UDK: 004.9

A SECURE AND AUTOMATED DIGITAL FRAMEWORK FOR HEALTHCARE PERSONNEL AND DOCUMENT MANAGEMENT IN EMERGENCY AND HIGH-DEMAND CONDITIONS

БЕЗПЕЧНА ТА АВТОМАТИЗОВАНА ЦИФРОВА СИСТЕМНА РАМКА ДЛЯ УПРАВЛІННЯ МЕДИЧНИМ ПЕРСОНАЛОМ І ДОКУМЕНТАЦІЄЮ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ ТА ВИСОКОГО НАВАНТАЖЕННЯ

Азір Аліу[1], Реджеп Мустафовський[2]
Azir Aliu[1], Rexhep Mustafovski[2]

[1]South East European University – SEEU, Faculty of Computer Science, Skopje, North Macedonia
[2] Goce Delcev University' Stip, Military Academy "General Mihailo Apostolski", Skopje, North Macedonia
ORCID: https://orcid.org/0009-0000-3257-0989[2]
E-mail: redzep.mustafovski@ugd.edu.mk[2] , azir.aliu@seeu.edu.mk[1]

DOI: 10.15673/atbp.v18i1.3438

Abstract. *Healthcare systems operating under emergency and high-demand conditions face persistent challenges in coordinating medical personnel, managing critical documentation, and ensuring data security and regulatory compliance. Fragmented organizational structures and manual workflows often result in inefficiencies and delayed decision making, particularly during large-scale health crises. These issues highlight the need for secure and automated digital solutions that integrate personnel and document management within a unified system.*

This paper proposes a secure and automated digital framework for healthcare personnel and document management to support coordinated operations in emergency environments. The framework integrates structured coordination mechanisms, dynamic personnel assignment, and a digital platform for secure data handling. It emphasizes automation of business processes, role-based access control, decision-support functionality, and audit logging to ensure operational continuity, accountability, and cybersecurity. A system-oriented and methodological analysis demonstrates the framework's potential to improve coordination efficiency, data security, and resilience, making it suitable for national healthcare systems, emergency response organizations, and public health authorities.

Анотація. *Системи охорони здоров'я, що функціонують в умовах надзвичайних ситуацій та підвищеного попиту, стикаються з постійними проблемами в координації медичного персоналу, управлінні критично важливою документацією, а також у забезпеченні безпеки даних і дотриманні нормативних вимог. Фрагментовані організаційні структури та ручні робочі процеси часто призводять до неефективності та затримок у прийнятті рішень, особливо під час масштабних криз у сфері охорони здоров'я. Ці проблеми підкреслюють необхідність у безпечних та автоматизованих цифрових рішеннях, які інтегрують управління персоналом і документами в межах єдиної системи.*

У цій роботі пропонується безпечна та автоматизована цифрова структура (фреймворк) для управління персоналом і документацією в охороні здоров'я з метою підтримки координованих операцій у надзвичайних ситуаціях. Структура поєднує в собі механізми чіткої координації, динамічне призначення персоналу та цифрову платформу для безпечної обробки даних. Особлива увага приділяється автоматизації бізнес-процесів, рольовому управлінню доступом, функціоналу підтримки прийняття рішень та реєстрації подій аудиту для забезпечення безперервності операцій, підзвітності та кібербезпеки. Системно-орієнтований та

методологічний аналіз демонструє потенціал запропонованої структури щодо підвищення ефективності координації, безпеки даних та стійкості, що робить її придатною для використання національними системами охорони здоров'я, організаціями реагування на надзвичайні ситуації та органами управління охороною здоров'я.
Keywords: healthcare process automation, secure digital platforms, healthcare personnel management, document management systems, emergency response coordination, cybersecurity in healthcare

Ключові слова: автоматизація процесів в охороні здоров'я, безпечні цифрові платформи, управління персоналом в охороні здоров'я, системи управління документами, координація реагування на надзвичайні ситуації, кібербезпека в охороні здоров'я.

I. INTRODUCTION

Healthcare systems play a critical role in ensuring public safety and societal stability, particularly during emergency situations and periods of exceptionally high operational demand. Large-scale health crises, natural disasters, pandemics, and mass-casualty incidents place unprecedented pressure on healthcare organizations, requiring rapid coordination of medical personnel, timely access to critical documentation, and secure information exchange across multiple institutions. Under such conditions, the effectiveness of healthcare response is highly dependent on the ability to manage human resources and information flows in a coordinated, reliable, and secure manner [1]–[3].

Despite ongoing digital transformation efforts, many healthcare systems continue to rely on fragmented organizational structures and partially manual business processes. Personnel allocation is often managed through decentralized decision making, while medical documentation is distributed across heterogeneous information systems with limited interoperability. These conditions frequently lead to delayed response times, inefficient use of available medical staff, reduced situational awareness, and increased risk of data inconsistency or loss during emergencies [4]–[7]. Studies have shown that the absence of integrated digital platforms significantly limits the capacity of healthcare organizations to respond effectively to sudden surges in demand [8], [9].

Automation of technological and business processes has been widely recognized as a key enabler for improving efficiency and reliability in complex organizational systems, including healthcare environments [10]–[12]. Automated workflows, decision-support mechanisms, and digital coordination platforms can reduce administrative overhead, support faster decision making, and improve transparency in personnel management. However, the adoption of automation in healthcare introduces additional challenges related to data protection, regulatory compliance, and cybersecurity, particularly when sensitive medical and personnel information is involved [13]–[15].

Security and privacy concerns represent a major barrier to the widespread deployment of integrated healthcare information systems. Healthcare data are among the most sensitive categories of information, and unauthorized access or data breaches can have severe legal, ethical, and operational consequences. The increasing frequency of cyber attacks targeting healthcare institutions highlights the need for robust access control, auditability, and secure system architectures that can operate reliably even under adverse conditions [16]–[18]. These requirements become even more critical during emergency scenarios, where rapid access to information must be balanced against strict security and compliance constraints [19], [20].

