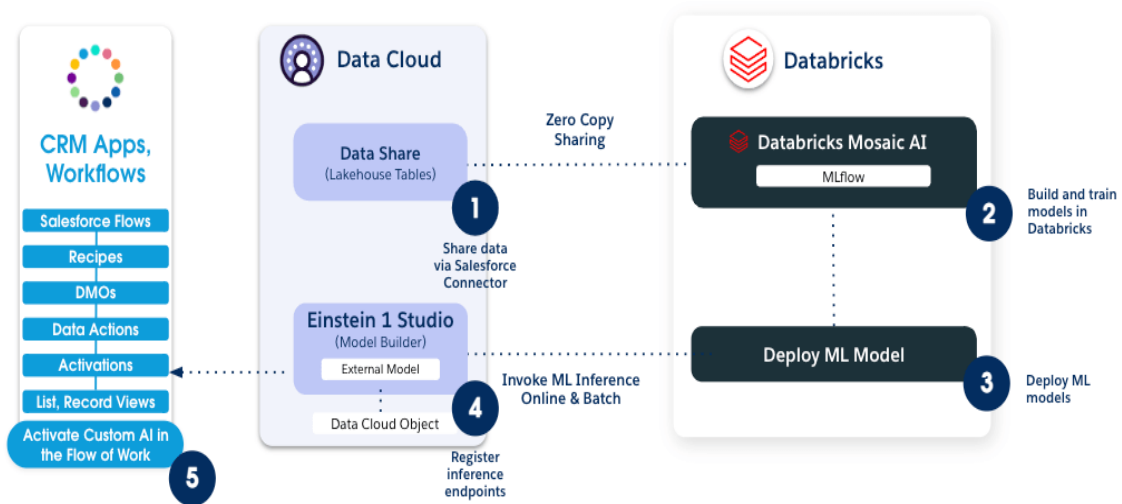


Figure 2: Typical scheme of embedding custom ML model into Data Cloud flow [8].

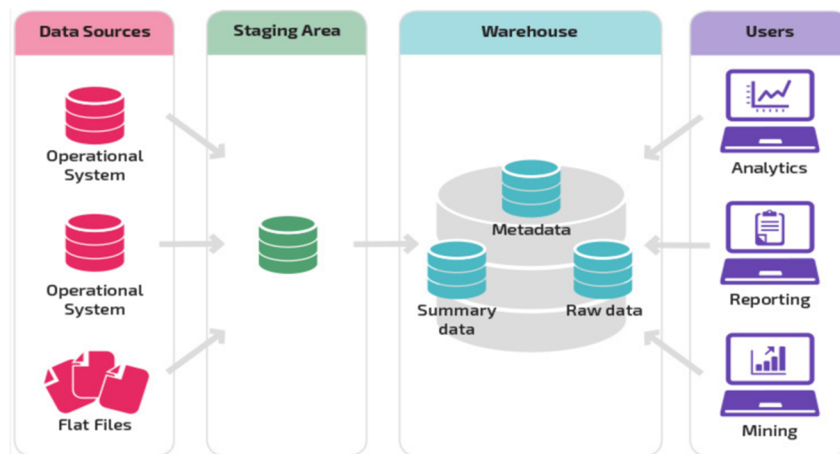


Figure 3: Airline's data warehouse flow [8].

In order to showcase how Salesforce Data Cloud can be utilized within Aviation CRM security, let us consider hypothetically a mid-sized airline that is based in Ukraine after a war and intends on upgrading their CRM platform. This airline faces the following problems concerning:

- Data quality and siloed databases are a common problem due to operational disruptions and differing legacy systems, known as fragmented data sources.
- Due to the implications of a post war setting, it is expected that there will not be a large pool of skilled cybersecurity professionals using automated and simplified solutions.
- As the airline aims to reacquaint itself with the global market, there is a significant need to follow international aviation regulations and the constantly changing data protection norms.

In order to achieve all the stated above next implementation steps are required:

- Infrastructure Assessment: An exhaustive evaluation of the airline's CRM systems reveals local silo databases, Excel passenger registers, and other third-party ticket selling applications.
- Data Cloud Configuration: Data Cloud is set up to support encryption-at-rest and in-transit using the proposed risk mitigation policies in the Solution Framework.
- Stream Data Migration: Selected data elements such as bookings, loyalty information, and flight details are fetched securely using API. Error-proofing policies are created to ensure data integrity.
- Information Technology Security Policy: Delegate permissions to users by role in divisions (e.g. sales, operations, compliance). Set automated alarms for anomalous data access activity.
- Anomaly Detection: Machine Learning is applied to historical flight and passenger datasets in order to detect anomalies such as suspicious activity like high cancellation of booked flights or excessive failed logins.

