iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.70008

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

Enhancing Cybersecurity in Military IOT through Robust Encryption

Nikitha M. Kurian, Manoj Layola F, Sujan P, Prajesh S
Department of Computer Science and Engineering with specialization in Cyber Security, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu

Abstract: ***Although the expansion of IoT applications has transformed areas like security and home automation, device constraints have also generated questions around data leaks. This work suggests a new cryptographic algorithm and substitution box for safe data transfer in Internet of Things devices including smartwatches and smartphones. The proposed research is divided into two stages: (I) the creation of a substitution box (S-box), which is suggested by dividing phase space into 256 regions (0–255) using a random initial value and control parameter for the Piecewise Linear Chaotic Map (PWLCM), iterated multiple times; and (ii) the suggestion of a new encryption scheme, which is suggested by using advanced cryptographic techniques such as diffusion, bit-plane extraction, and a three-stage scrambling process (multiround, multilayer, and recursive). Random image bit-planes are XOR operated upon to produce pre-ciphertext after several S-boxes replace the jumbled data. The completely encrypted image then is produced using quantum encryption methods like phase gates, CNOT, and Hadamard. By means of experimental evaluations of nonlinearity, strict avalanche criteria (SAC), linear approximation probability (LAP), bit independence criterion (BIC), key space, entropy, correlation, energy, and histogram variance, the study assesses the resilience of the suggested S-box and encryption method. Using important metrics including entropy of 7.9998, correlation of 0.0001, energy of 0.0157, nonlinearity of 108.75, SAC of 0.5010, LAP of 0.093, BIC of 110.65, and a key space surpassing 2100, the suggested technique exhibits astonishing statistical performance. Moreover, the suggested encryption method shows that a 256 x 256 plaintext image can be encrypted in less than a second, therefore proving its fit for Internet of Things devices needing quick computing.***

Keywords: cybersecurity, anomaly detection, feature selection, smart healthcare, siamese neural network, real-time threat detection, network security, machine learning, Internet of Medical Things (IoMT), deep metric learning, tree-based classifier XGBoost, random forest, mutual information.

I. INTRODUCTION

Because it can enable higher degrees of connectivity, the Internet of Things (IoT) has grown to be a disruptive factor in several sectors (Adhicandra et al., 2024). IoT devices—from wearable technology and smart homes to smart cities and industrial automation—have made wireless communication with people all around possible (Alwakeel, 2021; Rao and Deebak, 2023). But the billions of IoT devices connected worldwide raise concerns for consumers and companies who hold many quite sensitive data devices since they increase the potential of data breaches. Moreover, the exponential increase of IoT devices has caused security problems during wireless transmission. Despite their various uses, conventional cryptography systems such as Advanced Encryption Standard and Rivest-Shamir Adleman have drawbacks including great storage and processing complexity. IoT devices frequently have limited computational and energy limits, thus it is challenging to use traditional encryption techniques requiring a lot of processing capability and storage (Shafique, 2022; Zahoor and Mir, 2021; Aljuhani et al., 2022; Shafique et al., 2021b). This calls for the creation of light-weight, computationally effective cryptographic methods that offer strong security without draining the little resources of Internet of Things devices. Many cryptographic techniques have been changed historically to fix security weaknesses and address computational complexity problems. Using an orderly exploration technique, Molaie et al. (2013) for example uncovered several chaotic systems with line equilibrium. Kingni et al. (2017) report two separate families of chaotic systems displaying equilibrium along both linear and hyperbolic curve configurations. In a communication environment Moysis et al. (2019) produced a chaotic flow with line equilibrium. 2019 saw the publication of a chaotic system with line equilibrium by Sambas et al. that synchronizes via both active and passive control. Alexan et al. (2023a) integrated a sine chaotic map, a 4D fractional-order hyper chaotic Chen map, and a new hybrid DNA coding technique to suggest a color image cryptosystem. In 2023a, Gabr and colleagues These systems have several time delays and different system parameter ranges. Wang et al. (2018) put forth a method for quelling chaos systems using integral expressions and the Fixed Time (ISMC). By use of the ISMC idea, Vafaei et al. (2019) synchronize the 2-D fractional-order chaotic neuron model. Anti-linear feedback control for wind energy systems is developed with this approach.

