International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

Secure Online Tender Document Submission With Bid Evaluation And Audit Monitoring

Marella Shivani, Nalla Rajender Reddy*
Vaagdevi Engineering College, Warangal, 506005, Telangana, India.
*Correspondence: Nalla Rajender Reddy

ABSTRACT

With the rapid growth of digital procurement platforms, organizations increasingly rely on online tendering systems to manage vendor selection, contract bidding, and document exchange. While digital tendering improves accessibility and operational efficiency, it also introduces serious security challenges related to data confidentiality, bid integrity, and unauthorized access. Sensitive bid documents, pricing information, and communication between buyers and sellers are often exposed to risks such as data leakage, tampering, and impersonation when handled through conventional web portals or email-based systems. In traditional tender management systems, bid submissions and documents are usually stored in plain format or protected only by basic login mechanisms. Such systems lack strong encryption, audit trails, and controlled access, making them vulnerable to cyberattacks, insider threats, and disputes regarding bid authenticity. The absence of traceability and real-time monitoring further reduces trust among participants and weakens the transparency of the procurement process. To overcome these limitations, this research integrates a web-based platform built using Flask with a Camellia with Advanced Encryption Standard (AES) Cryptographic framework to protect all sensitive data including bids, documents, and messages. Role-based access control (RBAC) ensures that administrators, buyers, and sellers can only perform authorized operations. Encrypted storage and secure file handling prevent unauthorized viewing or modification of tender data, an audit logging mechanism records every critical action, providing traceability and accountability throughout the tender lifecycle. The significance of this system lies in its ability to combine security, transparency, and usability within a single platform. By ensuring encrypted data handling, controlled access, and comprehensive audit monitoring, the proposed system enhances trust between all stakeholders and provides a reliable foundation for modern digital procurement and e-tendering environments.

Keywords: Electronic Tender Management, Camellia Encryption, Advanced Encryption Standard (AES), Role-Based Access Control (RBAC), Secure Document Management, Digital Procurement

1. INTRODUCTION

Public procurement is a fundamental process through which government organizations and public authorities acquire goods, services, and infrastructure projects from qualified suppliers in a transparent and competitive manner. It plays a vital role in ensuring that public funds are utilized efficiently while maintaining fairness, accountability, and competition throughout the procurement process. The primary objective of public procurement is to identify and select the most suitable contractor capable of delivering the required products or services according to predefined technical, financial, and quality requirements. Public procurement frameworks also establish standardized procedures that provide equal opportunities for bidders and promote transparency during contract awarding, thereby supporting economic growth and improving public service delivery [1].

The effectiveness of public procurement largely depends on the proper implementation of tendering procedures and the competency of the stakeholders involved in preparing,

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

evaluating, and awarding contracts [2]. Procurement activities are widely employed across sectors such as transportation, healthcare, education, energy, and construction, where governments undertake projects including roads, bridges, airports, public buildings, and utility infrastructure [3]. However, conventional tendering methods often rely on manual documentation and paper-based workflows, making the procurement process slow, labor-intensive, and susceptible to administrative errors, delays, and corruption. To address these limitations, many organizations have adopted electronic procurement and electronic tendering systems that automate tender publication, bid submission, evaluation, and contract management through digital platforms.

Fig. 1: Online tender document submission

Electronic tendering offers numerous advantages over traditional procurement methods by reducing operational costs, shortening procurement cycles, simplifying documentation, improving stakeholder communication, and increasing the competitiveness of submitted proposals [4]. Digital procurement platforms also enhance transparency, auditability, and decision-making through centralized data management and automated workflows, thereby minimizing opportunities for fraudulent activities. Despite these advantages, the adoption of electronic tendering continues to face challenges such as cybersecurity threats, protection of sensitive bidding information, limited technical awareness among stakeholders, and organizational barriers that affect user acceptance. Addressing these issues through secure digital infrastructures, robust access control mechanisms, and effective stakeholder training is essential for developing reliable, transparent, and efficient public procurement systems capable of supporting future digital governance initiatives [5].

