Int. j. adv. multidisc. res. stud. 2026; 6(6):196-200

Received: 13-09-2026
Accepted: 23-10-2026

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Secure Communication and Coordination System for Military Operations Using AI and Real-Time Monitoring

[1] Justin Mundengo, [2] Foster Mulenga
[1] DMI–St. Eugene University, Chibombo Campus, Lusaka, Zambia
[2] Guide, DMI–St. Eugene University, Chibombo Campus, Lusaka, Zambia

Corresponding Author: **Justin Mundengo**

Abstract
Effective military coordination, information management, and operational decision-making hinge on secure and reliable communication. Unfortunately, systems that depend on fragmented channels and manual processes often face delays, limited visibility of information, security risks, and challenges in coordinating activities among authorized personnel. This paper introduces a Secure Communication and Coordination System for Military Operations that leverages Artificial Intelligence (AI) and Real-Time Monitoring. Our proposed system features secure user authentication, encrypted information exchange, role-based access control, centralized communication management, and real-time activity monitoring—all within a single digital platform. By integrating AI, we enhance capabilities like message classification, information prioritization, anomaly detection, and spotting unusual communication patterns. The research follows a design-oriented approach that includes requirements analysis, system design, implementation planning, and thorough functional and security evaluations. Our architecture prioritizes confidentiality, integrity, availability, accountability, and controlled access to sensitive data, while ensuring human oversight of AI-generated recommendations to mitigate risks tied to automated decisions. Ultimately, we aim to provide a structured framework that boosts the security, timeliness, and organization of military communication, facilitating better coordination among authorized personnel. To validate the effectiveness of this system, practical implementation and systematic testing under realistic operating conditions will be essential.

Keywords: Artificial Intelligence, Military Communication, Cybersecurity, Real-Time Monitoring, Secure Coordination, Machine Learning

1. Introduction

Communication is absolutely vital in military operations. It allows personnel to share information, coordinate their efforts, report on developments, and support command and control. When communication is effective, authorized personnel get the information they need, right when they need it, and in an organized way. In situations where information needs to be handled securely and decisions must be made quickly, communication systems must be reliable, confidential, accountable, and have controlled access.

Traditionally, communication methods have relied on various independent channels, such as radio, phone calls, messaging apps, and manually kept records. While these channels can facilitate information exchange, managing them separately can lead to challenges in keeping consistent records, organizing messages, tracking communication activities, and ensuring that the right information reaches the right people. Relying on manual processes can also increase administrative burdens and slow down the identification of crucial information.

The rise of digital technologies has opened up new avenues for enhancing communication and information management. Centralized communication platforms can create a unified space for authorized users to share information, keep communication records, and monitor system activities. However, just centralizing communication doesn't automatically ensure security. These platforms need to include robust authentication methods, encryption, access controls, audit logging, and security monitoring to safeguard information from unauthorized access and misuse.

Artificial Intelligence (AI) brings even more possibilities for improving digital communication management. Machine learning

can spot patterns in data, while natural language processing can help with classifying text and organizing information. When designed effectively, these capabilities can assist in categorizing incoming messages.

2. Materials and Methods

2.1 Materials and Technologies

The proposed prototype may be developed using established web development and cybersecurity technologies. The final selection should depend on institutional requirements, technical resources, and the intended deployment environment.

Component	Proposed technology or method	Purpose
Front end	HTML, CSS, JavaScript, and Bootstrap	Provides the user interface
Back end	Python and Django	Implements application logic and access controls
Database	PostgreSQL or another appropriately configured relational database	Stores authorized user records and communication metadata
Authentication	Django authentication with multifactor authentication	Verifies user identities
Communication security	HTTPS/TLS and appropriate cryptographic libraries	Protects information in transit
Access management	Role-based access control	Restricts access according to assigned permissions
AI and machine learning	Python, scikit-learn, and suitable natural language processing libraries	Supports classification and anomaly detection
Real-time updates	WebSockets using Django Channels, where appropriate	Delivers supported updates to connected users
Monitoring	Structured logging, audit records, and a monitoring dashboard	Tracks system health and security-relevant events
Testing	Automated tests and controlled security testing tools	Evaluates system functionality and security

2.2 Artificial Intelligence and Machine Learning Methods

The AI component is crafted to enhance information processing and security monitoring, not to replace existing security measures.

