MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 674-682

LAWFORT AI: A SECURE DIGITAL GOVERNANCE AND MANAGEMENT PLATFORM FOR LEGAL AND CYBER CRIME SERVICES

Nithiyasree KC[1] Dr.N.Palanivel[2], Kavi Amudan S[3], J Sanjay V[4], Pavithran E[5], Sharan Kumar K[6]
[1]Asst. Professor, [2]Professor,[3,4,5,6] UG Scholar, Dept. of CSE (IoT and Cybersecurity including Block chain Technology), Manakula Vinayagar Institute of Technology, Puducherry, India.
nithyasreekcr@gmail.com | hodcseicb@mvit.edu.in | kaviamudan10@gmail.com | sanjayofficial1302@gmail.com| pavithran2730@gmail.com| sharankumar572005@gmail.com

ABSTRACT
There is an increasing demand for smart, accessible and safe legal aid platforms due to the emergence of new generation of digital governance and growing complexity in cyber laws (Digital Personal Data Protection Act 2025, amended Information Technology Act 2000, directives from CERT-In and Digital India Bill). Although there are static legal information repositories including India Code, eCourts, NyayGuru and police cyber portal, none of them have provided natural language interaction, context based reasoning or adaptive user support for different type of users. Thus LawFort AI aims at bridging this gap by creating a unique AI driven legal and cyber-aided service platform for citizens, law students, lawyers and law enforcement agencies (LEAs). In addition to the advanced NLP models and hybrid semantic retrieval technology, the LawFort AI System has included role-based access control (RBAC) , phishing link detection module and evidence handling/ workflow guidance modules for LEA exclusive use. Therefore it provides operational security as well as accessibility.
The methodology of the LawFort AI System is layered in three levels: Citizen Legal Helper Module, Cybercrime Awareness & Web Safety Module and Law Enforcement Investigation Suite. A series of NLP Pipelines using transformer based architectures allows users to semantically query the system. The Lawfort AI System uses a Hybrid Decision Engine with Fuzzy Search, Rule Based Logic, and Embeddings to enhance the systems overall accuracy. The Lawfort AI System incorporates a Secure Role-Based Access Control (RBAC) system which restricts access to sensitive law enforcement tools including digital evidence handling procedures, investigation workflow generator, internal legal references, etc. to be used by confirmed Police Personnel only after they have received Admin-issued Credentials. The LawFort AI System was developed in accordance with privacy and security principles consistent with those outlined in DPDP 2025, and CERT-In reporting protocols. LawFort uses audit logging, encrypted request processing, and restricted endpoints to enforce legal use of the system; preclude unauthorized access to or misuse of law enforcement-related tools; and maintain transparency into its use. LawFort's modular and scalable architecture allows it to adapt to emerging cyber laws and feature additions including multilingual support, chat interfaces, offline case documentation, etc.
Overall, the study demonstrates that legal systems that utilize AI can significantly reduce information gaps, enhance public legal literacy, and improve investigative efficiency for law enforcement agencies (LEAs) while maintaining compliance with legal and ethical standards. Furthermore, the findings suggest that hybrid approaches to AI are required that emphasize transparency, accessibility, and security. In conclusion, LawFort represents a unique, practical, and secure solution that bridges the gap between advanced legal technology solutions and India's evolving cyber law ecosystem.
Keywords : AI Legal Assistant, Cyber Law, Digital Forensics, Legal NLP, Role-Based Access Control, Secure Web Systems.