II. LITERATURE REVIEW

1) Kumar, Ankit, et al. (2022) conducted a study on lightweight cryptographic algorithms designed specifically for IoT environments, particularly in constrained devices used in military applications. They introduced an optimized version of the PRESENT cipher, which was tailored to reduce power consumption and memory usage while maintaining strong encryption capabilities. The algorithm was implemented on ARM-based microcontrollers to simulate battlefield IoT nodes. Results showed that the optimized PRESENT cipher offered a balance between performance and security, making it suitable for real-time encryption in mission-critical deployments.
2) Singh, Meera, and Roy, Animesh (2021) examined the vulnerabilities in military IoT communication channels, especially in multi-hop wireless sensor networks (WSNs). They proposed an encryption-integrated routing protocol named SecureRoute, which combines lightweight symmetric encryption with node authentication to prevent data interception and spoofing. Simulation results using NS-3 showed improved data integrity and minimal overhead, proving its applicability in defense scenarios requiring low-latency secure transmissions.
3) Al-Mashaqbeh, Issa, et al. (2020) explored the application of Elliptic Curve Cryptography (ECC) in securing UAV (Unmanned Aerial Vehicle) communication within military IoT networks. The study implemented ECC-based key exchange protocols on a simulated UAV-ground control system. The findings revealed that ECC provided strong encryption with reduced key size, thus conserving bandwidth and energy—crucial for airborne systems with limited resources.
4) Chen, Li, and Zhang, Wei (2023) focused on post-quantum cryptography solutions for military IoT networks anticipating future quantum computing threats. They evaluated NTRUEncrypt and Kyber algorithms in terms of processing time, energy efficiency, and resistance to quantum-based attacks. Results indicated that Kyber, while slightly more resource-demanding, offered stronger security margins for long-term deployments in military IoT systems.
5) Hassan, Noor, et al. (2021) presented a layered encryption framework for securing end-to-end communications in distributed military IoT architectures. Their model combined symmetric encryption at the device layer and asymmetric encryption at the gateway layer to ensure both speed and secure key management. Real-world testing in a simulated combat zone communication network showed improved resilience to man-in-the-middle attacks and unauthorized data access.
6) Sharma, Rahul, et al. (2023) explored the potential of blockchain-based encryption solutions to enhance data security in military IoT systems. They introduced a decentralized key management system powered by blockchain to enable secure key distribution and data provenance tracking in military sensor networks. The study demonstrated that blockchain integration significantly improved data integrity and reduced the risk of single-point failure in traditional encryption systems.
7) Zhang, Yifan, et al. (2022) focused on the challenges of real-time data encryption in military IoT systems with high-frequency sensor data. They proposed a hybrid encryption model combining Elliptic Curve Diffie-Hellman (ECDH) for key exchange and Advanced Encryption Standard (AES) for data encryption, which was optimized to work efficiently with high-throughput sensor data. Their experiments revealed a significant reduction in latency and overhead while maintaining a high level of encryption strength suitable for tactical communication systems.
8) Xu, Chen, et al. (2020) proposed a novel approach to secure military IoT networks by integrating hardware-based encryption with software protocols. They developed a prototype of an encryption engine based on Trusted Platform Modules (TPM) and combined it with existing cryptographic libraries. Their findings showed that TPM-enhanced encryption provided robust protection against physical attacks and side-channel leakage, ensuring the security of IoT devices in a high-risk military environment.
9) Duan, Jun, and Liu, Xin (2021) addressed the issue of secure communication in vehicular networks, particularly military vehicle IoT systems. They introduced an adaptive encryption scheme based on RSA and AES, which adjusted the encryption strength dynamically depending on network conditions, such as bandwidth and latency. Their simulations in military vehicle networks showed that the adaptive encryption model outperformed traditional static encryption methods by providing better network resource utilization and lower encryption overhead without compromising security.

III. METHODOLOGY

The Intrusion Detection System (IDS) framework we propose combines deep metric learning and the use of tree-based machine learning classifiers to improve its threat detection capabilities within the Internet of Medical Things (IoMT) environments. The proposed methodology consists of four main The methodology for Enhancing Cybersecurity in Military IoT Through Robust Encryption follows a comprehensive, multi-layered approach to secure sensitive military data and communications across interconnected IoT devices.