Early results from this implementation suggest:

- The airline's IT security team now has access to data flows across the organization which increases their reactions to any data anomalies.
- An increase in automated encryption and advanced anomaly detection protocols resulted in an aggregate decrease in risk measures that were previously set in the Solution Framework.
- Readiness to Comply with Standards is Improved: Integrated audit trails and policy execution processes aid in reporting to regulatory authorities which facilitates the airline's reintegration into global standards.

7. Discussions

We now analyze the results of implementation. Many parts of data cleansing and stock for an organization involving sensitive passenger info and operational data is greatly facilitated using Salesforce Data Cloud. When multiple non similar sources are brought together into a single dashboard, the security teams are able to detect threats and respond to them in near real time.

A measurable improvement was noted in the business aggregated risk functions which indicates reduction by encryption protocols, role based access controls, machine learning anomaly detection systems and other modern IT security solutions. There is opposing literature which states AI and cloud based architecture do not aid in ameliorating the CRM security framework. Furthermore, automation of policy compliance, along with monitoring of the entire system has simplified compliance in other regions that have stringent data security laws.

Despite these opportunities, issues and constraints arise. First and foremost, the overdependence on sophisticated infrastructure and specialized personnel could pose a problem in post-conflict reconstruction settings, where IT capabilities may be scarce. Staff members need to be sufficiently monitored as they learn how to use the Data Cloud features, since any mishandling could lead to the negation of the automation benefits provided, which also takes time to manage effectively. Second, there is a need for further integration or development of other specialized security control tools (e.g. advanced SIEM) to overcome complex or target specific cyber threats within the Salesforce Data

Cloud, even though its real time threat detection capabilities are top-notch. Lastly, overseeing multi-objective optimization complexity would become more complicated as the airline grows and incorporates more data-centric services; balancing throughput, latency, and risk exposure can become more daunting.

All things considered, Salesforce Data Cloud appears to be a useful tool for securing aviation CRM data and information, especially during the context of modernizing a critical infrastructure. However, scaling, training, and specialized security integration should be approached more astutely to garner maximum advantage of the Data Cloud. In another aspect, the case study could be deepened by analyzing more airlines in different locations to gain more nuances for optimal aviation data security practices.

8. Conclusions

The demand for enhancing cybersecurity capabilities of CRM in aviation as shown in this thesis is possible by the Salesforce Data Cloud which, through its single scalable solution, addresses the complex nature of cyber challenges. Its capacity for real-time monitored data, automatic compliance features as well as AI anomaly detection makes Salesforce Data Cloud a strong candidate for sensitive data protection in highly regulated and complex industries.

Creating risk mitigation alongside a security overhead through mathematical models will aid in the problem set of data stream integration. This thesis case study illustrates the applicability of the Salesforce Data Cloud features such as encryption and role-based access control in a post-war construction as a case study thesis, showing that Salesforce Data Cloud is viable even with limited resources and enforced security.

The implementation of such systems however requires substantial training, infrastructure, and resources in order to ensure constant monitoring of ever shifting cyber landscapes. Other factors that warrant further research include area comparison in diverse industries, integration of multi-cloud systems, and the use of comprehensive threat intelligence. These practices would help stakeholders in the aviation industry uncover better practices for CRM systems, improving security even during Ukraine's post-war recovery and on a global scale.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

- [1] K. Cherednichenko, O. Sokolova, V. Ivannikova, Mathematical model of airport aviation security, in: *Proceedings of Transbaltica XIII: Transportation Science And Technology*, Springer, Cham, 2023, pp. 773–781. doi: 10.1007/978-3-031-25863-3_75.
- [2] A. Bieliatynskiy, S. Yang, V. Pershakov, M. Shao, M. Ta, The use of fiber made from fly ash from power plants in China in road and airfield construction, *Construction and Building Materials* 323 (2022) 126537. doi: 10.1016/j.conbuildmat.2022.126537.
- [3] D. Shevchuk, O. Yakushenko, L. Pomytkina, D. Medynskiy, Y. Shevchenko, Neural Network Model for Predicting the Performance of a Transport Task, *Lecture Notes in Civil Engineering*, Springer, Singapore, 2020, pp. 271–278.
- [4] O. Sushchenko, et al., Integration of MEMS inertial and magnetic field sensors for tracking power lines, in: *Proceedings of IEEE XVIII International Conference on the Perspective Technologies and Methods in MEMS Design (MEMSTECH)*, IEEE, Polyana, Ukraine, 2022, pp. 33–36. doi: 10.1109/MEMSTECH55132.2022.10002907.
- [5] D. Shevchuk, O. Yakushenko, I. Steniakin, A. Shyshka, Delivery Route Optimization with Neuron Network. In: A.K. Nagar, D.S. Jat, D. Mishra, A. Joshi (Eds.), *Intelligent Sustainable Systems*. WorldS4 2023. *Lecture Notes in Networks and Systems*, vol. 803, Springer, Singapore, 2024.

