BAG-INTEL: A Hierarchical Multi-Cloud IoT-Edge-Cloud Architecture for Enhanced Airport Security and Operations

George Bardas, georgios.bardas@netcompany.com, Greece, Netcompany-Intrasoft
Panayiotis Michael, panayiotismichael@mail.ntua.gr, Greece, National Technical University of Athens
Panayiotis Tsanakas, panag@cs.ntua.gr, Greece, National Technical University of Athens
George Lalas, george.lalas@netcompany.com, Greece, Netcompany-Intrasoft
Henrik Larsen, henrik@legind.com, Denmark, Legind Technologies AS

Abstract

The EU Horizon project BAG-INTEL integrates Internet of Things (IoT) devices with Artificial Intelligence (AI) within a hierarchical multi-cloud architecture to enhance airport security and operations. The design of the BAG-INTEL system is presented in this study. It consists of three layers: common European data environments for non-sensitive information transmission, national governmental cloud clusters for secure interface with federal resources, and edge computing for local data processing. BAG-INTEL tackles latency and data security concerns by utilizing artificial intelligence and a scalable, safe cloud architecture. Its effectiveness and adaptability are demonstrated by deployment scenarios at different airports. Because of its scalability, the architecture can be applied to additional security-sensitive sectors. In the future, it may also be enhanced with global cloud integration and AI-driven predictive analytics. A new benchmark for the integration of cloud, edge, and IoT technologies in airport security is established by BAG-INTEL. The system's architecture, implementation, and possible uses are described in this paper, with a focus on how they may affect cloud computing, airport security, and the Internet of Things.

Keyword**:** Internet of Things (IoT),Artificial Intelligence (AI), Airport Security, Multi-cloud Architecture, Customs, Edge Computing, Cloud Computing

1 Introduction

1.1 Background and Motivation

Airports are complex environments where security, efficiency, and operational effectiveness are paramount. The growing number of passengers and the complexity of potential security threats require modern technology solutions. Conventional systems that depend significantly on human resources and outdated technologies frequently find it challenging to meet the requirements of modern airport operations. The BAG-INTEL project seeks to tackle these difficulties by combining Internet of Things (IoT) devices with Artificial Intelligence and an advanced multi-cloud architecture that improves the security and effectiveness of airport operations.

The project emphasizes the utilization of AI-driven tools for luggage inspection, integrated with a secure and scalable cloud infrastructure, which is fundamental to its innovation.

1.2 Objectives

The primary objective of this paper is to present the architectural design of the BAG-INTEL system, with a focus on its hierarchical, multi-cloud structure. The document will describe the architectural framework and its components.

- Demonstrate how the architecture natively fosters data security and facilitates real-time processing.
- Examine the scalability and application of the architecture across several domains, establishing a paradigm for secure and efficient data processing infrastructures.

2 Related Work

2.1 IoT and Cloud Computing in Airport Security

IoT devices have become increasingly prevalent in airport security, offering critical data from sensors, cameras, and various monitoring systems. Nevertheless, the integration of these devices into a unified system capable of real-time data processing and responsive security threat management continues to be challenging. The current literature underscores the drawbacks of centralized cloud systems, including latency challenges and data security difficulties, which the BAG-INTEL architecture seeks to address.

The study indicates that BAG-INTEL's strategy of integrating edge computing with cloud technology addresses these difficulties by facilitating local data processing at the airport, hence minimizing latency and improving security.

2.2 Multi-Cloud Architectures

Multi-cloud architectures are increasingly adopted in security-sensitive settings as they provide workload distribution among various cloud providers, hence improving resilience and mitigating vendor lock-in. The hierarchical structure of BAG-INTEL's architecture enhances this methodology by incorporating additional layers of security and control, guaranteeing that data is transferred solely when essential and in accordance with strict security rules.

The project demonstrates that BAG-INTEL's multi-cloud architecture, featuring separate layers for on-premises processing, governmental cloud integration, and European data sharing, represents a strong strategy for managing sensitive data across various cloud environments.