Recent research has explored various digital solutions for healthcare coordination, including electronic health records, hospital information systems, and emergency management platforms [21]–[23]. While these solutions address specific functional needs, they are often developed as standalone systems and lack a unified architectural perspective that integrates personnel management, document handling, process automation, and cybersecurity within a single framework. As a result, healthcare organizations may deploy multiple disconnected tools that fail to provide comprehensive support during complex emergency operations [24]–[26].

There is therefore a clear need for a secure and automated digital framework that unifies healthcare personnel management and document handling while supporting coordinated operations across institutional boundaries. Such a framework should automate key business processes, enable dynamic allocation of medical personnel, ensure secure and auditable access to critical information, and support decision making under time-critical conditions. At the same time, it must be adaptable to national healthcare systems and compliant with regulatory and organizational requirements [27]–[29].

In this context, this paper proposes a secure and automated digital framework for healthcare personnel and document management designed specifically for emergency and high-demand conditions. The proposed approach adopts a system-oriented and architectural perspective, focusing on the integration of automation, cybersecurity, and decision-support mechanisms rather than isolated technological components. The framework is analyzed using architectural reasoning and representative operational scenarios to demonstrate its applicability and potential benefits. By addressing both technological and organizational challenges, the proposed solution aims to contribute to the advancement of secure automation practices in healthcare systems operating under critical conditions [30].

II. RELATED WORK

Research on digital transformation and automation in healthcare systems has intensified in recent years, driven by increasing operational complexity, demographic pressures, and the growing frequency of emergencies and high-demand situations. Existing studies address various aspects of healthcare digitization, including information system integration,

personnel coordination, cybersecurity, and decision support. However, these contributions are often fragmented and insufficiently aligned with the combined requirements of emergency response, secure automation, and coordinated personnel and document management. This section critically reviews the relevant literature and positions the proposed framework within the identified research gaps.

Several foundational studies emphasize the structural challenges faced by healthcare systems during emergencies. Works such as [1] and [2] analyze large-scale healthcare disruptions and highlight how insufficient coordination mechanisms and information delays directly affect patient outcomes. While these studies provide valuable insights into systemic weaknesses, they remain largely descriptive and do not propose concrete digital frameworks capable of automating coordination processes under pressure.

The role of digital health platforms in improving operational efficiency has been explored in [3] and [4], where the authors examine the adoption of hospital information systems and electronic documentation. These systems improve data availability within individual institutions but often lack interoperability and cross-organizational integration. From a critical perspective, such solutions are insufficient for emergency scenarios that require coordinated action across multiple hospitals, agencies, and administrative levels.

Personnel management during crises has been addressed in studies such as [5] and [6], which investigate workforce allocation strategies and staffing optimization in healthcare. Although these approaches introduce useful models for personnel planning, they typically rely on manual decision making or isolated optimization tools. They do not consider automation of the entire personnel assignment workflow nor its integration with secure document management and real-time decision support, limiting their applicability in time-critical environments.

Automation of healthcare business processes is discussed extensively in [7]–[9]. These works demonstrate that workflow automation can reduce administrative burden and improve efficiency under normal operating conditions. However, they largely assume stable operational environments and do not adequately address emergency conditions characterized by uncertainty, incomplete information, and rapidly changing requirements. Moreover, security considerations are often treated as secondary concerns rather than core architectural requirements.

Cybersecurity in healthcare information systems is a central theme in [10]–[12]. These studies analyze common attack vectors, regulatory requirements, and data protection strategies. While they provide essential guidelines for securing healthcare data, their focus is predominantly on static systems such as electronic health records. They do not sufficiently address the dynamic and distributed nature of emergency coordination platforms, where access control, auditing, and real-time authorization play a critical role.

Decision-support systems for healthcare operations are examined in [13] and [14], where analytical and rule-based tools are proposed to assist medical and administrative decision making. Although these systems enhance situational awareness, they are often designed as standalone modules that depend heavily on accurate and timely input from multiple sources. Without an integrated automation framework, their effectiveness during large-scale emergencies remains limited.

Several studies explore the use of integrated digital platforms for emergency and disaster management in healthcare settings [15], [16]. These platforms aim to improve communication and coordination between responders. However, many of them prioritize communication over structured personnel and document management. As a result, they lack mechanisms for automated role assignments, compliance tracking, and secure handling of sensitive information.

Interoperability and data integration challenges are discussed in [17] and [18]. The authors highlight how heterogeneous systems and standards hinder seamless information exchange across healthcare organizations. While these studies correctly identify interoperability as a key obstacle, they do not propose architectural solutions that combine interoperability with process automation and security enforcement in a unified framework.

The application of modern information technologies, including cloud-based platforms and service-oriented architectures, is explored in [19] and [20]. These approaches offer scalability and flexibility, which are valuable in high-demand scenarios. Nevertheless, reliance on centralized cloud infrastructures introduces concerns related to availability, data sovereignty, and resilience. From a critical standpoint, these solutions require complementary architectural measures, such as edge-level components and distributed control, to ensure robustness during emergencies.

Security-aware automation frameworks in healthcare are partially addressed in [21] and [22]. These works introduce access control models and auditing mechanisms tailored to healthcare workflows. However, they are typically limited to internal organizational processes and do not extend to cross-institutional coordination or national-level healthcare management.

Process modeling and optimization techniques for healthcare operations are presented in [23] and [24]. While these techniques improve process understanding and efficiency, they often remain abstract and disconnected from implementation considerations such as cybersecurity, compliance, and system integration. Their practical deployment during emergency situations is therefore constrained.

The importance of regulatory compliance and accountability in healthcare information systems is emphasized in [25]. These studies underline the need for traceability, logging, and audit mechanisms. However, compliance is frequently addressed through policy measures rather than being embedded directly into system architecture and automated workflows.