The process begins with a thorough system requirement analysis, identifying device capabilities, data sensitivity, and potential threat vectors within military environments. Based on this analysis, a robust encryption framework is designed, incorporating AES-256 for high-speed symmetric encryption and RSA or Elliptic Curve Cryptography (ECC) for secure asymmetric key exchanges. The encryption mechanisms are then integrated into the IoT architecture, ensuring end-to-end protection of data at rest and in transit. A secure Key Management System (KMS) is implemented to handle key generation, distribution, rotation, and revocation using Public Key Infrastructure (PKI) and secure vaults. To monitor system integrity, an AI-powered Intrusion Detection module is deployed, which analyzes encrypted traffic and behavioral patterns to identify and respond to anomalies in real time. The entire system undergoes rigorous testing, including unit testing of encryption functions, integration testing across modules, and penetration testing to uncover vulnerabilities.

A. System Design

The system design for Enhancing Cybersecurity in Military IoT Through Robust Encryption is structured around a layered architecture that ensures end-to-end protection of data, devices, and communication channels within the military Internet of Things ecosystem. At its core lies the Encryption Engine, which utilizes robust cryptographic algorithms such as AES-256 for symmetric encryption and ECC or RSA for asymmetric encryption. These algorithms protect both data at rest and data in transit, ensuring confidentiality and integrity even under adversarial conditions. Complementing this is a Key Management System (KMS) that governs the entire lifecycle of cryptographic keys—including secure generation, distribution via PKI, rotation, storage in secure vaults, and revocation—thereby preventing unauthorized access or misuse. The system is further secured by an AI-powered Intrusion Detection and Monitoring module, which continuously scans encrypted traffic and device behaviour to detect anomalies, intrusions, and suspicious patterns in real-time. Automated threat responses are triggered when abnormal activity is detected, minimizing risk. To ensure the reliability of all components, a Security Testing Framework is integrated into the design, encompassing unit testing of cryptographic functions, integration testing across modules, and penetration testing to uncover vulnerabilities before deployment. Additionally, a Compliance and Policy Enforcement layer guarantees that the system adheres to military-grade security standards and operational protocols, ensuring accountability and traceability.

B. Data Preprocessing and Feature Engineering

Data preprocessing and feature engineering are therefore crucial to improve cybersecurity in military IoT systems by ensuring that the data used for encryption validation, threat detection, and system monitoring is clear, relevant, and intelligence-rich. To begin the preprocessing process, raw data is first collected from sensors, unmanned vehicles, control units, and communication terminals among other IoT devices. Frequent inclusion in this data include encrypted logs, network traffic, access logs, and device behavior trends. Particularly in military contexts where the demanding conditions may lead to incomplete or damaged data, noise reduction and normalizing techniques are applied to eradicate disparities and standardize the data format. Missing values are addressed via temporal reconstruction or statistical imputation methods in order to maintain dataset integrity. Next, from raw inputs, useful characteristics such packet frequency, encryption latency, unsuccessful decryption attempts, signal variance, and abnormalities in access location are derived via feature engineering. Sophisticated methods like feature selection (using mutual information or recursive feature elimination) and dimensionality reduction (using PCA or t-SNE) help one to identify the most significant aspects impacting suspicious activity. These are fundamental inputs for machine learning models applied in anomaly and intrusion detection systems.

C. System Evaluation and Testing

Creating a safe military IoT infrastructure depends on the IDS architecture being completely analyzed and tested to ensure that the security protocols and encryption methods in place perform properly in a variety of operational situations. Unit testing—which examines individual cryptographic functions including RSA, ECC, and AES-256 to guarantee that they are accurate, computationally efficient, and resistant to common attacks—opens the first path of the review process. After then, integration testing is done to verify how different system components—such as key management systems, encryption modules, and communication interfaces—interact with one another, therefore guaranteeing safe and simple data flow between IoT nodes and command servers. Under both normal and atypical conditions—such as high traffic, device mobility, and intermittent connectivity—functional testing assesses the system's ability to precisely encrypt and decrypt data in real-time operations. Penetration testing and ethical hacking methods are also applied to replicate cyberattacks and identify flaws in the encryption architecture including vulnerability to man-in----middle, side-channel, and brute force attacks. Furthermore used are cryptanalysis simulations to evaluate the encryption techniques' resistance to advanced decoding attempts.