3 BAG-INTEL Architecture Overview

3.1 Architecture and IoT Layers

The BAG-INTEL architecture is designed under the IoT-edge-Continuum and split into the following main layers:

- **Cloud Layer:** Performs deeper data analysis, coordination, and long-term storage
- **Fog Layer:** Balances the workload between the edge and the cloud
- **Edge Device Layer:** Responsible for collecting real-time data and processing it locally

And supplementary layers:

- **IoT Sensors Layer:** Contains all the sensors of the system
- **External Data Layer:** Contains all the external data sources and is part of the Edge Device Layer
- **Offline Layer:** Contains all the ML training procedures and is part of the Cloud layer
- **User Interface Layer:** The layer comprising all the visualizations and end-user interfaces

3.1.1 Cloud Layer

At the cloud layer, powerful computer resources are provided together with data storage and management, coupled with high-performance computing (training of AI models). It hosts the offline layer (described below), which includes all the ML training sessions, all the cloud data processing, management and persisting, and the system's digital twin. Furthermore, it addresses the security of data through the interim repository, which is utilized to process externally retrieved data, stored with privacy until they are legally clear to be stored in the system. After data are cleaned, becoming legally and ethichally safe, they can be persisted in the External Knowledge Base. The Cloud Layer also hosts the digital twin.

3.1.2 Fog Layer

The fog layer acts as a bridge between the edge and the cloud layers. We opt to host processes here that are located closer to the edge data to improve response times and reduce bandwidth consumption. All the main processes of the system are located here including both the baggage reidentification and luggage risk classification modules. Placing these two main components at the Fog Layer secures direct access to both the edge and cloud layer's data. Fog layer is part of the cloud layer and hence not visible in Figure 1.

3.1.3 Edge Layer

At the edge layer is where the data generation and initial processing happens. Apart from hosting the IoT Sensors Layer (described below), which generates real-time data and the initial processing components for bag triggering, unique ID generation and AI contraband detection, the internal BAG-INTEL Database is also hosted at the Edge Layer. This database will be utilized to persist all the generated and processed system data related to the baggage records. These data are unique for each airport use case and will be persisted for processing by the system and demonstration to the end-users. Finally, the message bus will be hosted at the Edge Layer to ensure real-time asynchronous communications between the system's components. This layer is split into "Outside Airport premises" and "On Airport premises" layers as shown in Figure 1.

3.1.4 Supplementary Layers

As supplementary, we define all layers which are not considered as reference layers in the Iot-Edge-Continuum but are introduced in order to assist the system's architecture:

External Data layer: Includes all the external data sources, independently whether they include sensitive data or not, which will be utilized by the cloud layer of the system to populate, through the Interim Repository, the external knowledge base. This data will be utilized mainly from the Luggage Risk Classification module. This layer can be officially considered as part of the Cloud Layer.

Offline layer: Hosts all the training of the ML models and can run asynchronously and before the system's online operation. This layer can be officially considered as part of the Cloud Layer.

IoT Sensors Layer: Comprises all the sensors setup at the airport (cameras, dog, label scanner, X-ray scanner) and generates real-time data which the system further processes. This layer can be officially considered as part of the Edge Device layer.

User Interface Layer: The user interface layer comprises all the visualizations that are essential to provide input and output to the end-user. Without them, the end-user would not be able to receive the results of the system or introduce input and parameterizations.

3.2 The Hierarchical model of the Multi-Cloud, IoT-Edge-Cloud Continuum Architecture

The BAG-INTEL architecture enables the orchestration of the intelligent analysis performed at different checkpoints along the moving conveyor belt and until the luggage exits the airport through the customs area. The architecture has been designed based on the Cloud-Edge-IoT Continuum paradigm, enabling real-time responsiveness, by pushing complex, time-critical computation at the edge and even on the IoT while ensuring security and privacy.

A number of state-of-the-art equipment is used including X-ray scanners and cameras for image acquisition. These devices are modeled in the architecture within the IoT layer (Figure 1). An IoT orchestrator enables the integration of the devices, the unification of the data in the platform of the Airport Cloud and their further analysis by AI/NN components.