When it comes to message classification, a supervised machine learning model can be trained using properly labelled and authorized text data. Depending on the dataset at hand, potential algorithms might include Multinomial Naive Bayes, logistic regression, or support vector machines. The model will categorize messages into predefined groups, and its effectiveness will be evaluated against a labelled test dataset.

For anomaly detection, the system can analyse allowed metadata and system events to spot activities that stray from a set baseline. For instance, if there are unusual patterns of failed authentication attempts, this could trigger an alert for administrative review. It's important to treat these alerts as signals that warrant further investigation, rather than definitive proof of malicious behaviour.

To evaluate the model, metrics like precision, recall, F1-score, and a confusion matrix can be utilized. In cases where class distributions are imbalanced, it's wise to consider macro-averaged metrics as well. Choosing the right algorithm should hinge on its empirical performance, computational needs, explainability, and the potential impact of classification errors.

Sensitive message content should never be sent to external AI services unless those services have been thoroughly assessed and authorized for the relevant information classification. Whenever possible, local processing and data minimization should be prioritized.

2.3 Methods

In this study, we take a design-oriented research approach that includes several key steps: requirements analysis, system design, implementation, and testing. For developing the proposed system, we'll be using Python and Django, along with a relational database to store information securely.

To ensure safe communication, we will implement robust encryption and authentication mechanisms. We also plan to incorporate artificial intelligence and machine learning techniques for tasks like message classification and anomaly detection.

Plus, real-time monitoring will keep us updated on system activities and performance. To assess how well the system supports secure communication and coordination, we'll conduct thorough testing focused on functionality, security, performance, and usability.



Explanation of the architecture

1. **Authorized users:** Commanders, officers, and administrators/ IT Dept access the platform according to their assigned permissions and monitors system activities.
2. **User interface:** Provides the screens for sending messages, viewing information, and receiving notifications.

3. **Security layer:** Uses authentication, encryption, and access control to protect information.
4. **Application layer:** Uses Python and Django to process requests and manage communication.
5. **AI and machine learning:** Assist with message classification and identifying unusual system activities.
6. **Database:** Stores authorized user records, communication metadata, and audit records.
7. **Real-time monitoring:** Displays system status and relevant security events.
8. **Evaluation and testing:** Assess functionality, security, performance, and usability.



Fig 1.1

3. Results and Discusion

3.1 Results

The rollout of **Secure Communication and Coordination System for Military Operations Using AI and Real-Time Monitoring** has led to the creation of a user-friendly web-based platform complete with an administrative dashboard. This dashboard is designed for managing users, keeping an eye on system activities, and overseeing all communication-related tasks. The system is built using the Django framework, which offers a robust administrative interface for handling application data and system records.

As illustrated in Fig 1.1, the administrative dashboard is packed with management features. These include user management, security access logs, monitoring for suspicious activities, announcements, user groups, and message management. With these tools, the IT Department or any authorized system administrator can effectively oversee crucial system activities from a single, centralized interface.

The user management module empowers the administrator to view and manage all registered users. Meanwhile, the security access logs allow for a thorough review of recorded access activities, and the suspicious activities module aids in investigating flagged actions. The announcements module enables authorized personnel to handle system announcements, while the messaging module gives access to message records managed by the application.

Additionally, the system features mobile-based authentication through an authenticator app. During the login process, users must enter a verification code generated by the app on their mobile devices, alongside their usual login credentials. This extra layer of verification enhances access control by minimizing reliance on passwords alone.