1.1 Research Motivation

In real-world organizations such as construction companies, IT firms, manufacturing industries, and public sector agencies, tender platforms are the primary means of selecting vendors and awarding contracts. These organizations exchange large volumes of cost estimates, design documents, legal agreements, and technical proposals through digital systems. Data analysis is required to evaluate vendor reliability, pricing trends, and historical bidding behavior. Insecure or poorly managed platforms increase the risk of fraud, data leaks, and biased evaluations, which can lead to financial losses and legal disputes. As procurement operations grow in scale and complexity, organizations need reliable digital systems that can manage data securely while supporting effective analysis and decision-making.

2. LITERATURE SURVEY

Srishti Dubey et al. [6] addressed issues in government tender allocation by providing a decentralized, secure, and transparent blockchain-based platform for procurement. Their proposed architecture enables trustless and anonymous interactions while ensuring openness and accessibility for all participants. The system improves the efficiency of public procurement by modifying the decision-making parameters within the tender allocation process. Martin Betts et al. [7] identified the major security and legal challenges involved in designing electronic tendering systems. They proposed a new e-tendering architecture based on distributed trusted third parties, making it suitable for secure, large-scale operations such

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

as those in the construction industry. David Kohout et al. [8] addressed cybersecurity challenges in smart metering infrastructure, focusing on compliance with the Czech Decree 359/2020 and the DLMS security suite. They introduced a comprehensive testing methodology to verify cybersecurity requirements, evaluate smart meter security parameters, and assess wireless communication technologies against European regulatory standards. Dan Wang et al. [9] proposed a decentralized electronic bidding system based on blockchain and smart contracts. Their system replaces traditional databases with blockchain and employs chaincode for business logic execution. To strengthen privacy, cryptographic techniques such as graph isomorphism-based zero-knowledge proofs are incorporated, improving participant anonymity, secure data transmission, traceability, and verifiability.

Li Li et al. [10] proposed SecTEP, a secure tender evaluation method for blockchain-based procurement systems. The framework considers both bid prices and supplier quality while preserving the confidentiality of bidding and evaluation results. It utilizes advanced cryptographic techniques to perform encrypted bid validation, bid comparison, quality score aggregation, and winner declaration. Jaydeep Howlader et al. [11] introduced a secure receipt-free sealed-bid electronic auction protocol that prevents bid-rigging through coercion. Their approach eliminates receipt generation, ensuring bidders cannot prove their submitted bids to coercers, thereby preserving bid secrecy and strengthening auction security. Qusef et al. [12] proposed a fully automated web-based e-tendering model that digitizes every stage of the tendering process. The conceptual framework integrates all related departmental systems and stakeholders, enabling efficient, paperless, and automated procurement operations. Abikoye et al. [13] presented an enhanced Advanced Encryption Standard (AES) algorithm by modifying the SubBytes and ShiftRows transformations. The SubBytes operation was made round key-dependent, while ShiftRows was randomized, significantly increasing diffusion and making the encryption process more resistant to cryptographic attacks. Piyush Kumar Shukla et al. [14] evaluated the security efficiency of white-box implementations of AES and DES encryption algorithms. Their work examined both practical implementation techniques and their theoretical foundations while performing cryptanalysis to assess the robustness of white-box cryptography for secure digital signature verification.

3. PROPOSED SYSTEM

The proposed Secure Online Tender Document Submission System is implemented as a Flask-based web application with a structured front-end and a secure back-end architecture. The front end is developed using HTML, CSS, Bootstrap, providing separate login portals for administrators, buyers, and sellers. Role-based authentication is enforced at the server side using Flask session management, ensuring that users can access only the functions permitted to their role. The back end is developed in Python using the Flask framework and uses TinyDB as the database to store user accounts, tender details, bids, documents, and audit logs. All sensitive information such as bids, proposals, messages, and uploaded files is protected using Camellia-based symmetric encryption, which is implemented through a AES block-cipher encryption module operating in CBC mode with 256-bit keys as shown in Fig. 2. Before storing any bid or document, the data is encrypted to ensure confidentiality and prevent unauthorized access. Secure key generation and management are used to control access to encrypted data. The system also includes an audit logging mechanism that records every important user activity such as login, upload, bid submission, and file download. By combining a web-based interface with

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

cryptographic protection and secure database storage, the system provides a controlled and reliable environment for digital tender management.