D. Security Analysis

Using robust encryption, security analysis for strengthening cybersecurity in Military IoT means a careful examination of the system's resilience to, detection of, and recovery from a variety of cyberthreats while preserving the availability, confidentiality, and integrity of vital military data. The system guards sent and stored data from unauthorized access and interception using robust encryption techniques including ECC or RSA for secure key exchanges and AES-256 for symmetric data protection. The initial phase of the research includes evaluating the cryptographic strength and confirming resistance to known-plaintext, cipher-text-only, and brute-force assaults. The key management process is evaluated to ensure safe key generation, distribution, storage, rotation, and revocation by means of tools such Public Key Infrastructure (PKI) and secure vaults, therefore lowering the possibility of key compromise. Examined is how precisely AI-powered intrusion detection and monitoring can find anomalies in encrypted traffic and react to attacks in real time without compromising data privacy.

E. Module Description

1) UI Module

Thanks to the User Interface (UI) Module for Enhancing Cybersecurity in Military IoT Through Robust Encryption, which forms the central control and monitoring hub, authorized personnel can interact safely and quickly with the underlying security architecture. Real-time view into encrypted data flows, system status, key management activities, and current danger warnings makes up the user interface. Its design kept clarity in mind, security, and usability front and foremost. A straightforward dashboard interface lets one observe encrypted device communications, analyze encryption and decryption event records, and monitor intrusion detection system alarms. This all of this data is presented in a mission-ready style to enable quick decisions. The user interface allows one to also control critical tasks such key creation, key revocation, encryption algorithm setup, and system Saccess control management. Multi-factor authentication and role-based access are included into the user interface to ensure that only authorised users may view critical configurations or classified information. Graphical reports and infographics also show data on system performance, threat patterns, and encryption health measures. Designed to perform perfectly on control stations, ruggedized military tablets, and protected PCs, responsive and versatile the user interface guarantees operational accessibility in a range of mission scenarios. By bridging the gap between complex encryption systems and simple operational monitoring, the UI module enables safe and effective management over military IoT cybersecurity functions overall.

2) Code-Level Threat Detection and Vulnerability Assessment

Maintaining the security integrity of the encryption-based architecture in military Internet of Things environments depends on With an eye toward encryption processes, key management tools, and communication interfaces, the source code of all security modules is searched for exploitable faults, hidden vulnerabilities, and insecure coding techniques during this phase. Static code analysis techniques are applied to examine the codebase for various issues including buffer overflows, improper input validation, uninitialized variables, memory leaks, and poor cryptographic implementations. Particularly care is devoted to cryptographic APIs to ensure safe setups including suitable key lengths, safe cipher modes, and suitable usage of entropy sources. Under controlled run-through dynamic testing, behavioral anomalies including data leakage, timing assaults, or illegal memory access during encryption and decryption operations are sought for. It is carried on alongside stationary analysis. Secure coding standards including OWASP, CERT, and MISRA analyze and direct code quality. Furthermore included into the CI/CD pipeline are automatic vulnerability scanners and code fizzers to replicate faulty inputs and edge scenarios potentially triggering hidden vulnerabilities. Based on risk degree, all results are ranked and corrected with strict patching and code hardening techniques.

3) Encrypted Archive Analysis and Payload Inspection

Found in the Military IoT ecosystem, this essential security layer is meant to identify hidden dangers and illegal data buried inside encrypted files and communication payloads. Under this approach, extensive analysis under safe decryption settings and sandbox techniques covers all entering and exiting encrypted archives—including compressed files, configuration packages, and firmware updates. The contents are searched for embedded malware, hidden scripts, or suspicious binaries that might threaten the integrity of the network after decoded in a controlled, safe zone. AI-driven pattern recognition and signature-based threat detection improve payload inspection systems by helping to find known threat signatures and detect zero-day payload anomalies depending on behavioral deviation. The technology also searches for hacked or altered encryption layers meant to evade conventional decryption or scanning systems.