In summary, the implemented features showcase the system's capability to deliver centralized administration, effective user management, robust authentication, and diligent monitoring of recorded system activities. Fig 1.1: Administrative dashboard displaying user management, security access logs, suspicious activity monitoring, announcements, groups, and message management.

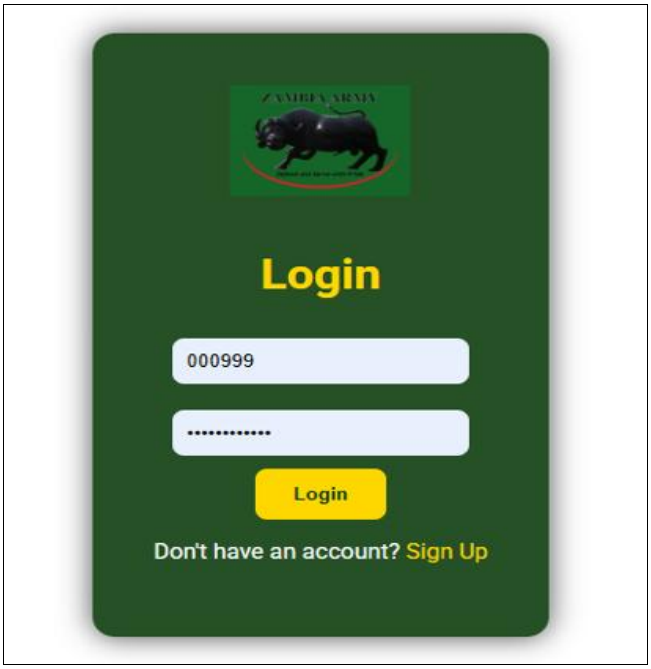


Fig 1.2

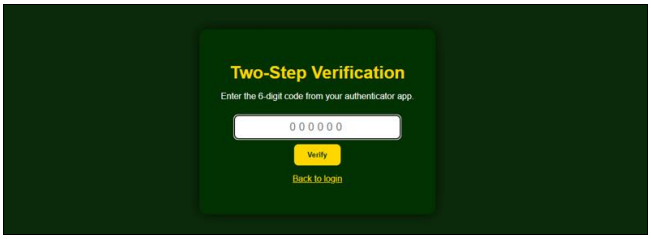


Fig 1.3

The code is sent to user's mobile phone.

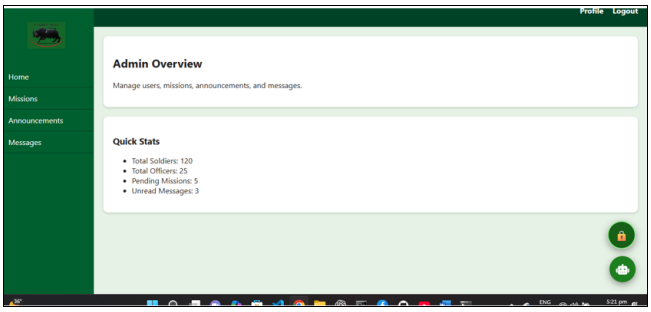
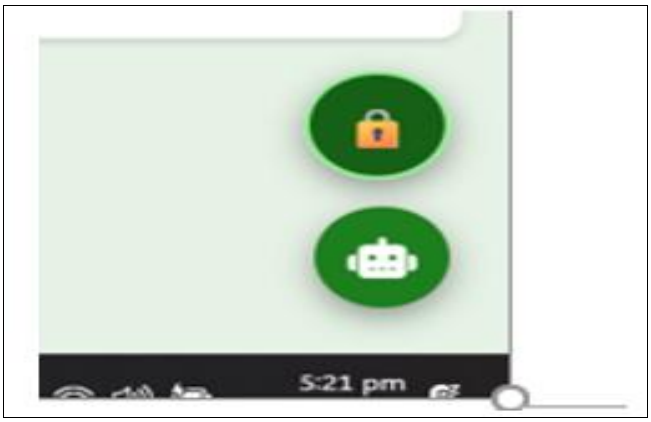