Recent research has begun to acknowledge the need for holistic approaches that integrate technology, organization,

and security. Studies such as [26] and [27] advocate for system-level design of healthcare digital platforms. Despite this progress, these works often remain conceptual and lack detailed architectural frameworks that can be directly applied in emergency and high-demand conditions.

The role of national and regional healthcare coordination platforms is discussed in [28], where the authors emphasize centralized oversight combined with decentralized execution. While this aligns conceptually with emergency management needs, concrete mechanisms for automating personnel management and secure document handling are not sufficiently detailed.

Emerging work on resilient healthcare information systems under crisis conditions is presented in [29]. These studies recognize the importance of adaptability and robustness but do not explicitly address automation of business processes or integrated cybersecurity mechanisms.

Finally, [30] highlights the urgent need for digital solutions that support coordinated healthcare response during emergencies while maintaining high standards of security and compliance. This work underscores the limitations of current systems and implicitly motivates the development of integrated, automated frameworks.

The reviewed literature demonstrates substantial progress in healthcare digitization, automation, and security. However, existing solutions predominantly address isolated aspects such as documentation, cybersecurity, decision support, or workforce management. Few studies adopt a unified architectural perspective that integrates automated personnel management, secure document handling, business process automation, and decision support within a single framework tailored for emergency and high-demand conditions. This fragmentation represents a critical research gap. The framework proposed in this paper directly addresses this gap by offering secure and automated digital architecture designed to support coordinated healthcare operations across organizational boundaries during critical situations.

Tab. 1 – Comparative Review of Related Work on Healthcare Automation, Security, and Emergency Coordination

Reference	Research Focus	Key Contributions	Limitations and Critical Assessment
[1]	Healthcare system response during large-scale crises	Identifies structural and organizational weaknesses in emergency healthcare response	Lacks concrete digital or automated solutions; primarily descriptive
[2]	High-demand healthcare operations	Highlights coordination challenges under extreme workload conditions	Does not propose integrated personnel or document management mechanisms
[3]	Hospital information systems	Improves internal data availability and documentation handling	Limited interoperability across institutions; not suitable for multi-organization emergencies
[4]	Electronic documentation platforms	Enhances digital record management in healthcare	Focused on routine operations; security and emergency automation not central
[5]	Healthcare workforce allocation	Proposes models for staffing optimization	Relies on manual decision making; no automated workflow integration
[6]	Personnel planning in healthcare	Addresses human resource constraints during crises	Does not integrate with real-time digital coordination platforms
[7]	Business process automation in healthcare	Demonstrates efficiency gains through workflow automation	Assumes stable operating conditions; emergency scenarios not addressed
[8]	Administrative automation	Reduces administrative burden in healthcare organizations	Security and compliance treated as secondary considerations
[9]	Process digitalization	Improves operational transparency	Lacks decision-support and cross-institutional coordination
[10]	Healthcare cybersecurity	Analyzes threats and protection mechanisms	Focuses on static systems; limited relevance to dynamic emergency coordination
[11]	Data privacy and compliance	Addresses regulatory requirements in healthcare IT	Does not integrate automation with compliance enforcement
[12]	Secure health information systems	Proposes technical safeguards for healthcare data	Insufficient attention to operational continuity during emergencies
[13]	Decision-support systems	Enhances situational awareness for healthcare management	Standalone tools; dependent on external data integration
[14]	Analytical support tools	Assists medical and administrative decision making	Limited automation of underlying business processes
[15]	Emergency management	Improves communication among	Weak integration of personnel and

	platforms	responders	document management
[16]	Disaster response coordination	Supports information exchange in emergencies	Lacks automated role assignment and secure workflow control
[17]	Healthcare interoperability	Identifies barriers to system integration	No architectural framework for automation and security
[18]	Data exchange standards	Proposes approaches for interoperability	Does not address emergency-driven automation requirements
[19]	Cloud-based healthcare systems	Provides scalability and flexibility	Centralized dependency raises availability and resilience concerns
[20]	Service-oriented architectures	Enables modular healthcare applications	Security and emergency coordination insufficiently addressed
[21]	Access control in healthcare workflows	Introduces role-based access models	Limited to internal organizational processes
[22]	Auditing and accountability	Enhances traceability in healthcare IT	Not integrated into automated emergency workflows
[23]	Process modeling	Improves understanding of healthcare operations	Abstract models with limited implementation guidance
[24]	Process optimization	Enhances efficiency through optimization techniques	Does not consider cybersecurity or emergency constraints
[25]	Regulatory compliance	Emphasizes logging and accountability	Compliance handled procedurally rather than architecturally
[26]	System-level healthcare platforms	Advocates holistic digital design	Lacks concrete automated framework implementation
[27]	Integrated healthcare systems	Promotes coordination across institutions	Security and automation mechanisms not fully defined
[28]	National healthcare coordination	Highlights centralized oversight models	Personnel and document automation not detailed
[29]	Resilient healthcare IT	Recognizes need for adaptability	Automation of business processes not explicitly addressed
[30]	Digital healthcare under crisis	Motivates secure and coordinated digital solutions	Does not provide a unified automated framework

Table 1 presents a comparative review of selected studies related to healthcare automation, digital coordination, and security under emergency and high-demand conditions. The table highlights the primary research focus, key contributions, and inherent limitations of each work. As shown, existing studies typically address isolated aspects such as documentation systems, personnel planning, cybersecurity, or decision-support tools. However, few approaches integrate automated personnel management, secure document handling, business process automation, and cybersecurity within a unified framework. This comparative analysis reveals a clear research gap that motivates the proposed secure and automated digital framework, which aims to provide holistic and resilient support for coordinated healthcare operations during critical situations.