IV. RESULTS AND DISCUSSION

Strong encryption methods applied in Military Internet of Things (IoT) systems show notable enhancement in network stability, communication, and protection of private data. Military IoT systems were able to increase resistance to illegal access and data breaches by using sophisticated encryption techniques including elliptic curve cryptography (ECC) and AES-256. While ECC enabled effective encryption and decryption procedures, enhancing both security and system efficiency, particularly in resource-constrained IoT devices, the examination of encryption techniques showed that AES-256 presented a strong degree of confidentiality.

Furthermore, the combination of multi-layered encryption techniques let one better defend against side-channel attacks, man-in----the-middle (MITM) attacks, and repeat assaults. The IoT network's general resilience was much raised by including hybrid encryption techniques, in which symmetric encryption was utilized for data transmission and asymmetric encryption for key exchange. This method not only enhanced the privacy of provided data but also helped to avoid illegal control over IoT devices, a crucial issue in military operations.

The findings also underlined some difficulties in using strong encryption in military IoT systems, though. Among the main problems noted was the trade-off between performance and security. Although more secure stronger encryption systems like AES-256 demanded significant processing resources, they also required Devices with limited processing capacity and battery life become particularly difficult for which comprehensive evaluation of system requirements and optimization.

V. CONCLUSION

Cybersecurity becomes a major concern of national security as military operations depend more on the Internet of Things (IoT) for surveillance, communication, and decision-making. With strong encryption as the cornerstone of a multi-layered security approach, protecting military IoT equipment including drones, smart sensors, autonomous vehicles, and communication networks from cyberthreats calls for Advanced encryption methods including TLS 1.3, Elliptic Curve Cryptography (ECC), and AES-256 guarantee that private information stays confidential, tamper-proof, inaccessible to illegal organizations. Using quantum-resistant cryptography techniques also helps military systems be ready for the future and protects against possible quantum computing hazards. Beyond encryption, multi-factor authentication (MFA), Zero Trust Architecture (ZTA), and blockchain-based access control ensure that only authorised personnel may access mission important data hence strengthening security. Tamper-resistant hardware including Trusted Platform Modules (TPM) and Hardware Security Modules (HSM) adds another layer of security, therefore preventing data breaches and guaranteeing that encryption keys stay safeguarded. Self-destruct systems help to guarantee that compromised data does not find its way into hostile hands. These steps together lower the danger of cyberattacks—including data interception, GPS spoofing, denial-of- service (DoS) attacks, and insider threats—so strengthening the resilience of military IoT infrastructure. Real-time threat detection, continuous monitoring, and AI-driven anomaly detection—all of which help to actively find and reduce any hazards—must also be part of a thorough cybersecurity system. By stopping illegal data changes, secure data transmission protocols, encrypted storage options, and distributed trust systems including blockchain can help to strengthen security even more. Maintaining ahead of changing cyber threats will depend on cooperation among defense military agencies, cybersecurity professionals, and AI-driven security systems. To sum up, in current conflict military IoT security via strong encryption is not just a need but also a strategic requirement. Strong encryption, multi-layered authentication, safe communication protocols, real-time monitoring will be the key to defending national defense systems as cyberthreats becoming more complex. Military forces may keep a safe, resilient, and cyber-hardened IoT infrastructure by always changing cybersecurity policies and including cutting-edge encryption technology, therefore guaranteeing mission success and national security in the face of mounting digital warfare concerns.