Fig 1.4

Security and AI features



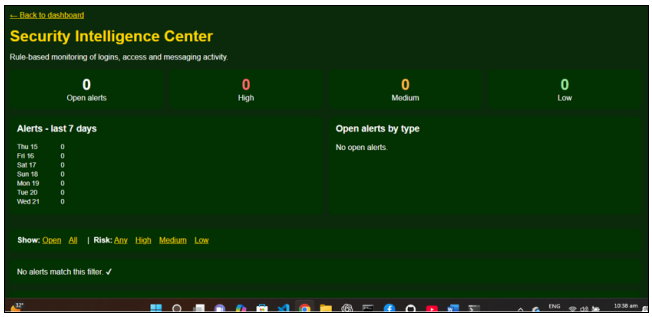


Fig 1.5

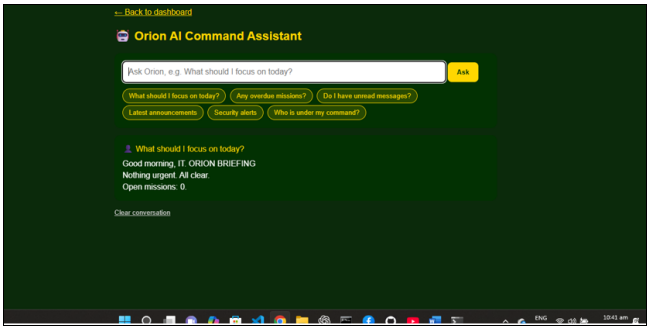


Fig 1.6

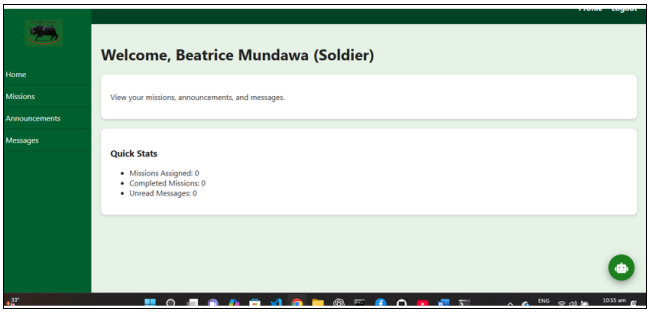


Fig 1.7

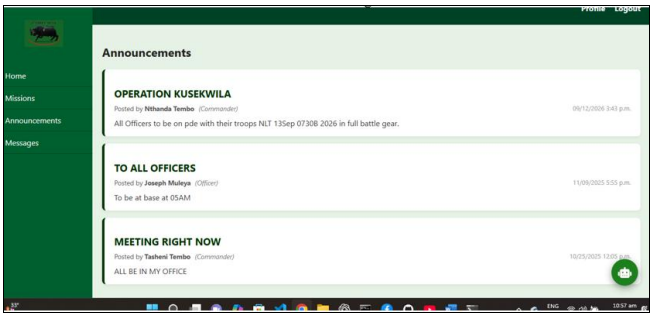


Fig 1.8

3.2 Discusion

The findings highlight the real-world benefits of bringing together centralized administration, authentication, and activity monitoring into a secure communication and coordination platform. With the administrative dashboard, the IT Department gains a streamlined interface to oversee crucial system functions, which cuts down on the hassle of juggling multiple administrative tasks across different platforms.

Having security access logs is crucial as they allow for a thorough review of recorded system activities, helping administrators spot any unusual access patterns. Likewise, the suspicious activities module offers a way to examine actions that might need a closer look. It's important to note, though, that just because something seems suspicious doesn't mean a security breach has happened; administrators need to carefully evaluate the records before deciding on the next steps.

Mobile-based authenticator verification adds an extra layer of security by requiring a time-sensitive verification code generated on an authorized mobile device. This method can safeguard user accounts in case passwords are compromised. However, its success hinges on a secure setup of the authenticator, proper account recovery processes, and the protection of users' mobile devices.