III. METHODOLOGY

The methodology adopted in this study follows a system-oriented and architecture-driven approach aimed at designing a secure and automated digital framework for healthcare personnel and document management under emergency and high-demand conditions. Rather than focusing on isolated software modules or individual organizational procedures, the methodology treats healthcare operations as an interconnected socio-technical system in which personnel coordination, document flows, decision making, and cybersecurity must be jointly addressed. This approach allows the proposed framework to be evaluated not only in terms of technical functionality but also in terms of operational coherence, resilience, and suitability governance at institutional and national levels.

The methodological process begins with the analysis of current healthcare coordination practices during emergency scenarios. In many existing systems, personnel allocation is managed through manual communication channels, informal coordination between hospitals, and static staffing plans. Document handling is often distributed across multiple repositories with limited integration, resulting in delayed access to critical information and reduced situational awareness. These limitations are exacerbated during emergencies, when rapid reassignment of medical personnel and secure access to up-to-date documentation are essential. The first figure represents this operational context by illustrating healthcare coalitions, emergency medical personnel pools, and assignment processes that are currently handled through partially automated or non-integrated mechanisms.

Building on this analysis, the proposed methodology introduces a structured transformation of these processes into an automated and digitally coordinated model. The first enhancement involves formalizing healthcare coalitions and

personnel pools as logical system entities rather than informal organizational constructs. Hospitals within a coalition are modeled as coordinated nodes that share access to a common personnel pool, which is dynamically divided into normal and emergency medical personnel resources. This enables systematic reassignment of doctors, nurses, and supporting staff based on real-time demand rather than predefined static schedules. The methodology explicitly distinguishes between personnel serving general patients and those assigned to infected or high-risk patients, enabling controlled transfer and reassignment under predefined rules. This structured modeling represents a significant change from existing ad hoc coordination practices.

The second methodological enhancement focuses on the automation of personnel assignment decisions. Instead of relying on manual judgment alone, the framework introduces rule-based and workflow-driven assignment mechanisms that consider staff availability, qualifications, workload, and emergency classification. These mechanisms are conceptually represented in the first figure through the transition from personnel pools to assignment blocks. The novelty lies in embedding these assignment processes within a secure digital platform rather than treating them as external administrative tasks. This allows personnel movements and role changes to be tracked, audited, and adjusted dynamically as conditions evolve.

The methodology then extends beyond personnel coordination to address documents and information management, which is represented in the second figure. A key methodological contribution is the integration of document management and personnel management within a single digital architecture. In existing healthcare systems, these functions are often implemented through separate platforms with limited interaction. The proposed framework unifies them through a central document and personnel management server that enforces access control, role management, and configuration policies across all connected institutions.

Document sources such as clinical records, administrative documents, and operational guidelines are ingested into a structured document storage subsystem. This subsystem is divided into document repositories, metadata repositories, and archival repositories, enabling version control, traceability, and long-term compliance. The methodology emphasizes controlled application programming interfaces as the primary means of interaction between system components. This design choice enhances security and interoperability while reducing the risk of unauthorized data access. Backup mechanisms for both documents and personnel data are integrated as core architectural elements rather than optional extensions, improving system resilience.

Personnel data management is handled through a dedicated storage subsystem that maintains personnel profiles, roles, qualifications, and activity logs. The methodology introduces continuous synchronization between personnel status and assignment workflows, ensuring that decision-support mechanisms operate on up-to-date information. This represents a significant enhancement over traditional systems, where personnel records are often updated manually and asynchronously. Audit and activity logs are embedded at the architectural level, supporting accountability and regulatory compliance without requiring additional external monitoring tools.

A central methodological aspect of the proposed framework is the implementation of role-based access control and authorization as foundational system functions. Access to documents, personnel data, and assignment workflows is determined by user roles, institutional affiliation, and operational context. This approach ensures that sensitive information is accessible only to authorized users while still supporting rapid information sharing during emergencies. By embedding authorization logic within the core architecture, the methodology addresses cybersecurity concerns that are frequently treated as secondary considerations in healthcare automation projects.

Decision support and workflow automation form the final pillar of the methodology. The framework includes a workflow and decision-support engine responsible for automating approval processes, personnel assignment rules, and compliance monitoring. Alerts and notifications are generated when predefined thresholds or conditions are met, such as staff shortages, excessive workload, or policy violations. These mechanisms enhance situational awareness for healthcare administrators and enable proactive management rather than reactive response. The novelty here lies in integrating decision support directly with personnel and document management rather than deploying it as a standalone analytical tool.

Importantly, the methodology does not rely on quantitative performance evaluation or simulation results. Instead, it employs architectural analysis and representative operational scenarios to demonstrate how the proposed framework improves coordination efficiency, security, and resilience. This methodological choice aligns with the objectives of the study, which focus on system design and process automation rather than algorithmic optimization. It also ensures that the framework can be adapted to different national healthcare contexts without requiring extensive customization.

The proposed methodology introduces a systematic transformation of healthcare personnel and document management from fragmented, manually coordinated processes into a secure and automated digital framework. By formalizing healthcare coalitions, automating personnel assignments, unifying document and personnel management, and embedding cybersecurity and decision support into the system architecture, the methodology provides a clear path toward enhanced operational readiness under emergency and high-demand conditions. The two figures that follow visually represent this transformation, illustrating both the operational coordination model and the supporting digital platform architecture.