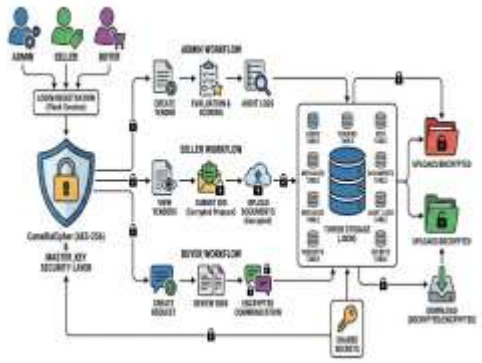

Fig. 2: Proposed system architecture for secure online tender document submission with bid evaluation.

User Login and Authentication: Admin, Seller, and Buyer log in through the web interface. Flask session management verifies credentials and assigns role-based access.

Security and Encryption Layer: All sensitive data such as bids, documents, and messages pass through the CamelliaCipher security layer, where encryption is applied before storage or transmission.

Tender and Request Management: Administrators create tenders and buyers submit procurement requests. These details are stored securely in the TinyDB database.

Bid Submission and Document Upload: Sellers view active tenders, submit encrypted bid proposals, and upload encrypted supporting documents.

Encrypted Data Storage: All encrypted bids, documents, messages, and user records are stored in TinyDB and protected file directories.

Bid Review and Communication: Buyers review submitted bids and communicate with sellers using encrypted messages through the system.

Evaluation, Audit, and Download: Administrators evaluate and score bids, audit logs are maintained for all actions, and authorized users can download encrypted or decrypted documents.

3.1 Camellia Encryption

Camellia encryption is used to convert sensitive data into a secure and unreadable format before it is stored or transmitted. The Camellia layer controls how encryption keys are managed and how data is prepared for cryptographic processing. AES-256 operates as the core block cipher that performs the actual encryption of data blocks. This combination provides strong protection for files, messages, and records. The encryption process ensures that original information cannot be understood without the secret key. By applying this encryption before storage, the system prevents unauthorized access and data exposure.

Input Data Collection: Fig. 3 states that the encryption module receives raw data such as text or files from the application. This data is converted into a binary format suitable for encryption.

Key Generation and Setup: A secure 256-bit secret key is generated and loaded into the Camellia control layer. This key determines how the AES engine will encrypt the data.

Data Preparation: The input data is divided into fixed-size blocks and padded to meet the AES block size requirement. This ensures that all data can be processed correctly by the cipher.

Camellia Control Layer Processing: The Camellia layer applies encryption rules and passes the prepared data and key to the AES-256 engine. It controls the encryption workflow and security parameters.

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

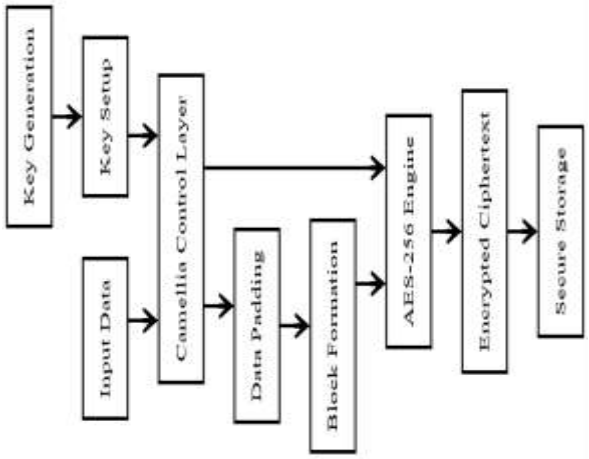

Fig. 3: Internal Workflow of Camellia Encryption

AES-256 Encryption: The AES-256 algorithm encrypts the prepared data blocks using the secret key. The original data is transformed into unreadable ciphertext.