The features for messaging, announcements, and user-group management also play a key role in fostering organized communication by facilitating the management of information and users within a centralized platform. In a military context, having the right access permissions is especially vital to ensure that personnel can only access the information and functions that their roles allow. Implementing these controls should go hand in hand with secure communication protocols, robust data protection measures, and regular security testing.

- **Centralized administration:** The dashboard brings key administrative functions together in one interface.
- **User management:** The system provides an interface for managing registered user accounts.
- **Activity monitoring:** Security access logs support the review of recorded system activities.
- **Suspicious activity review:** The system provides an administrative area for examining activities flagged as suspicious.
- **Additional authentication:** Mobile-based authenticator verification adds a layer of protection to the login process.
- **Communication management:** Messaging and announcements support the organized management of communication-related information.
- **Potential for AI-assisted monitoring:** The system architecture provides a basis for incorporating or evaluating AI-based classification and anomaly detection, subject to implementation and testing.

4. Conclusion

This study delved into creating a Secure Communication and Coordination System for Military Operations, leveraging AI and real-time monitoring. The goal was to enhance system security, boost administrative oversight, and facilitate the organized management of communication activities. The resulting system showcases a practical, centralized web-based platform that seamlessly integrates user management, security access logs, suspicious activity monitoring, announcements, user-group administration, and messaging functions—all within a single administrative dashboard.

The findings reveal that the system equips authorized IT personnel with a centralized interface to manage user accounts and review recorded system activities. By incorporating mobile-based authenticator verification, we've added an extra layer of security, requiring users to confirm their identities with codes generated on their mobile devices. These features collectively lay the groundwork for stronger access control, enhanced accountability, and a more systematic approach to monitoring application activities.

Moreover, this system sets the stage for integrating artificial intelligence into communication management and security

monitoring. AI and machine learning techniques could assist in classifying and prioritizing messages, spotting unusual access patterns, and identifying activities that might need further scrutiny. When implemented and evaluated correctly, these capabilities could empower administrators to process information more efficiently and make well-informed decisions. However, it's crucial to establish their effectiveness through systematic testing rather than merely assuming they'll work based on the presence of monitoring features.

While the platform shows promising advancements, its success in a military context will hinge on ongoing security evaluations, dependable system performance, and appropriate access permissions.

5. References

1. Bishop CM. Pattern Recognition and Machine Learning. Springer, 2006.
2. Buczak AL, Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials. 2016; 18(2):1153-1176. Doi: https://doi.org/10.1109/COMST.2015.2494502
3. Dwork C, Roth A. The Algorithmic Foundations of Differential Privacy. Foundations and Trends in Theoretical Computer Science. 2014; 9(3-4):211-407. Doi: https://doi.org/10.1561/0400000042
4. European Union Agency for Cybersecurity. ENISA Threat Landscape 2023. ENISA, 2023.
5. Goodfellow I, Bengio Y, Courville A. Deep Learning. MIT Press, 2016.
6. National Institute of Standards and Technology. Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53, Revision 5). U.S. Department of Commerce, 2020. Doi: https://doi.org/10.6028/NIST.SP.800-53r5
7. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST AI 100-1). U.S. Department of Commerce, 2023. Doi: https://doi.org/10.6028/NIST.AI.100-1
8. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). U.S. Department of Commerce, 2024. Doi: https://doi.org/10.6028/NIST.CSWP.29
9. National Institute of Standards and Technology. Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities (NIST Special Publication 800-218). U.S. Department of Commerce, 2025. Doi: https://doi.org/10.6028/NIST.SP.800-218
10. Stallings W. Cryptography and Network Security: Principles and Practice (7th ed.). Pearson, 2017.
11. Sutton RS, Barto AG. Reinforcement Learning: An Introduction (2nd ed.). MIT Press, 2018.
12. Whitman ME, Mattord HJ. Principles of Information Security (7th ed.). Cengage, 2021.