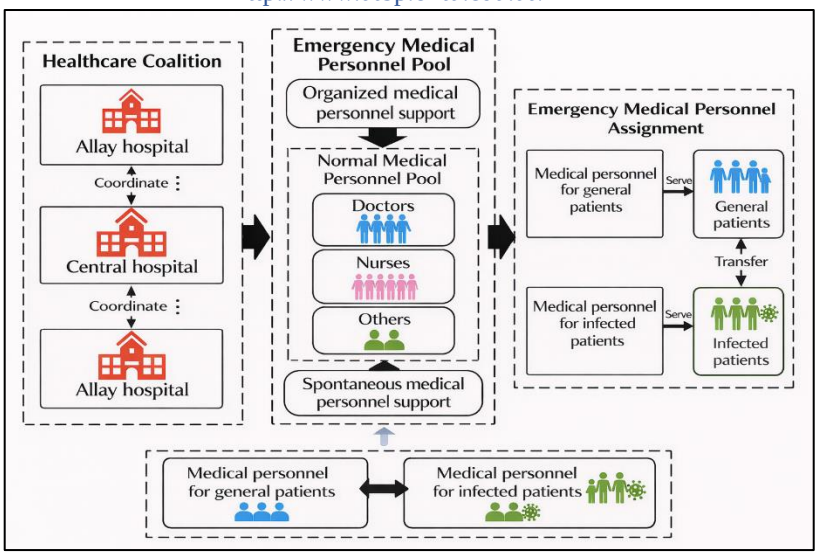

Fig. 1 – Coordinated Emergency Medical Personnel Pooling and Assignment Model [1]

Figure 1 illustrates the proposed operational model for coordinated management and assignment of medical personnel under emergency and high-demand conditions. The model is structured around a healthcare coalition composed of central and allied hospitals that cooperate through a shared coordination mechanism. Medical personnel are organized into a unified emergency personnel pool, which integrates normal medical staff including doctors, nurses, and supporting personnel, as well as spontaneously available emergency support resources. Based on operational needs, personnel are dynamically assigned to serve either general patients or infected and high-risk patients. The model supports controlled transfer of personnel between these assignments, enabling flexible reallocation in response to evolve emergency conditions. This structured approach enhances coordination efficiency, reduces response delays, and provides a foundation for automated and secure personnel management within a digital healthcare framework.

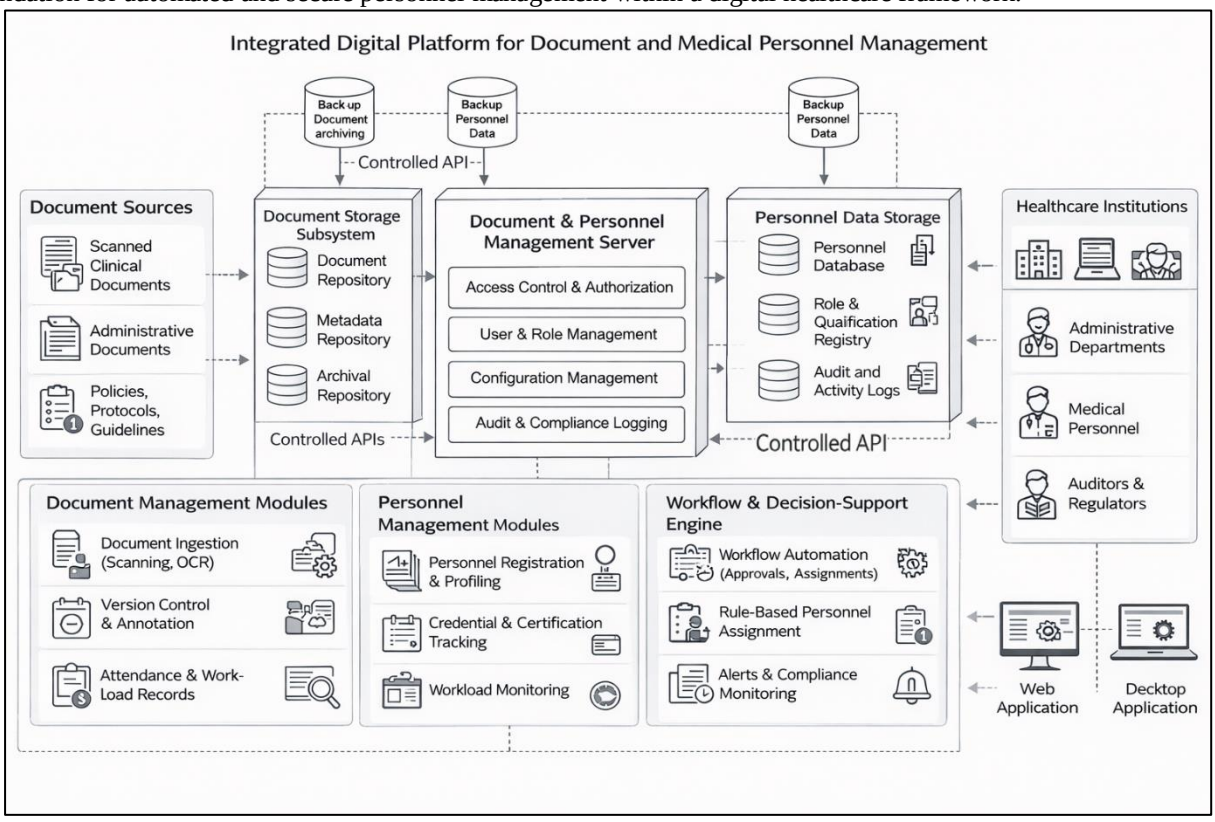

Fig. 2 – Integrated Secure Digital Platform for Healthcare Personnel and Document Management

Figure 2 presents the architecture of the proposed integrated digital platform designed to support secure and automated management of healthcare personnel and documentation under emergency and high-demand conditions. The platform

integrates multiple functional layers, including document storage, personnel data management, access control, and workflow automation, through controlled application programming interfaces. Document sources such as clinical records, administrative documents, and operational guidelines are ingested into a structured document storage subsystem that supports metadata management, version control, and archival functions.

At the core of the architecture, the document and personnel management server enforces role-based access control, user and role management, configuration management, and audit and compliance logging. Personnel data are maintained within a dedicated storage subsystem that includes registries for roles, qualifications, and activity logs, ensuring accountability and regulatory compliance. Backup mechanisms for both documents and personnel data enhance system resilience and operational continuity.

