UDC 629.7.063.6(045)
DOI:10.18372/1990-5548.83.19878

[1]**K. O. Dzhelalov,**
[2]**O. I. Smirnov,**
[3]**Yu. M. Kemenyash**

COMPREHENSIVE SECURITY SYSTEM OF DATA TRANSMISSION NETWORKS OF CIVIL AVIATION ENTERPRISES

Aviation Computer-Integrated Complexes Department, State Non-Profit Enterprise
"State University "Kyiv Aviation Institute", Kyiv, Ukraine
E-mails: [1]kdzhelalov@gmail.com, [2]osmirnovfaee@gmail.com, [3]lindysik999@gmail.com

Abstract*—A comprehensive security system for data transmission networks in civil aviation enterprises is considered, which is aimed at overcoming the growing cybersecurity threats in modern aviation infrastructure. Vulnerabilities such as outdated systems, human errors and integration of IoT devices pose significant risks to data confidentiality, integrity and availability. To mitigate these challenges, the system integrates advanced cryptographic algorithms, DevOps methodologies for automated security updates and real-time monitoring tools such as Grafana and Prometheus. The use of fault tolerance mechanisms ensures uninterrupted operation and resilience during security incidents.*

Keywords—Cybersecurity; civil aviation; data transmission; cryptography; fault tolerance; systems monitoring.

I. INTRODUCTION

Data transmission networks are indispensable to aviation, underpinning operations such as flight co ordination, air traffic control, and passenger data management. The seamless and secure flow of information is not only essential for operational efficiency but also crucial for ensuring safety and maintaining trust among passengers and stakeholders. However, these networks are increasingly exposed to cyber security threats, including data breaches, unauthorized access, and sophisticated attacks targeting critical systems. Such incidents have the potential to disrupt operations, compromise sensitive information, and jeopardize safety.

The interconnected nature of aviation systems amplifies these challenges. Networks link onboard avionics, ground control stations, airline data centers, and more, creating an extensive attack surface. Legacy systems, often lacking modern security features, further exacerbate vulnerabilities.

This research aims to develop a comprehensive security framework for aviation data networks. By leveraging cryptographic methods, such as symmetric and asymmetric encryption, and adopting DevOps practices like CI/CD pipelines and containerization, the proposed solution enhances scalability, resilience, and security. Rigorous testing under simulated conditions evaluates the framework's ability to mitigate risks, ensuring it is equipped to address evolving threats, operational demands effectively [1], [2].

II. PROBLEM STATEMENT

The aviation industry's reliance on interconnected and real-time systems exposes it to significant cybersecurity risks. Legacy technologies and complex system architectures create vulnerabilities that are increasingly exploited by sophisticated cyber threats. Data breaches, unauthorized access, and targeted attacks can disrupt operations and compromise sensitive information, potentially leading to safety hazards and financial losses.

Traditional security measures are often inadequate for addressing the dynamic challenges of modern aviation networks. These measures struggle with scalability, resilience, and the ability to adapt to evolving threats. Therefore, there is a pressing need for an innovative approach that integrates advanced security practices, such as cryptographic techniques and automated DevOps workflows, to ensure robust and reliable data transmission within aviation networks [2].

III. PROBLEM SOLUTION

To address the critical vulnerabilities in aviation data networks, this research proposes a multifaceted security framework incorporating advanced cryptographic methods, containerization technologies, and DevOps practices. The solution addresses scalability, efficiency, and security, establishing a robust foundation for secure aviation operations [3].

Cryptography ensures the confidentiality, integrity, and authenticity of transmitted data. Symmetric encryption algorithms, such as advanced encryption standard (AES), are particularly well-suited for securing large volumes of data quickly, making them indispensable for real-time aviation operations. By encrypting data blocks efficiently, AES maintains high throughput and ensures that latency-sensitive operations, such as air traffic management, are not adversely impacted.

Asymmetric encryption, exemplified by algorithms like Rivest–Shamir–Adleman (RSA) and elliptic curve cryptography (ECC), plays a vital role in securing key exchanges. This functionality is crucial in distributed aviation networks, where components such as ground control systems, onboard avionics, and external communication hubs require encrypted channels to transmit sensitive information securely.

Elliptic curve cryptography, in particular, offers significant advantages due to its smaller key sizes, which reduce computational overhead while maintaining high security levels

Hybrid cryptographic systems combine the strengths of symmetric and asymmetric methods, enhancing efficiency and security. In these systems, symmetric keys are securely exchanged using asymmetric encryption, followed by the rapid encryption of bulk data with symmetric algorithms. This hybrid approach is particularly effective in aviation, where both high performance and robust security are essential.