1. INTRODUCTION

Traditional Legal Support platforms are fragmented; requiring users to consult multiple portals, documents, and manuals to access legal assistance — creating inefficiencies and reducing clarity around legal requirements. This fragmentation also limits the applicability of legal support platforms within enforcement-oriented environments. Given the limitations associated with legal support platforms, there exists a need for unified platform that incorporates both Legal Interpretation and Cybercrime Assistance through a single intelligent framework.LawFort AI addresses these challenges by integrating artificial intelligence (AI), natural language processing (NLP), and role-based access control (RBAC) to create a unified legal and cybercrime assistance ecosystem tailored specifically for the Indian context. LawFort enables users to interact with legal content using natural language queries. Once those natural language queries are processed, they can retrieve structured and authenticated legal information. Additionally, the platform provides context-aware explanations based on the user query. To process the user's query through fuzzy search and semantic similarity techniques, followed by adaptive selection of local AI models, explainable AI mechanisms, or cloud-based large language models depending upon sensitivity and complexity of the user's query. The purpose of this research is to identify whether LawFort has addressed some of the challenges facing traditional legal support platforms. Therefore, we will investigate how well LawFort integrates artificial intelligence (AI) with natural language processing (NLP). We will evaluate how well LawFort uses role-based access control (RBAC) to enable users to interact with legal content.

1.1 Background on AI in Legal and Cyber Systems

Legal research systems that use artificial intelligence and cybercrime intelligence systems have developed quickly over the last decade, largely due to advances in transformer-based language models and deep learning [1], [2] and [5]. Traditional legal systems rely heavily upon keyword-based search methods and static data sets and are therefore unsuitable for conversational interaction and evolving legal structures [2], [9]. Research has shown that NLP models such as LEGAL-BERT, domain-specific transformers, and semantic embedding frameworks can be used to automate analysis of legal documents, extract clauses from legal documents, and classify documents into various categories [3], [7], [17]. However, most existing legal intelligence systems suffer from several serious limitations. Many of these systems were trained primarily using western legal data sets which makes them poorly aligned with the structure, interpretation, and application of laws in India [9], [10]. Most of these systems also rely on cloud based large language models (LLM) which results in greater risks associated with hallucinations outputs, privacy concerns regarding user data, and dependency on external servers [1], [11]. Furthermore, current solutions fail to support role specific access controls, i.e., restricted investigation modules designed specifically for law enforcement agencies [8], [14]. In contrast to these limitations, LawFort AI addresses each one of these challenges through integration of locally deployed AI models, explainable AI (XAI) reasoning frameworks, hybrid query interpretation techniques, and customized Indian legal databases [3], [7], [16], [18], [19]; therefore, ensuring higher precision, accountability and compliance with India's rapidly changing digital governance ecosystem [16], [18]. The objective of LawFort AI is to design and implement a platform for intelligent legal assistance capable of providing accurate legal interpretations, cybercrime assistance and structured investigative guidance [1], [3], [9]. This system seeks to improve accessibility to Indian cyberlaws by simplifying complex legal language and improving user comprehension through the aid of AI-assisted natural language processing techniques [2], [7], [8]. This system will provide AI-powered explanations of the law to assist law students, advocates, and citizens while equipping law-enforcement officers with standardized and role-specific procedural workflows aligned with Indian cybercrime regulations and reporting standards [4], [14], [19]. By reducing reliance upon time-consuming manual legal research and static keyword-based systems, this platform improves operational efficiency and ensures consistency in legal interpretation and procedural compliance [1], [10], [17]. In addition to increasing operational efficiency and ensuring consistency in legal interpretation and procedural compliance, LawFort AI includes an auditable and explainable decision-making framework using explainable AI (XAI) principles to ensure transparency, accountability, and legal reliability — essential requirements for technology assisted legal systems [5], [11]. Therefore, through enhanced public awareness of the law, structurally supporting investigations, and enhancing cyber safety practices; this platform bridges the gap between legal complexity and user understanding thereby promoting responsible digital citizenship and empowering stakeholders across both the legal and cybersecurity domains within India's continuously developing digital governance ecosystem [16], [18], [19].