The platform further incorporates workflow and decision-support modules that automate personnel assignments, approvals, and compliance monitoring, while providing alerts and workload monitoring capabilities. Interaction with healthcare institutions, administrative departments, medical personnel, and regulatory bodies is enabled through secure web and desktop applications. This integrated architectural design enhances coordination efficiency, data security, and transparency, providing a robust foundation for digital healthcare process automation in emergency scenarios.

IV. SECURITY AND RESILIENCE ANALYSIS

Security and resilience are critical requirements for healthcare information systems operating under emergency and high-demand conditions, where system failures, data breaches, or operational delays can have direct consequences for patient safety and institutional stability. The proposed digital framework addresses these requirements through an architecture that integrates cybersecurity mechanisms, controlled automation, and operational redundancy at both organizational and technical levels.

From a security perspective, the framework is designed around the principle of controlled access and least privilege. All interactions with documents, personnel records, and workflow functions are governed by role-based access control mechanisms enforced at the core management server. Medical personnel, administrative staff, and regulatory authorities are granted access strictly according to their roles, qualifications, and operational context. This prevents unauthorized access to sensitive clinical or personnel data while still allowing rapid information availability during emergency operations. By embedding access control within the core architecture rather than treating it as an external add-on, the framework ensures consistent enforcement across all participating healthcare institutions.

Data confidentiality and integrity are further supported through controlled application programming interfaces that mediate all communication between system components. These interfaces limit exposure to internal services and reduce the attack surface of the platform. Document ingestion, personnel updates, and workflow execution are all performed through authenticated and authorized channels, minimizing the risk of data manipulation or injection attacks. Audit and activity logging functions are integrated at the architectural level, enabling continuous monitoring of system usage and providing traceability for compliance verification and post-incident analysis.

Resilience against operational disruption is addressed through both organizational and technical mechanisms. At the organizational level, the healthcare coalition model allows multiple hospitals and institutions to operate as coordinated nodes rather than isolated entities. This distributed coordination model reduces dependency on a single institution and enables redistribution of personnel and responsibilities if one facility becomes overloaded or temporarily unavailable. The dynamic personnel pooling and assignment mechanisms support rapid reconfiguration of human resources in response to changing emergency conditions, enhancing operational continuity.

At the technical level, the framework incorporates redundancy through backup document archiving and personnel data replication. These backup mechanisms ensure that critical information remains accessible even in the event of partial system failures or data loss incidents. The separation of document storage, personnel data storage, and workflow management into logically distinct subsystems further improves resilience by preventing cascading failures across the entire platform. If one subsystem experiences degradation, core coordination and decision-support functions can continue to operate.

Automation plays a central role in strengthening resilience by reducing reliance on manual intervention during high-stress situations. Automated workflows for personnel assignments, approval processes, and compliance monitoring help maintain consistent operations even when administrative capacity is limited. Alerts and monitoring mechanisms provide early warnings of abnormal conditions such as excessive workload, staffing shortages, or policy violations, allowing administrators to respond proactively rather than reactively. This contributes to system stability and supports sustained operation during prolonged emergencies.

Cyber resilience is also enhanced by the framework’s emphasis on transparency and accountability. Continuous audit logging and workload monitoring create a detailed operational record that supports both real-time oversight and post-event evaluation. This is particularly important in emergency healthcare environments, where rapid decisions must still comply with legal and ethical standards. By integrating compliance monitoring directly into the operational workflow, the framework reduces the risk of procedural violations while maintaining operational flexibility.

Overall, the security and resilience analysis demonstrates that the proposed framework provides a balanced approach that combines strong cybersecurity controls with operational adaptability. By unifying personnel coordination, document

management, automation, and security within a single architectural framework, the system enhances the ability of healthcare organizations to withstand cyber threats, operational disruptions, and extreme demand conditions. This integrated approach represents a significant improvement over fragmented and manually coordinated healthcare systems and provides a robust foundation for secure and resilient healthcare operations.

V. FUTURE WORK

Future research will focus on extending and validating the proposed secure and automated digital framework through practical implementation and advanced analytical enhancements. One important direction involves the development of a prototype deployment within a real or pilot healthcare environment, enabling evaluation of system behavior under controlled emergencies and high-demand scenarios. Such deployment would allow assessment of usability, scalability, and organizational acceptance, as well as identification of operational challenges that may arise during real-world adoption.

Another promising avenue for future work is the integration of advanced decision-support techniques, including data-driven analytics and artificial intelligence methods, to further enhance personnel allocation and workload balancing. Machine learning models could be employed to predict staffing needs based on historical emergency data, seasonal trends, or early warning indicators, thereby improving proactive resource planning. These capabilities could complement the existing rule-based assignment mechanisms and support more adaptive and context-aware decision making.

Interoperability with national and international healthcare information systems also represents an important area for further development. Future work may explore standardized data exchange interfaces and compliance with emerging healthcare interoperability frameworks, enabling seamless coordination across regional or cross-border healthcare coalitions. This would be particularly relevant for large-scale crises that require cooperation between multiple jurisdictions and public health authorities.

From a security perspective, future research may incorporate advanced cyber resilience mechanisms such as anomaly detection for insider threats, automated incident response workflows, and continuous risk assessment models. These enhancements would further strengthen the framework's ability to operate securely in adversarial or highly stressed environments. Additionally, formal security verification and compliance validation against international standards could be conducted to support broader institutional adoption.

Future studies may investigate the applicability of the proposed framework beyond healthcare, such as in civil protection, emergency management, or other critical infrastructure sectors that face similar coordination and security challenges. By adapting the architectural principles and automation mechanisms to different domains, the framework could contribute to a wider class of secure and resilient digital systems for emergency and high-demand operations.