Modern cryptographic protocols, including TLS 1.3 and IPsec, further bolster aviation network security. TLS 1.3 provides enhanced encryption performance and reduced latency, making it ideal for webbased interfaces and operational dashboards. IPsec ensures secure packet-level communication across IP-based networks, protecting data integrity and confidentiality during transmission. Additionally, quantum-resistant algorithms are being explored to future-proof the security of cryptographic systems against emerging quantum computing threats.

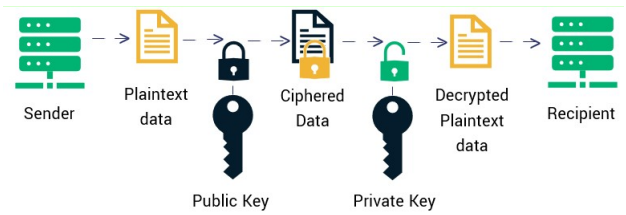

Fig. 1. Scheme of cryptographic encryption of data transmission

Containerization revolutionizes application deployment and management by encapsulating applications and their dependencies into isolated units. This modularity ensures consistency across diverse environments, reducing compatibility issues and streamlining the deployment process.

A significant advantage of containerization lies in its ability to isolate individual services within aviation systems. For example, flight data processing, passenger management, and weather analytics can operate as separate containers. This separation enhances security by limiting potential breaches to a single container and simplifies updates and trouble shooting. Furthermore, containers enable version control for applications, allowing quick rollbacks in case of deployment issues.

Containers are inherently lightweight, allowing for optimal resource utilization. Unlike traditional virtual machines, which duplicate an entire operating system for each instance, containers share the host OS kernel. This efficiency translates into reduced memory and CPU overhead, enabling aviation systems to handle higher workloads without significant infrastructure upgrades. Container runtimes like Docker and CRI-O provide streamlined management, while tools like Podman ensure secure, daemon less container execution.

Orchestration platforms like Kubernetes amplify these benefits. Kubernetes dynamically allocates resources based on real-time demand, ensuring that systems scale elastically during operational peaks. For instance, during extreme weather conditions causing flight delays, the system can allocate additional resources to passenger support services without disrupting other operations. Furthermore, Kubernetes facilitates blue-green and canary deployments, enabling seamless updates with minimal risk.

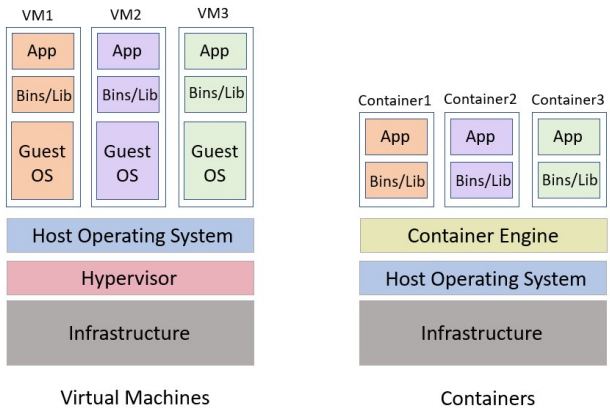

Fig. 2. Generalized structure of containerization

Kubernetes serves as the cornerstone of modern containerized environments, providing advanced orchestration capabilities that ensure system reliability and scalability. One of its core features is selfhealing, which automatically restarts or replaces failed containers, minimizing downtime and maintaining operational continuity. This ensures that critical aviation systems remain functional even in the event of hardware or software failures.

Horizontal scaling is another critical advantage of Kubernetes. By adding or removing container instances based on workload requirements, Kubernetes optimizes resource utilization and ensures consistent performance. For example, during high passenger volumes, additional resources can be allocated to booking and checkin systems, enhancing user experience without manual intervention. Kubernetes also supports autoscaling, which dynamically adjusts resources in response to predefined metrics, such as CPU usage or request latency.

Multi-cluster management allows Kubernetes to deploy applications across geographically distributed data centers. This capability ensures global redundancy and disaster recovery, critical for aviation systems that require uninterrupted operations across multiple regions. Additionally, Kubernetes' native load balancing ensures efficient distribution of traffic across containers, preventing bottlenecks and enhancing overall system performance.

Kubernetes' network policies enforce strict access controls, preventing unauthorized communications between containers and reducing the risk of lateral movement by attackers. Service meshes like Istio or Linkerd can be integrated to enhance observability and security, offering features like mutual TLS authentication and advanced traffic management. Furthermore, Kubernetes integrates seamlessly with Continuous Deployment (CD) tools, automating the rollout of application updates while ensuring consistency across environments.