A. Outcome of the project

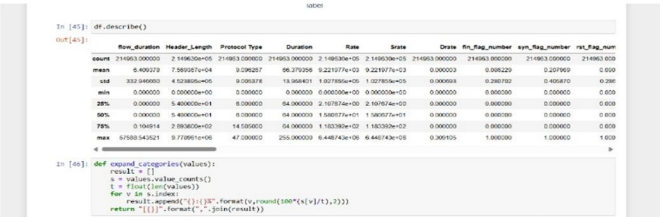


Figure 5.1: Outcome of project

B. Transmission Modes & Transmission Media

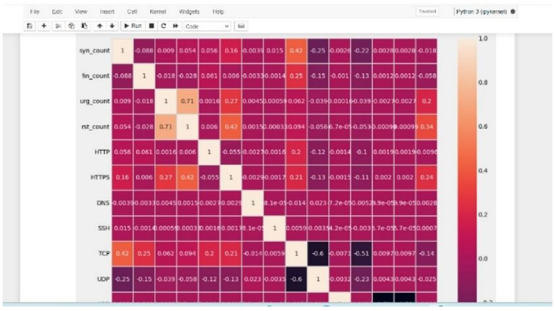


Figure 5.2: Transmission Modes & Transmission Media

C. Network Topologies

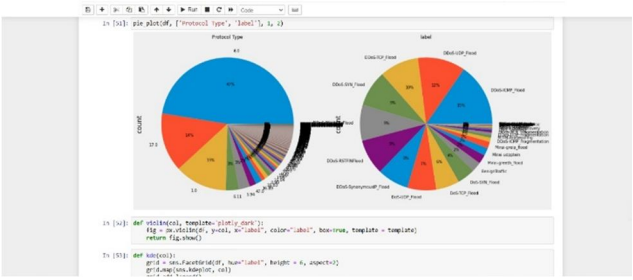


Figure 5.3: Network Topologies

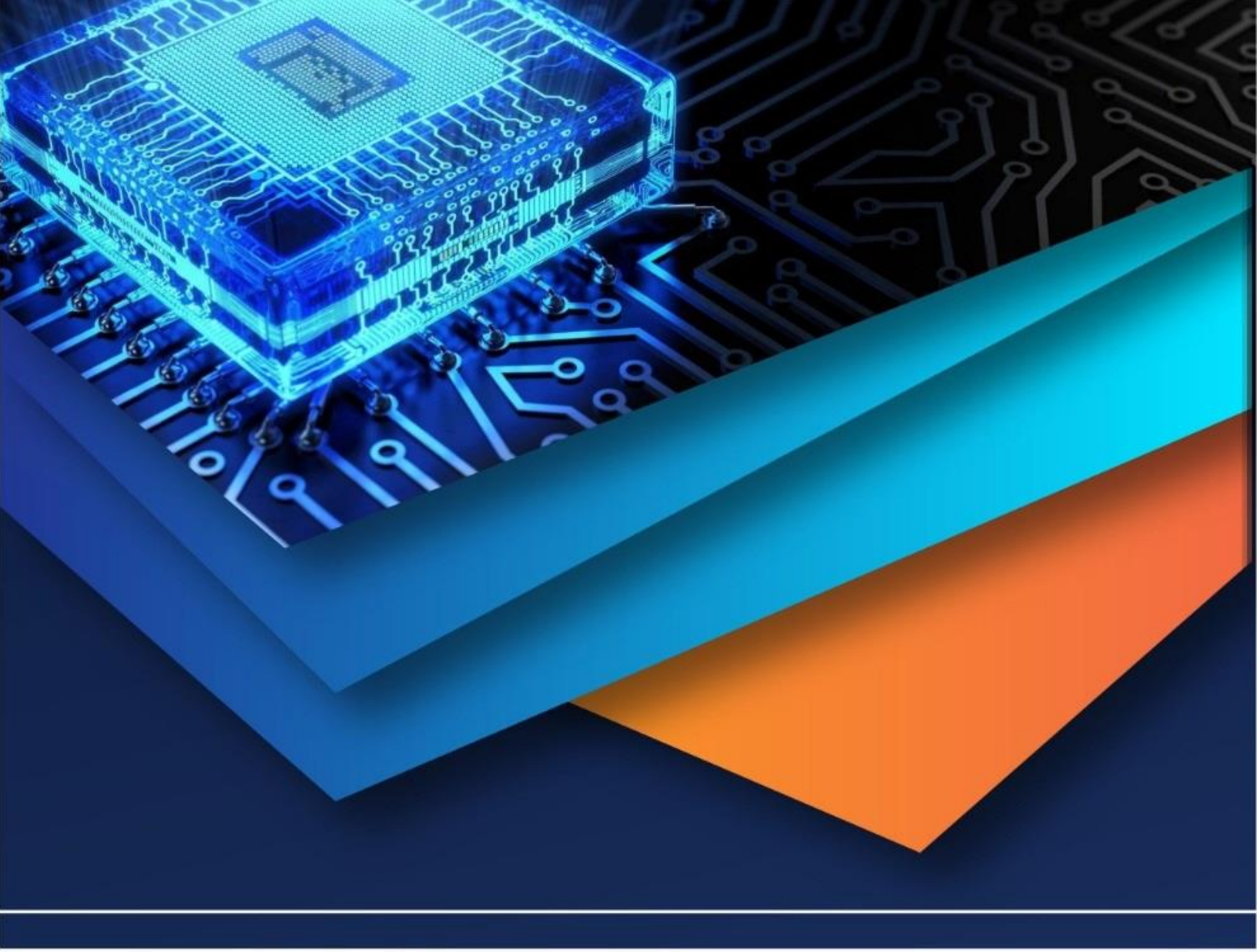
D. Common Network Protocols and Port Numbers