VI. CONCLUSIONS

This paper presented a secure and automated digital framework for healthcare personnel and document management designed to support coordinated operations under emergencies and high-demand conditions. The study addressed critical challenges faced by modern healthcare systems, including fragmented organizational structures, manual coordination of medical personnel, limited interoperability, and increasing cybersecurity and compliance requirements. By adopting a system-oriented and architectural perspective, the proposed framework responds to these challenges in a holistic and scalable manner.

The contribution of this work lies in the integration of healthcare coalition coordination, dynamic medical personnel pooling and assignment, and unified document and personnel management within a single digital architecture. Unlike existing approaches that focus on isolated functional components, the proposed framework combines business process automation, role-based access control, workflow-driven decision support, and auditability as core design principles. This integration enables more efficient coordination, improved situational awareness, and secure handling of sensitive information during critical operational scenarios.

Through architectural analysis and representative operational models, the paper demonstrated how the proposed framework enhances operational continuity, accountability, and resilience without relying on quantitative performance evaluation. The inclusion of controlled application programming interfaces, backup mechanisms, and automated compliance monitoring strengthens both cybersecurity and system reliability, which are essential requirements for healthcare systems operating under stress. The framework also supports adaptability by enabling dynamic reconfiguration of personnel resources and workflows in response to evolving emergency conditions.

Overall, this work contributes to the field of healthcare automation by providing a structured and security-aware digital framework that bridges organizational coordination and technological implementation. The proposed approach offers practical value for national healthcare systems, emergency response organizations, and public health authorities seeking to modernize healthcare operations while maintaining high standards of security, regulatory compliance, and operational reliability. The framework establishes a solid foundation for future research and practical deployment aimed at strengthening healthcare system preparedness and resilience in emergency and high-demand environments.

VII. REFERENCES

1. Luo, L.; Zhang, R.; Zhuo, M.; Shan, R.; Yu, Z.; Li, W.; Wu, P.; Sun, X.; Wang, Q. Medical resource management in emergency hierarchical diagnosis and treatment systems: A research framework. *Healthcare* 2024, *12*, 1358.
2. Chowdhury, P.; Paul, S.K.; Kaisar, S.; Moktadir, M.A. COVID-19 pandemic related supply chain studies: A systematic review. *Transportation Research Part E: Logistics and Transportation Review* 2021, *148*, 102271.
3. Wu, X.; Zhang, Y.; Guo, X. Research on the equity and influencing factors of medical and health resources allocation in the context of COVID-19: A case of Taiyuan, China. *Healthcare* 2022, *10*, 1319.
4. Xi, Y.; Ding, Y.; Cheng, Y.; Zhao, J.; Zhou, M.; Qin, S. Evaluation of the medical resource allocation: Evidence from China. *Healthcare* 2023, *11*, 829.
5. Moynihan, R.; Sanders, S.; Michaleff, Z.A.; Scott, A.M.; Clark, J.; To, E.J.; Jones, M.; Kitchener, E.; Fox, M.; Johansson, M.; et al. Impact of COVID-19 pandemic on utilisation of healthcare services: A systematic review. *BMJ Open* 2021, *11*, e045343.
6. Zhou, W.; Wang, A.; Wang, X.; Cheke, R.A.; Xiao, Y.; Tang, S. Impact of hospital bed shortages on the containment of COVID-19 in Wuhan. *International Journal of Environmental Research and Public Health* 2020, *17*, 8560.
7. Zhang, L. Research on the current situation of the allocation of public health human resources in China. *International Journal of Social Science and Education Research* 2020, *3*, 295–303.
8. Pan, A.; Liu, L.; Wang, C.; Guo, H.; Hao, X.; Wang, Q.; Huang, J.; He, N.; Yu, H.; Lin, X.; et al. Association of public health interventions with the epidemiology of the COVID-19 outbreak in Wuhan, China. *JAMA* 2020, *323*, 1915–1923.
9. Liu, W.; Yue, X.G.; Tchounwou, P.B. Response to the COVID-19 epidemic: The Chinese experience and implications for other countries. *International Journal of Environmental Research and Public Health* 2020, *17*, 2304.
10. Luo, L.; Wang, Y.; Jiang, P.; Zhuo, M.; Wang, Q. Emergency medical service planning considering dynamic and stochastic demands of infected and non-infected patients during epidemics. *Journal of the Operational Research Society* 2024, *75*, 705–719.
11. He, X.; Luo, L.; Tang, X.; Wang, Q. Optimizing large-scale COVID-19 nucleic acid testing with a dynamic testing site deployment strategy. *Healthcare* 2023, *11*, 393.
12. Holshue, M.L.; DeBolt, C.; Lindquist, S.; Lofy, K.H.; Wiesman, J.; Bruce, H.; Spitters, C.; Ericson, K.; Wilkerson, S.; Tural, A.; et al. First case of 2019 novel coronavirus in the United States. *New England Journal of Medicine* 2020, *382*, 929–936.
13. Mustafovski, R. *Military Communications Doctrine: A Systematic Guide to Command, Control, and Communications in Modern Armed Forces*; LAP LAMBERT Academic Publishing: Saarbrücken, Germany, 2026; ISBN 978-620-9-23709-6.
14. Mustafovski, R. *Secure Communication Systems for Modern Military Operations: Foundations, Technologies, and Future Directions*, 1st ed.; LAP LAMBERT Academic Publishing: Saarbrücken, Germany, 2025; ISBN 978-620-9-27053-6.
15. Mustafovski, R. Formula-Based Architectural Framework of the SecuDroneComm Platform for Unmanned Aerial Vehicle Communications. Management Science Advances, 2, 1, 288–303, 2025.
16. Mustafovski, R. Evaluating the Operational Impact of SecuDroneComm: Simulation-Based Assessment of Secure UAV Communication in Military Environments. Scientific Technical Review, 75, 1, 11–18, 2025. https://doi.org/10.5937/str2500002M
17. Mustafovski, R.; Risteski, A.; Shuminoski, T. Biothreat Early Assist and Response Command System (BEAR-CS). Automation of Technological and Business Processes, 17(1), 78–87, 2025. https://doi.org/10.15673/atbp.v17i1.3091
18. Mustafovski, R. Architectural framework of a mission-centric UAV communication platform. Automation of Technological and Business Processes, 17(4), 48–55, 2025. https://doi.org/10.15673/atbp.v17i4.3324
19. Kadhum Idrees, A.; Alhussein, D.A.; Harb, H. Energy-efficient multisensor adaptive sampling and aggregation for patient monitoring in edge computing-based IoHT networks. *Journal of Ambient Intelligence and Smart Environments* 2023, *15*, 235–253.
20. Safi, K.; Aly, W.H.F.; Kanj, H.; Khalifa, T.; Ghedira, M.; Hutin, E. Hidden Markov model for Parkinson's disease patients using balance control data. *Bioengineering* 2024, *11*, 88.
21. Merhej, J.; Harb, H.; Abouaissa, A.; Idoumghar, L. DeepChain: A deep learning and blockchain-based framework for detecting risky transactions on HIE systems. In *Proceedings of the IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, Paris, France, 14–16 December 2023; IEEE: Piscataway, NJ, USA; pp. 1–6.
22. Ali, S.; Abdullah; Armand, T.P.T.; Athar, A.; Hussain, A.; Ali, M.; Yaseen, M.; Joo, M.I.; Kim, H.C. Metaverse in healthcare integrated with explainable AI and blockchain: Enabling immersiveness, ensuring trust, and providing patient data security. *Sensors* 2023, *23*, 565.
23. Nahm, E.S.; Schoenbaum, A.; Behm, C.; Rowen, L. Health information exchange: Practical overview and implications for nursing practice. *JONA: Journal of Nursing Administration* 2020, *50*, 584–589.
24. Alharbi, A. Applying access control enabled blockchain (ACE-BC) framework to manage data security in CIS