2. LITERATURE REVIEW

The authors Donny Kurniawan and Siti Elda Hiererra introduced an AI Legal Companion as a way to increase the availability of legal services and raise the levels of legal literacy among the population via an NLP-based Public Legal Education Platform. This system enables users to better understand the legal rights and processes through simplified natural language responses. Although the method is very effective for the enhancement of general legal awareness and citizen empowerment, this method is not specialized for specific areas of law, such as cyber law and digital crime investigation. Also, the system does not enable the provision of explainable reasons for conclusions drawn from legal information or role-based access to limit the scope of applicability in enforcement and compliance oriented environments[1]. P. Vimala Imogen, J. Sreenidhi, and V. Nivedha presented an AI powered legal documentation assistant that uses NLP and automated document generation technologies to create and verify legal documents related to IT law. The system provides a reduction in the amount of time spent manually creating legal documents; increases the accuracy of legal documents created; and increases the productivity of legal professionals when creating legal documents. The model's performance depends heavily upon the quality and diversity of the training data used. In addition, the system has limitations in terms of its scalability and cannot adjust its intelligence to accommodate changes to legal amendments and variations in procedure[2]. The Cyber Mitra project developed by the Surat City Police along with the CyberPeace Foundation represents an AI chatbot that is linked to legal databases to assist law enforcement officers in the investigation of cyber crimes and the engagement with citizens. The platform enables faster and more efficient responses to citizen requests and some basic procedural guidance. Although the platform is useful in practice, it requires continual real-time legal and advisory updates and does not include advanced contextual

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 674-682

reasoning, explainable output, and standardized investigation workflows necessary to effectively investigate complex cyber crimes[3]. Dr. P. Sharma et al., developed an AI-driven digital forensics assistant to aid in the analysis of cybercrime evidence using automated forensic insights. The tool enables investigators to spend less time performing manual forensic workloads and to accelerate their ability to analyze evidence. The tool's accuracy and reliability are directly proportional to the quality and completeness of the forensic data used as input. Also, the tool does not contain layers for legal interpretations, therefore limiting its potential to connect technical evidence with applicable legal provisions[4]. [5] NyayGuru, an AI-based legal chatbot developed by Brainwave Technologies, enables ongoing legal assistance based on the Indian Penal Code. The system improves accessibility by providing twenty-four hours per day, seven days per week assistance to the public in obtaining answers to general legal questions and improving awareness about legal rights and responsibilities. Although the benefits of NyayGuru to public usage are significant, NyayGuru is incapable of handling complex legal reasoning, procedural sequences, and investigative decisions. Therefore, the inability of NyayGuru to specialize in cyber law and provide role-specific access to its functions limits its adoption in professional and enforcement environments. [6] Nikita Bhanushali et al., developed an auto-response system for legal consultations using RNN-based chatbots and keyword-driven retrieval mechanisms under the Indian IT Act, 2008. The system enables users to quickly obtain access to the relevant sections of the Indian IT Act, 2008 that define cyber law offenses and penalties. Although the system provides quick access to relevant cyber law sections and offenses and penalties, its reliance on keyword matching to find relevant sections of the act severely limits the semantic understanding, adaptability, and contextual accuracy of the system. In addition, the system is unable to provide explanations and does not provide for dynamic legal updates and investigative workflows. [7] Many studies on AI-based legal chatbots focus on the use of rule-based systems and predefined logic for querying and answering user inquiries. Although these methods provide determinate outputs, they fail to interpret complex legal inquiries that may include exceptions, cross-references and procedural relationships. These limitations reduce the effectiveness of these methods in real-world legal situations, especially in cybercrime investigations where contextual and sequential reasoning are paramount. [8] Recent developments in transformer-based NLP models, i.e. BERT and LEGAL-BERT, demonstrate superior performance in legal text classification, similarity analysis and statute retrieval compared to traditional rule-based NLP models. However, since most of the current transformer-based models are trained on Western legal datasets, they are not well-suited for use with Indian cyber laws that are structurally, terminologically, and procedurally different from those of the West. The above-mentioned limitations create obstacles for the use of these practices in India's legal and regulatory environment. The literature associated with digital governance and cybercrime reporting mechanisms generally focuses on the challenges of online complaint filing (registration), grievance redressal, and case management portal design. Online complaint filing (registration) and grievance redressal (case management) portals can improve access to complaints filed by individuals and organizations, as well as increase the efficiency of administration for complainants and respondents. However, few of the existing portals provide sophisticated legal interpretation functionality, standardized investigative procedures, or AI-assisted decision support to law enforcement agencies. Also, little attention has been paid to developing role-based access controls and auditing systems. [10] The existing literature indicates a clear gap exists in the integration of explainable AI, hybrid query processing, localized legal data sets, and compliance with Indian data protection regulations such as the DPDP Act. Most of the systems utilize either cloud-based AI models or static rule engines, leading to a number of concerns regarding hallucinations, privacy, and accountability. These limitations illustrate the necessity of establishing a secure, explainable, and role-aware AI-based legal platform to meet the needs of the Indian cyber law enforcement community that will serve as the foundation for the proposed LawFort AI System.

3. EXISTING SYSTEM

Existing legal assistance and cybercrime support mechanisms can be generally classified into four categories, namely, government operated portals, rule-based legal chatbots, international AI-based legal research tools, and non-AI cyber investigation practices. Although each category of systems contributes to legal accessibility and case management, each category of systems exhibits significant functional and operational limitations.

A. Government Portals: Government maintained portals such as the India Code and Bare Act repositories allow authorized access to statutes, rules, and legislative amendments. However, these portals primarily depend on exact keyword search functionality and do not offer natural language search capabilities, thus limiting their usability by non-expert users. The eCourts portal enables access to case status, judicial orders and judgments, and thus is a valuable resource for legal practitioners; however, the portal is not designed to facilitate legal education and investigative support. Similar to the eCourts portal, the National Cybercrime Reporting Portal established and administered by the Ministry of Home Affairs, enables citizens to register complaints related to cybercrimes; however, the portal does not provide any interpretative assistance to citizens, and instead requires citizens to have prior knowledge of how to classify offenses and what applicable legal provisions apply.B. Rule-Based Legal Chatbots: Rule-based legal chatbots, such as NyayGuru, developed by the CyberPeace Foundation and academic prototypes, are designed to rely on predefined rules and keyword-driven logic to determine the appropriate responses to user inquiries. Although rule-based legal chatbots are able to rapidly respond to basic legal inquiries, they are unable to interpret ambiguous or complex legal inquiries. Additionally, because the logic contained in the rule-base is fixed, the ability to adapt to changing legal frameworks, such as updates made pursuant to the DPDP Act 2023/2025, is greatly diminished, thus diminishing long-term reliability.

C. International AI-Based Legal Research Tools: The increasing sophistication of AI-based legal research platforms, such as CaseText (CoCounsel), Westlaw AI, and Lexis+ AI, enable superior capabilities for legal analysis in the context of Western jurisdictions using transformer-based NLP models. Although the technology behind these platforms is highly sophisticated, they were not trained on Indian statutory frameworks; the cost associated with subscribing to the service is typically high; the platforms consume large amounts of computational resources; and the platforms are not capable of being easily integrated into the workflows of the Indian government and/or law enforcement agencies due to regulatory and operational barriers.

D. Non-AI Cyber Investigation Practices: In absence of availability of AI based crime investigation methods for cybercrime, several Police Departments have continued to utilize non-AI based approaches such as manual documentation templates, static PDF based guidebooks, unstructured verbal communications, and independent web-based portals for reporting crimes and managing cases. Officer training is traditionally conducted individually whereas the typical way that workflow processes are utilized by investigators within an organization creates a variety of procedural irregularities and decreases operational efficiencies.