Figure 5.4: Common Network Protocols and Port Numbers

REFERENCES

[1] Oluwaseun Prisci la Olawale, Sahar Ebadinezhad. Cybersecurity Anomaly Detection: AI and Ethereum Blockchain for a Secure and Tamperproof IoHT Data Management, IEEE Access, 2024.
[2] Ahmad Rezaei, Linda D. Mason. Secure Key Management for Military IoT Using Quantum-Resistant Algorithms, IEEE Transactions on Information Forensics and Security, 2023.
[3] Carlos Mendes, Priya Sharma. End-to-End Encryption Techniques for Tactical IoT Networks in Defense Systems, Elsevier Journal of Network and Computer Applications, 2022.
[4] Tarek Alharbi, S. Krishnaswamy. Lightweight Cryptographic Protocols for Military Sensor Networks, IEEE Internet of Things Journal, 2023.
[5] Jingwei Zhou, Mary O. Kimani. Post-Quantum Cryptography for Secure Military Communications in IoT, Springer Cybersecurity Journal, 2024.
[6] Nour El-Din Mostafa, Rehan Qureshi. Blockchain-Based Access Control for Secure IoT in Defense Infrastructure, IEEE Access, 2022.
[7] Sanjay Yadav, Tania Li. Zero Trust Architecture for Military-Grade IoT Networks, Elsevier Computers & Security, 2023.
[8] E. N. Dlamini, V. Ramesh. AI-Driven Intrusion Detection Systems for Encrypted Military IoT Traffic, IEEE Transactions on Network and Service Management, 2024.
[9] Mahmud Ahmed, Carla Gonzalez. Secure Routing Protocols in IoT-enabled Battlefield Environments, ACM Transactions on Cyber-Physical Systems, 2023.
[10] Tomasz Kowalski, Yeon-Jin Park. Multi-Layer Encryption Framework for Military Surveillance IoT Devices, IEEE Communications Surveys & Tutorials, 2023.

[11] Nikita Singh, Abdul Basit. Elliptic Curve Cryptography for Resource-Constrained Military IoT Devices, Springer Security and Privacy Journal, 2024.
[12] Joon-Ho Lee, Efe Efeoglu. Secure Firmware Updates in Military IoT Using Blockchain Verification, IEEE Internet of Things Magazine, 2023.
[13] Marta Velasquez, Rahul Raj. Fog and Edge Computing Security for Mission-Critical IoT Systems, Elsevier Journal of Systems Architecture, 2022.
[14] Kevin Tang, Alessandra Moretti. Intrusion Prevention in Secure Military IoT Environments, Wiley Security and Privacy, 2023.
[15] Om Prakash, Daniel V. Ngoma. Role of Homomorphic Encryption in Battlefield IoT Data Analytics, IEEE Transactions on Dependable and Secure Computing, 2024.
[16] Shalini Ahuja, Kai Chen. Resilient IoT Communication Protocols for Military Field Operations, Elsevier Ad Hoc Networks, 2023.
[17] Farid Hamza, Naomi Ellis. Trusted Execution Environments for Cybersecurity in Military IoT, Springer Journal of Trust Management in Computing, 2024.
[18] Haruto Saito, Jenna L. Morris. Energy-Efficient Encryption Schemes for Combat Zone IoT Devices, IEEE Embedded Systems Letters, 2023.
[19] Aisha Bello, Thomas Gregson. Attribute-Based Encryption for Tactical Military IoT Applications, ACM Transactions on Privacy and Security, 2022.
[20] Arvind Ramesh, Felicia Zhou. Adaptive Cryptographic Methods for Dynamic Military IoT Networks, IEEE Transactions on Mobile Computing, 2024.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY