

## Secure Digital Court Hearing Scheduler Supporting Role Based Access and Case Update

Ursula Nithin, G. Arpitha\*

Vaagdevi Engineering College, Warangal, 506005, Telangana, India.

\*Correspondence: G. Arpitha

### ABSTRACT

The rapid growth in legal cases and the increasing workload of judicial institutions have created a significant demand for efficient, secure, and centralized digital court management systems. Many courts continue to rely on manual record-keeping, paper-based documentation, email communication, and disconnected software tools to manage case records, hearing schedules, and legal correspondence. These conventional approaches often result in scheduling conflicts, misplaced documents, delayed communication, limited transparency, and inefficient coordination among courts, lawyers, and clients. Furthermore, sensitive legal documents are frequently stored or transmitted without adequate security mechanisms, making them vulnerable to unauthorized access, data tampering, and confidentiality breaches. These challenges highlight the need for a secure and integrated digital solution for modern judicial administration. The proposed Digital Court Hearing Scheduling Platform provides a centralized web-based system developed using Flask with TinyDB for structured data management. The platform implements Role-Based Access Control (RBAC) to provide

courts, lawyers, and clients with secure, role-specific access to case records, hearing schedules, and legal documents. To protect confidential information, legal documents and messages are encrypted using the Affine Cipher before storage and sharing, ensuring secure communication and controlled access. The system also supports hearing scheduling, appointment management, secure file sharing, and real-time coordination through a unified interface. The proposed platform improves judicial efficiency by reducing manual workload, strengthening document security, enhancing transparency, minimizing scheduling conflicts, and enabling faster case management, thereby providing a reliable, scalable, and secure digital solution for modern court administration.

**Key words:** Digital Court Management, Court Hearing Scheduling, Role-Based Access Control, Secure Document Management, Judicial Information Systems, Flask Framework, Legal Case Management

### 1. INTRODUCTION

Electronic government (e-government) initiatives have grown considerably in the past two decades. These projects help governments deliver information and communication

technology (ICT)-based information and services. It gives residents, businesses, and the government additional chances to provide better services [1]. ICTs in public administration also help modernize governance and have huge administrative possibilities. This could improve government relationships with communities, businesses, and workers through decentralization, openness, and internal/external responsibility [3,4]. Many sorts of e-government programs are utilized globally in healthcare, education, and transportation. When the judicial system (JS) uses ICTs to improve its efficacy and efficiency, it can ease communication among JS parties (ministry, courts, and prisons) and help improve access to justice and the efficiency of legal proceedings [2]. E-court itself is a set of hardware, software, and networking solutions for the JS to aid court personnel and judges enhance case filing, hearing scheduling, and efficiency. Daily responsibilities include workflow, filing, and hearing scheduling.



Fig. 1: Court Hearing Scheduling

This research project refers to courtroom and client-courtroom technology as e-court. E-

court refers to courtroom technology used globally. According to research on court management, there are two types of court technologies: those used in the courtroom and those used to improve court, party, and public communication [3]. This category covers automated registers, case management systems, and financial management systems. First, we have court administration software that helps administrative staff and/or judges (such as jurisprudence databases and sentencing support systems). Second, we have apps that let parties share data and communicate (such as e-filing and provision through court websites). A legal system case registry is automated and helps improve court cases and data access [4]. ICT helps implement the JS's administrative theory and improve judicial efficiency. Despite significant investments, technical progress is questionable. Multiple studies find it to be inconsistent in terms of value for money. Previously, court management specialists decided to explore the relationship between technology and individual and organizational performance, mostly using descriptive research [5]

## 2. LITERATURE SURVEY

Romdoni M., et al. [6] proposed a research model to evaluate the success factors influencing the implementation of digital case management systems within the courts of Greater Jakarta. The study employed Structural Equation Modeling (SEM) to

analyse survey responses collected from legal professionals using the system. The proposed framework examined the impact of system quality, information quality, and service quality on overall user satisfaction and system effectiveness. Experimental results demonstrated that reliable information management, efficient system performance, and high-quality digital services significantly improve the adoption and operational success of electronic case management systems. The findings provide valuable theoretical and practical guidance for enhancing digital judicial platforms. Yunliang Li, et al. [7] proposed an advanced Role-Based Access Control (RBAC) model that separated user permissions into abstract roles and specific operational roles to improve access management in distributed environments. The proposed framework supported repeated role names, platform-domain isolation, inter-domain isolation, and fine-grained cross-domain resource sharing while maintaining secure authorization mechanisms. By introducing flexible role management and domain separation, the model strengthened access control, improved scalability, and enabled secure information sharing across multiple organizational domains. Zlatan Morić, et al. [8] introduced an Artificial Intelligence-based legal decision support framework that dynamically updated case outcome probabilities using Bayesian inference techniques. The proposed system integrated Conditional Probability Tables

(CPTs) with historical judicial records to continuously refine legal predictions as new evidence became available during court proceedings. This adaptive approach improved the interpretability of AI-generated recommendations, assisted legal professionals in evaluating case progress, and enhanced evidence-based judicial decision-making.

Tapasi Bhattacharjee, et al. [9] proposed JudicBlock, a blockchain-based Electronic Law Record (ELR) management system designed to improve the efficiency and security of judicial document storage. The proposed architecture integrated blockchain with the InterPlanetary File System (IPFS) to provide secure, decentralized storage and rapid retrieval of legal records. Experimental evaluation demonstrated improvements in mining cost, transaction processing capacity, query response time, block processing throughput, and document uploading latency compared to conventional electronic record management systems. The decentralized framework enhanced data integrity, reduced storage overhead, and provided tamper-resistant management of judicial records. Bing-Chang Chen, et al. [10] proposed a secure authentication mechanism for Mobile Radio Frequency Identification (RFID) systems using authenticated delegation techniques. The framework enabled RFID readers to obtain role-specific permissions through a backend database while performing mutual authentication with both the database server and RFID tags. This authentication

process protected sensitive information, limited unauthorized access attempts, and strengthened user privacy by enforcing controlled access to RFID resources. Jubaer, et al. [11] investigated the implementation of electronic court (e-court) systems, digital case management platforms, and online legal services to evaluate their impact on judicial efficiency, transparency, and accessibility. Using comparative case studies, policy analysis, and stakeholder interviews, the study examined technological, organizational, and regulatory challenges affecting digital court adoption while identifying best practices for successful implementation. The findings demonstrated that integrated digital judicial platforms significantly improve case management efficiency, public access to justice, and transparency throughout legal proceedings.

Hammi, et al. [12] proposed a blockchain-based verification framework that enabled almost instantaneous authentication of digital records after their storage on the blockchain network. The proposed approach eliminated conventional bilateral verification procedures between participating agencies by providing a decentralized and tamper-resistant verification mechanism. The implementation improved operational efficiency, strengthened trust among participating organizations, and reduced the complexity associated with traditional document validation processes. Jawad Ahmad, et al. [13] proposed a secure image encryption scheme that combined

random chaotic sequences with Affine Transformation to strengthen the protection of digital images. The proposed encryption process first removed the correlation among neighboring image pixels through simple XOR and addition operations before applying Affine Transformation to generate the final encrypted image. Comprehensive security evaluation using histogram analysis, entropy, correlation analysis, Peak Signal-to-Noise Ratio (PSNR), key sensitivity, key space analysis, and differential attack resistance demonstrated that the proposed encryption scheme provides strong confidentiality and robust protection against various cryptographic attacks, making it suitable for securing sensitive digital documents and judicial records.

### 3. PROPOSED SYSTEM

This research as shown in Fig. 2 is implemented as a web-based digital court management platform using the Flask framework to handle routing, user sessions, and role-based access control. The system uses TinyDB as a lightweight NoSQL database to store user profiles, case records, hearing schedules, encrypted file metadata, messages, and appointment information. For data security, the system employs affine encryption to protect all uploaded legal documents and confidential communication messages before they are stored on the server. The affine cipher applies a mathematical transformation on each byte of data to convert readable content into encrypted format. Encrypted files are stored in



**Data Preparation:** Fig. 3 the original message or file is converted into a sequence of byte values so that mathematical operations can be applied.

**Key Parameter Application:** Two fixed numerical parameters are applied to control how each byte is transformed during encryption.

**Mathematical Transformation:** Each byte is multiplied by the first parameter and increased by the second parameter to produce an encrypted value.

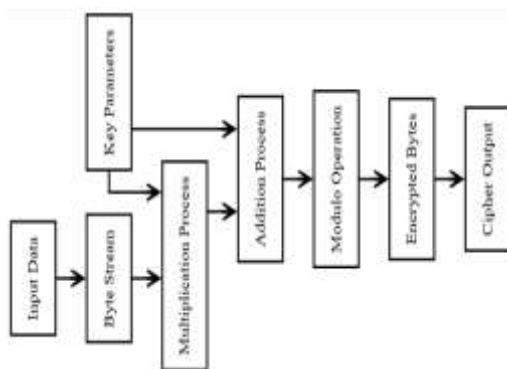


Fig. 3: Internal Workflow of Affine Encryption

**Modular Reduction:** The transformed value is reduced using modulo 256 to ensure it remains within the valid byte range.

**Encrypted Output Formation:** All encrypted byte values are combined to generate the final encrypted data used for secure storage or transmission.

### 3.2 Affine Decryption

Affine decryption is the reverse process used to recover original data from affine-encrypted

content. The encrypted data is processed as a sequence of numerical byte values. The same two numerical parameters used during encryption are applied in reverse using modular arithmetic. The decryption process first subtracts the additive parameter and then multiplies the result by the modular inverse of the multiplicative parameter. This restores each encrypted byte to its original value. The recovered byte stream is then converted back into its original readable form. This allows encrypted legal documents and messages to be correctly reconstructed for authorized users.

**Encrypted Data Reception:** Fig. 4 help in encrypting file or message is first received as a sequence of encrypted byte values. Each byte represents data that has already been transformed by affine encryption.

**Byte Stream Preparation:** The encrypted content is converted into a numerical byte stream so that mathematical operations can be applied to each value individually.

**Determination of Inverse Parameter:** The multiplicative key used during encryption has a corresponding modular inverse. This inverse is calculated to enable reversal of the multiplication applied during encryption.

**Offset Removal:** For each encrypted byte, the additive key is subtracted to eliminate the constant offset that was added during the encryption stage.

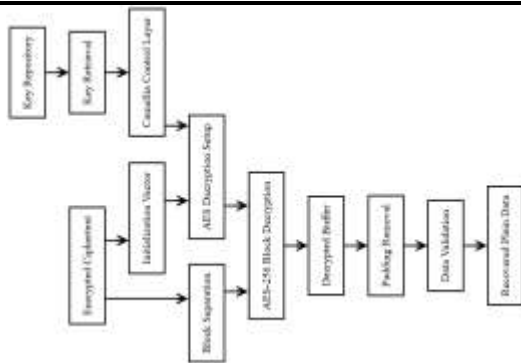


Fig. 4: Internal Workflow of Affine Decryption

**Reverse Linear Transformation:** After offset removal, each byte is multiplied by the modular inverse of the multiplicative key. This reverses the linear transformation applied during encryption.

**Modular Normalization:** The result is reduced using modulo 256 to ensure that the recovered byte value stays within the valid byte range.

**Byte Reconstruction:** All recovered byte values are combined in their original order to form a continuous stream of data.

**Original Data Formation:** The reconstructed byte stream is converted back into its original format, restoring the original document or message.

#### 4. RESULTS AND DISCUSSION

Fig. 5 depicts the case creation and management interface used to formally register and organize judicial cases within the system. The screen facilitates structured entry of case-related details, including case type, involved parties, and assigned legal

representatives. It supports systematic case tracking throughout the judicial lifecycle. The interface ensures consistency, traceability, and controlled access to case data. This module plays a critical role in maintaining accurate and auditable court records.



Fig. 5: Creating Cases Screen

Fig. 6 illustrates the hearing scheduling interface that enables courts to plan and manage judicial hearings efficiently. The screen allows association of hearings with registered cases while capturing essential scheduling parameters such as date, time, and judicial authority. It supports organized coordination between courts, lawyers, and clients. The interface ensures that hearing information is recorded securely and remains accessible to authorized users only. This functionality enhances transparency and procedural efficiency in judicial proceedings.



Fig. 6: Scheduling Hearings Screen

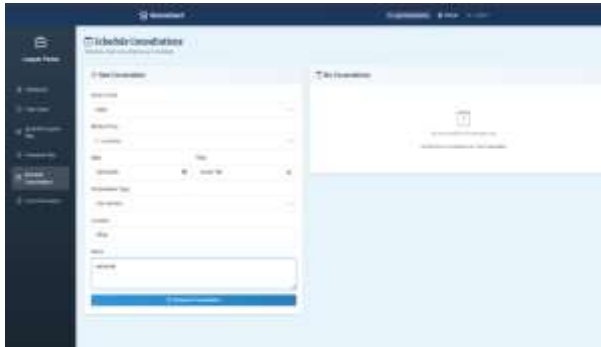


Fig. 7: Scheduling Consultations Screen

Fig. 7 illustrates the consultation scheduling interface that facilitates structured communication between lawyers and clients. The screen enables planning of consultations by capturing essential details such as related cases, time, and consultation type. It supports systematic coordination of legal discussions outside formal court hearings. The module ensures organized scheduling while maintaining secure access controls. This feature enhances client engagement and legal service efficiency.

Fig. 8 depicts the hearing dates screen that provides clients with a structured view of scheduled court hearings related to their cases. The screen enables tracking of hearing timelines and related case information. It supports timely awareness of judicial proceedings to ensure preparedness. The interface ensures that hearing details are securely accessible only to authorized users. This module improves communication and reduces uncertainty in court scheduling.



Fig. 8: Hearing Dates Screen

## 5. CONCLUSION

This research successfully demonstrates how web-based automation combined with encryption and role-based access control can significantly improve the efficiency and security of judicial operations. By integrating Flask with TinyDB and affine encryption, the system enables secure management of cases, hearings, legal documents, and communication between courts, lawyers, and clients. Compared to traditional manual and email-based systems, the platform reduces scheduling conflicts, minimizes document handling delays, and prevents unauthorized access to sensitive legal records. Encrypted file storage and controlled decryption ensure that confidential documents remain protected throughout their lifecycle. The use of centralized digital records improves retrieval speed, reduces data duplication, and enhances consistency across all court activities. Overall, the system achieves improved performance in terms of data security, scheduling accuracy, and operational transparency.

## REFERENCES

- [1] Bernroider, E.W.N.; Koch, S.; Stix, V. A comprehensive framework approach using content, context, process views to combine methods from operations research for IT assessments. *Inf. Syst. Manag.* 2013, 30, 75–88.
- [2] Yildiz, M. E-government research: Reviewing the literature, limitations, and ways forward. *Gov. Inf. Q.* 2017, 24, 646–665.
- [3] Currie, W.; Guah, M.W. IT-enabled healthcare delivery: The U.K. National Health Service. *Inf. Syst. Manag.* 2006, 23, 7–22.
- [4] Lussak, A.; Abdurachman, E.; So, I.G.; Setiowati, R. The effect of operational improvement on business survival with moderating role of continuous improvement (Case study: Food and beverage small business in Bali). *Int. J. Sci. Tech. Res.* 2019, 8, 617–621.
- [5] Commission of the European Communities. Towards a European E-Justice Strategy; The European Parliament and the European Economic and Social Committee: Brussels, Belgium, 2018.
- [6] Romdoni, M.; Lussak, A.; Darmawan, I. Success Factors for Using E-Court in Indonesian Courts. *Proceedings 2022*, 82, 58.  
<https://doi.org/10.3390/proceedings2022082058>
- [7] Li, Y.; Du, Z.; Fu, Y.; Liu, L. Role-Based Access Control Model for Inter-System Cross-Domain in Multi-Domain Environment. *Appl. Sci.* 2022, 12, 13036.  
<https://doi.org/10.3390/app122413036>
- [8] Morić, Z.; Dakić, V.; Urošev, S. An AI-Based Decision Support System Utilizing Bayesian Networks for Judicial Decision-Making. *Systems* 2025, 13, 131.  
<https://doi.org/10.3390/systems13020131>
- [9] Bhattacharjee, T.; Mahapatra, A.S.; De, D.; Chowdhury, A. JudicBlock: Judicial Evidence Preservation Scheme Based on Blockchain Technology. *Blockchains* 2025, 3, 11.  
<https://doi.org/10.3390/blockchains3040011>
- [10] Chen, B.-C.; Yang, C.-T.; Yeh, H.-T.; Lin, C.-C. Mutual Authentication Protocol for Role-Based Access Control Using Mobile RFID. *Appl. Sci.* 2016, 6, 215.  
<https://doi.org/10.3390/app6080215>
- [11] jubaer, shah. (2025). Digital Transformation in the Justice System: E-Courts, Case Management, and Legal Accessibility.  
<https://doi.org/10.5281/ZENODO.17127616>

- 
- [12] Hammi, B.; Zeadally, S.; Adja, Y.C.E.; Giudice, M.D.; Nebhen, J. Blockchain-Based Solution for Detecting and Preventing Fake Check Scams. *IEEE Trans. Eng. Manag.* 2022, 69, 3710–3725.
- [13] Ahmad, J., Hwang, S.O. A secure image encryption scheme based on chaotic maps and affine transformation. *Multimed Tools Appl* 75, 13951–13976 (2016).  
<https://doi.org/10.1007/s11042-015-2973-y>