Integrating monitoring tools, such as Prometheus and Grafana, into Kubernetes environments provides realtime analytics and insights. These tools enable proactive identification of bottlenecks and vulnerabilities, facilitating rapid response and continuous improvement. For example, anomalous network activity detected by Prometheus can trigger automated countermeasures, further enhancing system security. Kubernetes' builtin logging and event monitoring capabilities, combined with these tools, provide comprehensive observability.

The proposed framework significantly outperforms traditional infrastructures in several key aspects.

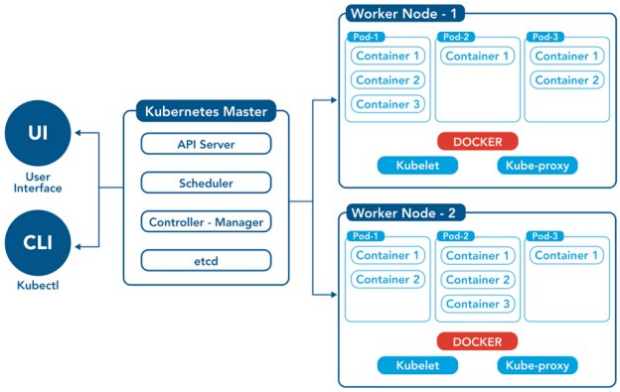

Fig. 3. Architecture of kubernetes operations

Scalability: Traditional systems often rely on rigid, hardware-dependent configurations that lack flexibility, making them unsuitable for dynamic aviation environments. In contrast, containerized architectures, orchestrated by Kubernetes, enable dynamic horizontal and vertical scaling. Workloads are distributed across nodes in real-time, ensuring optimal utilization of resources during peak operational periods, such as weather disruptions or high passenger volumes. Kubernetes' auto-scaling feature further enhances adaptability by dynamically provisioning resources based on real-time metrics like CPU utilization and request latency.

Automation: Legacy systems often require manual intervention for updates, patches, and deployments, leading to increased operational overhead and potential human errors. The proposed framework integrates CI/CD pipelines, automating these processes to deliver faster, error-free updates. Tools such as Jenkins, GitLab CI, and ArgoCD streamline workflows, reducing downtime and ensuring consistent deployments. This automation extends to rollback mechanisms, allowing seamless recovery in case of deployment issues.

Security: Legacy systems rely on perimeterbased security models that are insufficient against modern cyber threats. The proposed framework incorporates cryptographic methods, container isolation, and Kubernetes network policies to enforce a zerotrust security model. Features such as mutual TLS authentication within service meshes (e.g., Istio) and container runtime security tools (e.g., Falco) significantly enhance protection against breaches. Real-time monitoring and automated threat detection enable proactive mitigation of potential vulnerabilities.

Resilience: High availability is critical for aviation systems where downtimes can lead to operational and safety risks. Kubernetes' self healing capabilities ensure that failed containers are automatically replaced, minimizing disruptions. Multi-cluster deployments provide geographic redundancy, ensuring disaster recovery and operational continuity during regional outages. Traditional infrastructures, by contrast, are prone to single points of failure that require extensive manual intervention to resolve.

Cost-Effectiveness: Traditional infrastructures often involve significant capital expenditures on dedicated hardware and labor-intensive management. The proposed framework leverages containerized architectures and orchestration to optimize resource utilization, significantly lowering operational costs. Kubernetes' ability to pool and share resources across multiple applications reduces the need for over provisioning, while automation minimizes the reliance on manual oversight.

Observability and Insights: Unlike legacy systems with limited monitoring capabilities, the proposed framework integrates advanced observability tools like Prometheus, Grafana, and ELK stack. These tools provide granular visibility into system performance, enabling early detection of bottlenecks and anomalies. Insights derived from real-time analytics support predictive maintenance and enhance decision-making, further improving efficiency and reliability.

Adaptability to Emerging Technologies: Traditional systems often face challenges when integrating new technologies. The proposed framework's modularity and reliance on containerization make it inherently adaptable to advancements such as AI-driven analytics, blockchain-based data sharing, and quantum-resistant cryptography, ensuring long-term viability and innovation readiness.

IV. CONCLUSIONS

The integration of advanced cryptographic methods, containerization, and DevOps practices represents a paradigm shift in securing aviation data networks. This research addresses critical vulnerabilities inherent in legacy systems by introducing a framework that is scalable, resilient, and adaptive to evolving operational needs and technological advancements.

The framework's emphasis on scalability ensures that aviation systems can seamlessly handle fluctuating demands without compromising performance. Automation reduces operational overhead while improving the consistency and reliability of deployments. Advanced security measures, including cryptographic techniques and zero-trust models, provide robust protection against sophisticated cyber threats. Moreover, the resilience of Kubernetes-driven container orchestration ensures uninterrupted operations, even in the face of hardware failures or regional outages.