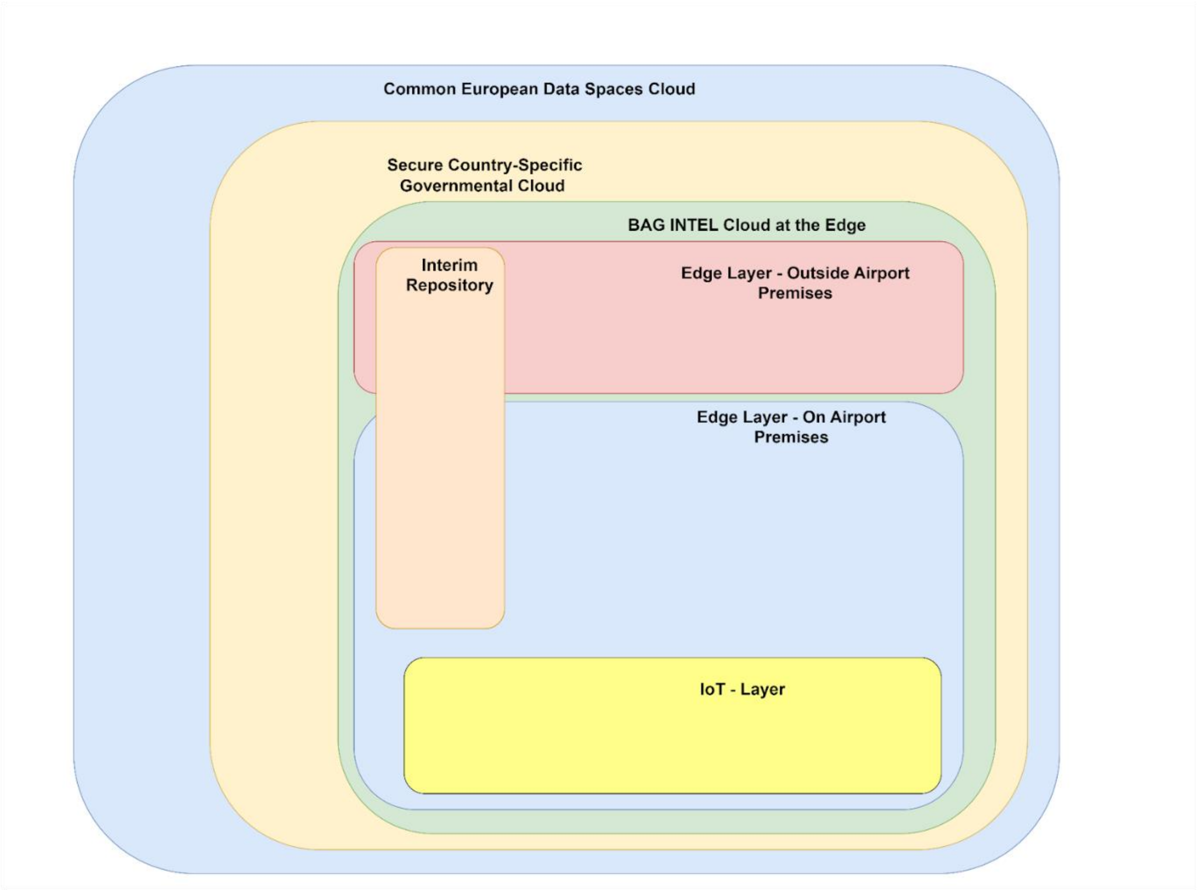
Common European Data Spaces Cloud
Secure Country-Specific Governmental Cloud
BAG INTEL Cloud at the Edge
Interim Repository
Edge Layer - Outside Airport Premises
Edge Layer - On Airport Premises
IoT - Layer

Figure 1: The Hierarchical model of the Multi-Cloud, IoT-Edge-Cloud Continuum Architecture

The data generated or used during the airport operations are mission-critical, and for this reason we need to avoid their transmission to the public cloud. Nevertheless, the benefits of elasticity, high-availability, resilience and scalability a Cloud environment offers, cannot be overlooked. For this reason, we have designed the development of a secure, airport-located (on-premises) cloud (BAG-INTEL Airport Cloud at the Edge) which provides these desired properties.