- [6] V. S. Guduru, Enhancing Customer Experience with Personalized Data Strategies in Salesforce Data Cloud, *Journal of Mathematical & Computer Applications* 1–5 (2023). doi: 10.47363/JMCA/2023(2)E112.
- [7] What Is Data Cloud?, 2023. URL: <https://www.salesforce.com/blog/what-is-data-cloud/>.
- [8] Learn How Data Cloud Works, 2023. URL: <https://trailhead.salesforce.com/content/learn/modules/data-cloud-powered-experiences/learn-how-data-cloud-works>.
- [9] J. Howard, S. Gugger, A layered API for deep learning, *Information* 11.2 (2020) 108. doi: 10.3390/info11020108.
- [10] J. Bergstra, Y. Bengio, Random search for hyper-parameter optimization, *Journal of machine learning research* 13(2) (2012).
- [11] J. Brownlee, A gentle introduction that the rectified linear unit (ReLU), *Machine learning mastery* 6 (2019).
- [12] A. Velu, Application of logistics regression models in risk management, *International Journal of Innovations in Engineering Research and Technology* 8(04) (2021) 251–260. URL: <https://repo.ijert.org/index.php/ijert/article/view/2594>.
- [13] L. Breiman, J. H. Friedman, R. A. Olshen, C. T. Stone, *Classification and Regression Trees*, Chapman and Hall/CRC, 1984.
- [14] I. Ostroumov, et al., A probability estimation of aircraft departures and arrivals delays, In: O. Gervasi, et al. (Eds.), *Computational Science and Its Applications – ICCSA 2021*. ICCSA 2021, volume 12950 of *Lecture Notes in Computer Science*, Springer, Cham, 2021, pp. 363–377. doi: 10.1007/978-3-030-86960-1_26.
- [15] O. Sushchenko, et al., Airborne sensor for measuring components of terrestrial magnetic field, in: *Proceedings of IEEE 41st International Conference on Electronics and Nanotechnology (ELNANO)*, IEEE, Kyiv, Ukraine, 2022, pp. 687–691. doi: 10.1109/ELNANO54667.2022.9926760.
- [16] O. Solomentsev, M. Zaliskyi, T. Herasymenko, O. Kozhokhina, Y. Petrova, Efficiency of operational data processing for radio electronic equipment, *Aviation* 23 (3) (2020) 71–77. doi: 10.3846/aviation.2019.11849.
- [17] N. Matthias, J. Jasmi, *XML parsing* 175 (2003). doi: 10.1145/956895.956898.
- [18] N. S. Kuzmenko, I. V. Ostroumov, K. Marais, An accuracy and availability estimation of aircraft positioning by navigational aids, in: *Proceedings of 2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC)*, IEEE, Kiev, Ukraine, 2018, pp. 36-40. doi: 10.1109/MSNMC.2018.8576276.
- [19] O. Solomentsev et al., Data Processing through the Lifecycle of Aviation Radio Equipment, in: *Proceedings of 2022 IEEE 17th International Conference on Computer Sciences and Information Technologies (CSIT)*, 2022, IEEE, Lviv, Ukraine, pp. 146–151. doi: 10.1109/CSIT56902.2022.10000844.
- [20] M. Zaliskyi, et al., Heteroskedasticity analysis during operational data processing of radio electronic systems, in: S. Shukla, A. Unal, J. Varghese Kureethara, D.K. Mishra, D.S. Han (Eds.), *Data science and security*, volume 290 of *Lecture Notes in Networks and Systems*, Springer, Singapore, 2021, pp. 168–175. doi: 10.1007/978-981-16-4486-3_18.
- [21] P. Jae, K. Ji, The Impact of Airport Managerial Type and Airline Market Share on Airport Efficiency, *Sustainability* 13 (2021) 981. doi: 10.3390/su13020981.
- [22] Scikit-learn: Machine Learning in Python, 2023. URL: <https://scikit-learn.org/stable/>.
- [23] F. Pedregosa, et al., Scikit-learn: Machine learning in Python, *Journal of machine learning research* 12 (2011) 2825–2830.
- [24] V. Ivanov, S. Kuang, V. Stabnikov, C. Guo, The removal of phosphorus from reject water in a municipal wastewater treatment plant using iron ore, *Journal of Chemical Technology and Biotechnology* 84 (1) (2009) 78–82. doi: 10.1002/jctb.2009.
- [25] N. Kuzmenko, et al., Airplane flight phase identification using maximum posterior probability method, in: *Proceedings of IEEE 3rd International Conference on System Analysis & Intelligent Computing (SAIC)*, IEEE, Kyiv, Ukraine, 2022, pp. 1–5. doi: 10.1109/SAIC57818.2022.9922913.