By significantly lowering operational costs and enhancing observability, the framework not only aligns with current operational goals but also positions aviation enterprises to adopt emerging technologies effectively. The proposed solution sets a new benchmark for secure, scalable, and efficient aviation data networks, offering a robust foundation for the industry's future challenges and opportunities.

REFERENCES

[1] David Farley and Jez Humble, *Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation*, Addison-Wesley Professional, 2010, p. 463. ISBN: 9780321670250

[2] G. Kim, P. Debois, J. Willis, and J. Humble, *The Phoenix Project: A Novel About IT, DevOps, and Helping Your Business Win*. IT Revolution Press, 2016.

[3] M. Saucier, *Aviation Cybersecurity: Protecting Modern Aviation Systems*. Springer, 2018.

Received December 12, 2024

Dzhelalov Kostiantyn. Master.
Department of Aviation Computer-Integrated Complexes, State Non-Profit Enterprise "State University "Kyiv Aviation Institute", Kyiv, Ukraine.
Education: National Aviation University, Kyiv, Ukraine (2024).
Research interests: security of data transmission networks, DevOps practicies.
Publications: 5.
E-mail: kdzhelalov@gmail.com

Smirnov Oleg. Candidate of Science (Engineering). Assocsate Professor.
Department of Aviation Computer-Integrated Complexes, State Non-Profit Enterprise "State University "Kyiv Aviation Institute", Kyiv, Ukraine.
Education: Kyiv High Military Engineering Aviation School of Air Forces, Kyiv, USSR, (1974).
Research interests: integrated processing of information in Inertial Navigation Systems.

Publications: more than 100 papers.
E-mail: osmirnovfaee@gmail.com

Kemenyash Yuriy. Senior Teacher.
Aviation Computer-Integrated Complexes Department, State Non-Profit Enterprise "State University "Kyiv Aviation Institute", Kyiv, Ukraine.
Education: National Aviation University, Kyiv, Ukraine, (1996).
Research area: automation, navigation.
Publications: more than 40.
E-mail: lindysik999@gmail.com

К. О. Джелалов, О. І. Смірнов, Ю. М. Кеменяш. Комплексна система захисту мереж передачі даних підприємств цивільної авіації

Розглянуто комплексну систему безпеки для мереж передачі даних на підприємствах цивільної авіації, яка спрямована на подолання зростаючих загроз кібербезпеки в сучасній авіаційній інфраструктурі. Такі вразливості, як застарілі системи, людські помилки та інтеграція пристроїв IoT, створюють значні ризики для конфіденційності, цілісності та доступності даних. Для пом'якшення цих викликів в систему інтегровані передові криптографічні алгоритми, методології DevOps для автоматизованого оновлення безпеки та інструменти моніторингу в реальному часі, такі як Grafana та Prometheus. Застосування механізмів відмовостійкості забезпечують безперебійну роботу та стійкість під час інцидентів безпеки. Запропонований підхід підвищує надійність системи, цілісність даних та відповідність міжнародним стандартам авіаційної безпеки, створюючи безпечну основу для критично важливих процесів передачі даних.
Ключові слова: кібербезпека; цивільна авіація; передача даних; криптографія; відмовостійкість; моніторинг систем.

Джелалов Костянтин Олександрович. Магістр.
Кафедра авіаційних комп'ютерно-інтегрованих комплексів, Державне некомерційне підприємство «Державний університет «Київський авіаційний інститут», Київ, Україна.
Освіта: Національний авіаційний університет, Київ, Україна (2024).
Наукові інтереси: безпека мереж передачі даних, практики DevOps.
Публікації: 5.
E-mail: kdzhelalov@gmail.com

Смірнов Олег Ігорович. Кандидат технічних наук. Доцент.
Кафедра авіаційних комп'ютерно-інтегрованих комплексів, Державне некомерційне підприємство «Державний університет «Київський авіаційний інститут», Київ, Україна.
Освіта: Київське вище військове інженерне авіаційне училище Військово-Повітряних Сил, Київ, СРСР, (1974).
Напрям наукової діяльності: інтегрована обробка інформації в інерціальних навігаційних системах.
Публікації: більше 100 наукових робіт.
E-mail: osmirnovfaee@gmail.com

Кеменяш Юрій Михайлович. Старший викладач.
Кафедра авіаційних комп'ютерно-інтегрованих комплексів, Державне некомерційне підприємство «Державний університет «Київський авіаційний інститут», Київ, Україна.
Освіта: Національний авіаційний університет, Київ, Україна, (1996).
Напрям наукової діяльності: автоматизація, навігація.
Кількість публікацій: більше 40 наукових робіт.
E-mail: lindysik999@gmail.com