The architecture has a hierarchical structure, allowing the connectivity of the BAG-INTEL Cloud at the Edge - forming a core layer (Layer 0) - with other clouds following a multi-cloud paradigm in a layered manner (Figure 1

The middle layer of the multi-cloud consists of other secure governmental (country specific) clusters which the BAG-INTEL Cloud can extend in an integrated manner (Layer 1, Figure 1). Information received from governmental sources are extremely important as they are processed by AI BAG-INTEL subsystems (External Knowledge subsystems) to generate risk signals.

The top layer of the multi-cloud (Layer 2, Figure 1) allows the sharing of non-sensitive information with Common European Data Spaces and the hosting of non-sensitive information (such as environmental data related to airports and traveling) on European Federated Cloud Infrastructures.

The overall design develops a novel, hierarchical, multi-layered, multi-cloud architecture for the Cloud-Edge-IoT Continuum. While our proposed architecture has been designed for the BAG-INTEL system and airport operations, it can be used as a general framework for other domains.

The BAG-INTEL system and processes aim to become an integral part of existing airport operations and systems; thus, we have defined its architecture to follow Secure-by-Design principles, establishing security measures that will be implemented early in the development of the BAG-INTEL system. Security measures are integrated with the overall architecture thus avoiding security-related modifications in the future. While the design of the architecture has as epicenter the BAG-INTEL Cloud at the Edge on Airport premises -- protected by the airport security processes and directives, data flows crossing the different cloud layers in the multi-cloud hierarchy, need special attention and specialized architectural designs to enforce security.

Another parameter affecting the overall security of the system, is the need for edge computation residing outside the airport, on technology suppliers' (direct peering sites) infrastructures. "Outside the airport" computational infrastructure, as a separate layer (Edge Layer-Outside Airport Premises, Figure 1), enables Continuous Integration Continuous Development (CI/CD) and has many benefits allowing development and operations teams to collaborate to deliver services to the BAG-INTEL Cloud at the Edge. Nevertheless, this layer creates serious security vulnerabilities that need to be appropriately addressed by security architecture designs, due to the direct access of the Cloud at the Edge on Airport premises, which is furthermore integrated with the overall airport IT infrastructure. The layers in the hierarchical multi-cloud structure are outlined in the following paragraphs:

- **Layer 0: BAG-INTEL Cloud at the edge**

  This layer consists of the Edge Layer-On Airport premises and the Edge Layer-Outside Airport premises.

  - **Layer 0.a: Edge Layer-On Airport premises**

    The Edge Layer-On Airport premises is implemented within the airport, ensuring that sensitive data from IoT devices, such as cameras and X-ray machines, is processed locally. This layer leverages the low latency of edge computing, essential for time-sensitive tasks such as security screening. This layer has a critical security role, as it keeps data generated by the BAG-INTEL system (e.g. video streams from the cameras subsystem, AI analyses results, external information trusted to the layer) confidential and within the secure airport infrastructure.

  - **Layer 0.b: Edge Layer-Outside Airport premises**

    The Edge Layer-Outside Airport premises, consists of the infrastructure of multiple vendors' development and operations teams, collaborating outside the airport to deliver services to the Edge Layer-On Airport premises. Such an infrastructure is necessary as it allows development agility and enables the improvement of the overall BAG-INTEL system through machine learning and regular training of the AI models of its subsystems. Nevertheless, strict security measures are required for this layer as it accesses the security critical operations at the Edge Layer-On Airport.

- **Layer 1: Secure Country-Specific Governmental Cloud Clusters**

  Country-Specific governmental data are important for the effectiveness of the BAG-INTEL system, as they are processed by the AI components of the External Knowledge subsystem to generate risk signals. BAG-INTEL interfaces with the secure federal cloud clusters, enabling the connection with national security databases and additional governmental resources, thereby enhancing the overall security response. The Security-by-Design architecture, ensures that data shared with governmental systems is protected by stringent security measures, complying with national regulations and standards.

  To strengthen the protection of sensitive data received from governmental data sources, an Interim Repository, which is a data repository covered by a legal and ethical umbrella has been included in the architecture as shown in Figure 1. The interim repository temporarily stores sensitive data received from Layer 1 in Layer 0, for privacy protection measures to be applied on them (e.g. anonymization), before these data are diffused within the overall Layer 0 infrastructure. The novel concept of the Interim Repository was first introduced in a white paper of the project PolicyCLOUD and StandICT.eu 2023 [8].

- **Layer 2: Private Cloud (Non-Sensitive Data)**

  The outer layer of the BAG-INTEL architecture promotes the dissemination of non-sensitive information among European federated cloud infrastructures. This layer is intended to oversee data that, although significant, does not pose the same security threats as the data handled at the lower layers. Such data are environmental data (e.g. CO2 emissions and statistics on the number of passengers, luggage flowing through the airports per season/country).

3.3 Data Flow Management and Security Protocols

The BAG-INTEL system is designed to oversee data flows across its layers securely and efficiently. Data flows are regulated by strict rules that guarantee the sharing of only crucial data between layers and external entities. Our approach enforces the implementation of sophisticated encryption methods, access restrictions, and auditing processes in order to protect data during its entire lifecycle within the BAG-INTEL system.

4 Implementation and Operational Scenarios

4.1 System Deployment in Airports

The BAG-INTEL system intends to be deployed in airport environments as a comprehensive solution for enhancing security and operational efficiency. The system plans to integrate seamlessly with existing airport infrastructure, allowing for the real-time processing of data from various sources, including security cameras, baggage scanners, and bag-tag readers. The on-premises cloud (Layer 0.a) handles critical tasks like threat detection and passenger flow management, ensuring rapid response times and reducing the workload on human operators.

4.2 Case Studies

The customs control of checked-in baggage from commercial passenger flights arriving at interior border airports is the main use case for the BAG-INTEL system. When a plane lands, its luggage is moved from the baggage conveyor belt to the carousel area, where travelers retrieve their possessions. Passengers are only allowed entry to the carousel area and are required to exit through a specific customs inspection point thanks to BAG-INTEL. To protect privacy and security, the carousel area is visually isolated from the pre-arrival procedures and baggage belt.

The luggage scanner and the end-to-end re-identification system are the two main parts of BAG-INTEL in this scenario. The scanner uses cutting-edge AI-driven approaches to identify suspicious things in order to discover and identify contraband hidden in the suitcase. From the time of arrival until it clears customs, the re-identification system guarantees continuous tracking of any baggage marked for examination. When suspect luggage is carried into the customs examination area, real-time alarms are sent to the customs officers. When customs consider scanning unnecessary in low-risk circumstances, the system can be turned off to maximize resource utilization.

The purpose of BAG-INTEL is to improve the efficiency of customs inspections by offering high-precision tracking and scanning that easily integrates with the current airport infrastructure. The following are actual instances of how the technology will be put into use and evaluated at different airports:

Use Case 1: Billund Airport, Denmark (Small International Airport)

In Denmark, the entire BAG-INTEL system will be installed at Billund Airport. The ultimate users will be the airport operator and Danish Customs. In this case, cameras will be installed for luggage recognition and registration, and Smiths Detection (SDE) will supply an X-ray/CT scanner.

Prior to installation, a controlled environment will be used to teach the AI system and scanner to detect specific forms of contraband, such drugs. In addition, a dataset of photos of luggage gathered at the beginning of the project will be used to train the camera and AI. This guarantees that luggage travelling through the airport may be successfully recognised and reidentified by the system. The re-identification system and the AI's capacity to identify contraband will be put to the test by customs inspectors, who will also make sure that any suspect luggage is appropriately identified and examined before it leaves the airport.

Use Case 2: Thessaloniki Airport, Greece (Medium-Sized International Airport)

The entire BAG-INTEL system will be installed in this use case at the airport in Thessaloniki, Greece. The principal end users will be Greek customs, border guards (Hellenic Police), and airport operator Fraport Greece. For this configuration, an X-ray/CT scanner will be provided by Smiths Detection (SDE), and the airport will supply handheld devices for scanning bag tag labels prior to the luggage entering the X-ray/CT scanner. Important details like the departure airport that are provided by these labels will be entered into the BAG-INTEL knowledge base for risk assessments.

While the camera/AI will be trained on a dataset of suitcase photographs gathered earlier in the project, the scanner/AI will be trained in a controlled environment, much like the Billund scenario. In this use case, the effectiveness of BAG-INTEL will be assessed using key performance indicators (KPIs), and the system's compatibility with the current customs, airport, and law enforcement systems will be tested. This guarantees that the BAG-INTEL system improves airport security agency collaboration.

Use Case 3: Adolfo Suárez Madrid–Barajas Airport, Spain (Large International Airport)

A high-risk setting will be used to test the BAG-INTEL system at Madrid-Barajas Airport, one of the busiest airports in Europe. The testing will involve border police (Guardia Civil), Spanish customs (AEAT), and other relevant parties. Because Madrid-Barajas is home to many foreign flights with a high risk of contraband, it offers a rare chance to stress-test the system in difficult circumstances.

Here, the degree of screening for arriving flights is already decided by the customs and border police using a predetermined risk assessment scale. All baggage on flights classified as "Very High Risk" or "High Risk" is subject to X-ray screening utilising mobile scanning trucks on the apron, which is outside the terminal building. Dogs that detect things are also used in this situation. The BAG-INTEL system faces a special problem because of this operation's mobility character, especially regarding the positioning and functionality of AI cameras, which could not be in fixed positions.

The BAG-INTEL system will be put to the test in a high-stakes, real-world setting in this large-scale use case to make sure it can handle the challenges of a sizable airport with a variety of operational requirements. In this context, the integration of AI tracking and mobile scanning will demonstrate the system's scalability and versatility.

5 Scalability and Applicability

5.1 Adaptation to Other Domains

The architecture of BAG-INTEL is engineered for scalability, enabling adaptation for many applications requiring robust and secure data processing. The identical hierarchical methodology might be utilized in border control, where the necessity for real-time data processing and secure transmission is equally critical. The document indicates that the system's design is sufficiently adaptable to accommodate the varied requirements of other industries, rendering it a desirable framework for other security-sensitive contexts.

5.2 Future Developments

The BAG-INTEL system suggests several possibilities for future enhancement, including the use of AI-driven predictive analytics to foresee security threats prior to their development. A potential advancement may include the expansion of the system's multi-cloud architecture to include worldwide cloud infrastructures, thereby augmenting its scalability and resilience.

6 Conclusion

The BAG-INTEL system represents a significant advancement in the integration of IoT, edge computing, and cloud technologies for airport security and operations. BAG-INTEL provides a scalable and secure solution for the various challenges of airport environments through the implementation of a hierarchical, multi-cloud architecture. The system's capacity to locally process crucial data while utilizing the advantages of cloud computing establishes a new benchmark for the successful management of sensitive operational data. The paper establishes the architecture and potential uses of the BAG-INTEL system, emphasizing its contributions to the domains of IoT, cloud computing, and airport security.

7 Acknowledge

The work is funded by the European Union (Project 101121309—BAG-INTEL). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

8 References

1. Miorandi, D., Sicari, S., Pellegrini, P., & Chlamtac, I. (2012). "Internet of Things: Vision, Applications and Research Challenges." Ad Hoc Networks, 10(7), 1497-1516.
2. García-Magariño, I., & García-Sánchez, F. (2020). "Multi-cloud Architectures for IoT Applications." Future Generation Computer Systems, 108, 101-113.
3. Almalki, A., & Alghamdi, A. (2021). "The Role of Artificial Intelligence in Enhancing Airport Security: A Review." Journal of Air Transport Management, 90, 101911.
4. Mansoor, M., & Ghafoor, K. (2021). "Edge Computing for IoT: A Survey." IEEE Access, 9, 123456-123478.
5. Gonzalez, A., & Ramos, J. (2020). "Cloud Computing in Airport Management: A Review of the Current State and Future Directions." Transportation Research Part C: Emerging Technologies, 119, 102753.
6. Kumar, P., & Singh, M. (2020). "AI-Driven Security Systems in Airports: Opportunities and Challenges." International Journal of Information Management, 52, 102101.
7. European Union Agency for Cybersecurity (ENISA). (2020). "Cloud Computing Security Risk Assessment."
8. Michael, P., Oikonomou, K., Ledakis, G., Willems, M., Mari, M., Smith, Z., Abergas-Arteza, J., Taborda Barata, M., & Bettiol, A. (2022). “Cloud for Data Driven Policy Management”. Zenodo. https://doi.org/10.5281/zenodo.7376071