Encrypted Data Output: The generated ciphertext is produced as the final encrypted output. This encrypted data is then ready to be stored or transmitted securely.

3.2 Camellia Decryption

Camellia decryption is used to convert encrypted tender data back into its original readable form for authorized users. The Camellia control layer manages how decryption keys are applied and how encrypted data is processed. AES-256 acts as the core block cipher that performs the actual decryption of the ciphertext. This ensures that only users with the correct secret key can recover the original information. The decryption process restores documents, bids, and messages without altering their content. This mechanism guarantees both confidentiality and controlled access to protected data.

Encrypted Data Input: Fig. 4 shows the decryption module receives encrypted ciphertext from storage or transmission. This ciphertext is prepared for cryptographic processing.

Key Retrieval and Setup: The secret 256-bit encryption key is retrieved and loaded into the Camellia control layer. This key is required to unlock the encrypted data.

Camellia Control Layer Processing: The Camellia layer verifies the key and controls the decryption flow. It passes the encrypted data to the AES-256 engine for decoding.

AES-256 Decryption: The AES engine decrypts the ciphertext using the secret key. This converts the unreadable encrypted data back into padded original data.

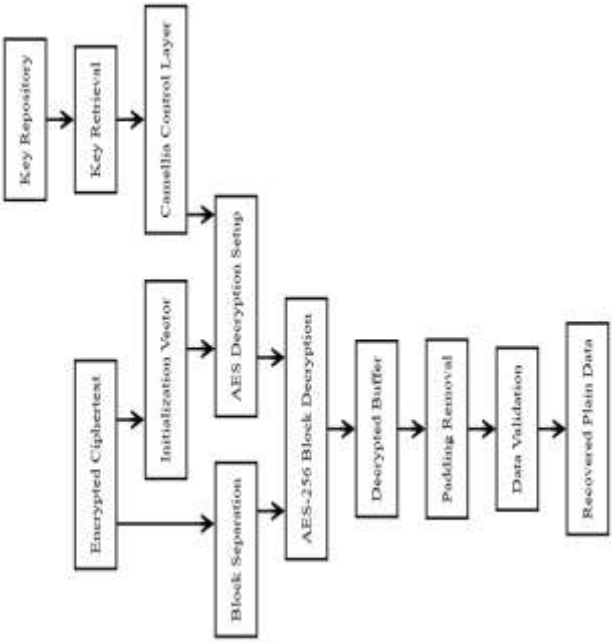

Fig. 4: Internal Workflow of Camellia Decryption

Data Reconstruction: Padding is removed and the original data blocks are reassembled. This restores the data to its original readable format.

Output of Plain Data: The recovered plaintext is delivered to the application. This data can now be used, viewed, or downloaded by authorized users.

9.4 Results Description

Fig. 5 depicts the User Management screen in the Admin panel, which enables administrators to monitor and manage registered users within the system. It provides a consolidated view of administrators, sellers, and buyers along with their associated details. The screen supports administrative oversight by allowing user status monitoring and role verification. It

Received: 30-05-2026 | Accepted: 01-07-2026 | Published: 08-07-2026

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

ensures accountability by maintaining a clear record of active participants in the tender system. This functionality is essential for maintaining controlled access and system integrity.

Fig. 6 illustrates the Creating Tender screen, which allows administrators to publish new tenders into the system. The screen captures critical tender information such as title, description, budget, deadline, and requirements. This functionality enables structured tender creation to ensure clarity and consistency for sellers and buyers. Once created, tenders become available for bid submission and monitoring. The screen plays a central role in initiating the secure tender lifecycle.