systems. *Sensors* 2023, *23*, 3020.
25. Reegu, F.A.; Abas, H.; Gulzar, Y.; Xin, Q.; Alwan, A.A.; Jabbari, A.; Sonkamble, R.G.; Dziyauddin, R.A. Blockchain-based framework for interoperable electronic health records for an improved healthcare system. *Sustainability* 2023, *15*, 6337.
26. Saad, G.; Harb, H.; Abouaissa, A.; Idoumghar, L.; Charara, N. A sensing-based patient classification framework for efficient patient–nurse scheduling. *Sustainable Computing: Informatics and Systems* 2023, *38*, 100855.
27. Aldousari, A.; Alotaibi, M.; Khajah, F.; Jaafar, A.; Alshebli, M.; Kanj, H. A wearable IoT-based healthcare monitoring system for elderly people. In *Proceedings of the International Conference on Bio-Engineering for Smart Technologies (BioSMART)*, Paris, France, 7–9 June 2023; IEEE: Piscataway, NJ, USA; pp. 1–4.
28. Suliyanti, W.N.; Sari, R.F. Blockchain-based double-layer Byzantine fault tolerance for scalability enhancement in building information modeling information exchange. *Big Data and Cognitive Computing* 2023, *7*, 90.
29. Mohan, R.; Ferris, T. The current state of healthcare information exchange (HIE) and proposing a blockchain HIE infrastructure. In *Blockchain in Healthcare: From Disruption to Integration*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 19–36.
30. Parekh, N.; Mangrulkar, R. Enabling blockchain architecture for health information exchanges. In *Unleashing the Potentials of Blockchain Technology for Healthcare Industries*; Elsevier: Amsterdam, The Netherlands, 2023; pp. 77–93.

УДК 004.896:[658.8:664.6]

КЛАСТЕРНИЙ АНАЛІЗ ПАРТІЙ БОРОШНА В СИСТЕМІ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ЕФЕКТИВНОСТІ ЗАМІСУ ТІСТА

CLUSTER ANALYSIS OF FLOUR BATCHES IN A DECISION SUPPORT SYSTEM FOR THE EFFICIENCY OF DOUGH KNEADING

Рустамов Р.Р.[1], Жигайло О.М.[2]
Rustamov R.R.[1], Zhygailo O.M.[2]

[1,2]Одеський національний технологічний університет, Одеса, Україна
[1,2]Odesa National University of Technology, Odesa, Ukraine
ORCID: [1]https://orcid.org/0009-0000-3667-892X, [2]https://orcid.org/0000-0001-6986-4673
Email: [1]mr.rustamov550@gmail.com, [2]dr_jam2006@ukr.net


DOI: 10.15673/atbp.v18i1.3439

Анотація. *У статті розглядаються результати оглядово-аналітичного дослідження щодо перспектив застосування методів кластеризації для вирішення завдань автоматизації на етапі аналізу сировини та замісу тіста. Впровадження інструментів аналізу даних спрямоване на розв'язання актуальної проблеми стабілізації якості хлібобулочних виробів в умовах, коли фізико-хімічні та реологічні показники основної сировини (борошна) є суттєво нестабільними та піддаються значним природним коливанням. Існуючі традиційні системи управління хлібопекарським виробництвом мають специфіку, пов'язану з використанням жорстко заданих технологічних програм. Ці програми не здатні адаптуватися до поточної варіабельності характеристик кожної конкретної партії борошна (зокрема, до змін кількості сирої клейковини, індексу її деформації та числа падіння), що неминуче призводить до нестабільності структурно-механічних властивостей напівфабрикатів і зниження якості готової продукції. Як базовий математичний інструментарій для інтеграції аналітичного та технологічного рівнів управління запропоновано застосування методу кластерного аналізу. У роботі наведено*