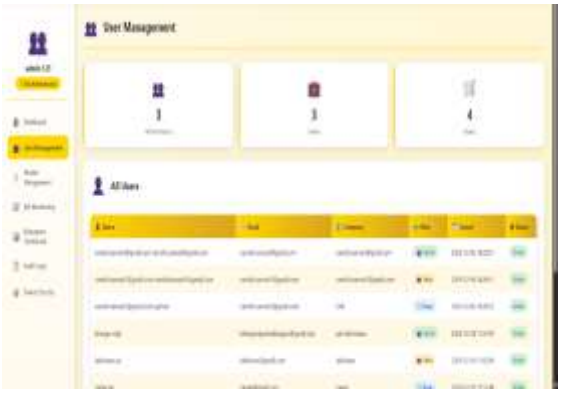

Fig. 5: User Management in Admin Panel Screen

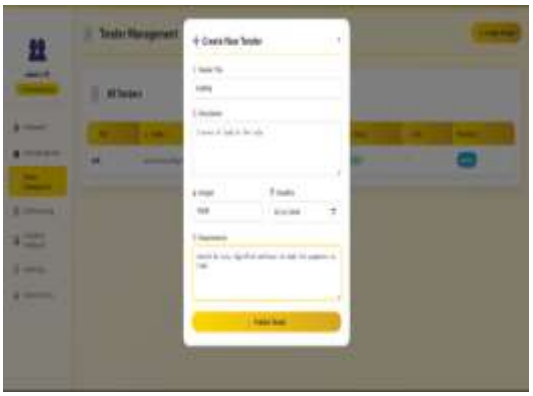

Fig. 6: Creating Tender Screen

Fig. 7 depicts the Bid Monitoring screen, which allows administrators to track all submitted bids for active tenders. It provides visibility into bid status, submission details, associated documents, and review progress. This screen supports evaluation workflows by enabling administrators to monitor pending and approved bids. It ensures transparency by maintaining a clear overview of bidding activity. The bid monitoring interface is essential for secure evaluation and audit-based decision-making.

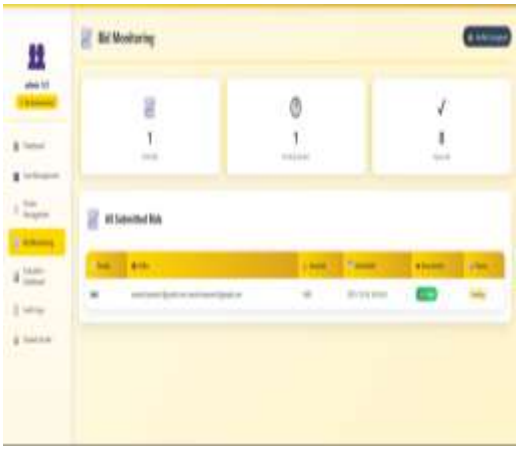

Fig. 7: Bid Monitoring Screen

Fig. 8 illustrates the Audit Logs screen of the Secure Tender System, which provides a comprehensive record of all critical activities performed within the platform. It captures actions such as user registration, login, tender creation, bid evaluation, and status updates along with timestamps and user roles. This screen supports transparency by enabling administrators to trace every operation carried out in the system. The audit mechanism helps detect unauthorized actions and ensures accountability among users. It plays a vital role in maintaining trust and integrity throughout the tendering process.

Fig. 8: Audit Logs Screen

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

Fig. 9 illustrates the Creating Tender Request screen, which allows buyers to initiate new procurement requests within the system. It captures essential details such as request title, description, estimated budget, deadline, category, and specific requirements. This screen ensures that buyer requirements are formally defined and recorded before tender publication. The structured request creation process supports clarity and consistency for sellers reviewing the tender. It represents the starting point of the buyer-driven tender workflow.

Fig. 9: Creating Tender Request Screen

Fig. 10 depicts the Reviewing the Bids screen, which enables buyers to examine and compare bids submitted by sellers for published tenders. It presents bid-related information such as seller details, bid amount, proposed timeline, evaluation score, and document availability. This screen supports informed comparison and selection of vendors based on defined criteria. It ensures transparency by displaying bid status and review outcomes. The interface plays a crucial role in the decision-making phase of procurement.

Fig. 10: Reviewing the Bids Screen

5. CONCLUSION

The Secure Online Tender Document Submission with Bid Evaluation and Audit Monitoring system successfully provides a reliable, transparent, and secure platform for handling digital tenders. By integrating Flask with Camellia with AES encryption and TinyDB storage, the system ensures that all bids, documents, and communications remain confidential and tamper-resistant. Role-based access control allows administrators, buyers, and sellers to operate within clearly defined permissions, reducing the risk of unauthorized actions. The inclusion of encrypted file storage and secure messaging significantly improves data protection compared to traditional manual or email-based tendering. Audit logging enhances accountability by tracking every critical operation performed within the system. Performance is improved through lightweight backend processing, fast AES-based encryption, and efficient JSON-based data retrieval, enabling quick bid submission, document handling, and evaluation.

REFERENCES

[1] Cook, M. Practical Guide to Public Procurement; Oxford University Press: Oxford, UK, 2015.

[2] Obolewicz, J. Zarządzanie bezpieczeństwem pracy w budownictwie (Occupational safety management in the construction industry). Przedsiębiorczość Zarządzanie **2014**, 15, 441–451.

[3] Ujdak-Dyńka, B. Zamówienia publiczne jako instrument optymalizacji wydatków publicznych (Public procurement as an instrument for optimisation of public expenditure). In Efektywność Zarządzania Zasobami Organizacyjnymi; Lenik, P., Ed.; Prace Naukowo-Dydaktyczne Państwowej Wyższej Szkoły Zawodowej im; Stanisława Pigonia: Krosno, Poland, 2015; Volume 68, pp. 257–275.

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

[4] Arslan, G.; Tuncan, M.; Birgonul, M.T.; Dikmen, I. E-Bidding Proposal Preparation System for Construction Projects. Build. Environ. 2006, 41, 1406–1413.

[5] Abdullahi, B.; Ibrahim, Y.M.; Ibrahim, A.; Bala, K. Development of E-Tendering Evaluation System for Nigerian Public Sector. J. Eng. Des. Technol. 2019, 18, 122–149.

[6] Dubey, Srishti & Singh, Priyanka & Verma, Rohan & Kamboj, Deepika. (2023). Government Tender Allocation Using Blockchain Technology. 1-6. 10.1109/ICICAT57735.2023.10263653.

[7] Betts, Martin & Black, Peter & Christensen, Sharon & Dawson, Ed & Du, Rong & Duncan, William & Foo, Ernest & Nieto, Juan. (2006). Towards secure and legal E-tendering. 11.

[8] Kohout, D.; Lieskovan, T.; Mlynek, P. Smart Metering Cybersecurity—Requirements, Methodology, and Testing. Sensors **2023**, 23, 4043. https://doi.org/10.3390/s23084043

[9] Wang, Dan & Zhao, Jindong & Mu, Chunxiao. (2021). Research on Blockchain-Based E-Bidding System. Applied Sciences. 11. 4011. 10.3390/app11094011.

[10] Li Li, Jiayong Liu, Peng Jia, SecTEP: Enabling secure tender evaluation with sealed prices and quality evaluation in procurement bidding systems over blockchain, Computers & Security, Volume 103, 2021, 102188, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2021.102188.

[11] Howlader, Jaydeep & Ghosh, Anushma & Pal, Tandra. (2009). Secure Receipt-Free Sealed-Bid Electronic Auction. Communications in Computer and Information Science. 40. 228-239. 10.1007/978-3-642-03547-0_22.

[12] Qusef, Abdallah & Sammour, George & Albadarneh, Aalaa. (2019). A New e-Tendering Model For Fully Automated Tendering Process. 193-201. 10.1109/ACIT47987.2019.8991136.

[13] Abikoye, O.C.; Haruna, A.D.; Abubakar, A.; Akande, N.O.; Asani, E.O. Modified Advanced Encryption Standard Algorithm for Information Security. Symmetry 2019, 11, 1484. https://doi.org/10.3390/sym11121484

[14] Shukla, P.K.; Aljaedi, A.; Pareek, P.K.; Alharbi, A.R.; Jamal, S.S. AES Based White Box Cryptography in Digital Signature Verification. Sensors 2022, 22, 9444. https://doi.org/10.3390/s22239444