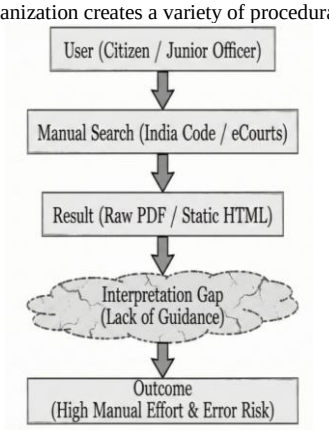


Figure 1: Limitations of Existing Legal Systems

3.1 Gaps in Technology and Accessibility

The existing gap in technology and accessibility for current legal and cybercrime help systems, combined with an overall lack of a singular, combined legal assistance and cybercrime support interface, limits users' access to relevant resources. Currently, users are required to locate legal assistance from numerous legal libraries, online portals, and static documents. All of today's legal and cybercrime help systems are based on either rule-based automation — in which a predefined set of rules assists users in obtaining legal help — or large language models (LLMs) — in which machine learning algorithms assist users in finding answers to legal questions. Neither of these technologies utilizes a hybrid AI model that includes fuzzy search, local processing, XAI, or advanced LLMs. Additionally, few if any current systems fully comply with each requirement of the Digital Personal Data Protection (DPDP) Act 2025 — including purpose limitation, minimal data storage, consent-based processing, and user control over their personal data. The majority of current systems do not include functional separation for various roles within the system (i.e., citizen, law student, law enforcement officer, etc.). Finally, LawFort AI has identified several limitations to the availability of AI-assisted

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 674-682

investigative tools — including automated FIR classifications, evidence collection workflows, investigation timelines generated by the AI system, and validation of procedures implemented by the system against the provisions of the IT Act and DPDP Act. Due to these constraints and barriers to accessibility — particularly those experienced by individuals with low levels of digital literacy who struggle to identify cyber threats and determine how to protect their rights under India's data protection laws — LawFort AI represents a unique opportunity to create a new class of legal intelligence systems that integrate compliance and transparency.

4. PROPOSED SYSTEM

LawFort AI is a hybrid legal intelligence system designed to facilitate real-time legal help, cybercrime investigations, and interpretative analyses of India's cyberlaws. Like previous legal information systems that relied solely on static database queries or singular AI models; however, LawFort AI employs a multi-layered processing framework that integrates fuzzy search methodologies, semantic embeddings, localized AI inference using transformer models, explainable AI (XAI) reasoning, and cloud-based large language models (LLMs). This hybrid methodology will allow for more accurate contextualization, minimize "hallucinations," and satisfy regulatory requirements. The system has been built around a secure role-based access control (RBAC) model to differentiate between citizen, law student, legal professional, and law enforcement roles, and thus enable each group to have access to specific functions within the system. The dual-mode architecture of LawFort AI includes a public legal assistance mode and a law enforcement mode. The public legal assistance mode includes simple legal explanation, cyber-safety awareness, phishing link detection, and access to updated legal provisions. The law enforcement mode includes structured investigation workflows, evidence handling protocols, procedural guidance for investigating cybercrimes from FIR registration through to charge sheet preparation, cybercrime categorization, and CERT-In reporting assistance. This will facilitate the inclusion of all user groups in both legal and operational contexts.

Key goals of the proposed system include: providing an accurate natural language understanding of legal questions asked; implementing a hybrid AI pipeline that combines both semantic retrieval and explainable reasoning; segregating different user groups through a secure role-based access control methodology; generating standard cyber investigation workflows for authorized users; ensuring compliance with Indian Digital Regulations, i.e., the DPDP Act 2023/2025, the IT Rules 2021, and the CERT-In Directives; increasing cyber-fraud awareness; ensuring auditable activity through comprehensive logging; and supporting future scalability and multilingual growth. LawFort AI addresses some major gaps in current legal and cybercrime support systems. First, LawFort AI democratizes legal knowledge by converting complicated statutory language into simply understood, context aware explanations. Second, for law enforcement agencies, LawFort AI introduces the use of standardized AI-assisted investigation workflows that cover FIR categorization, procedural sequencing, evidence integrity verification, and regulatory reporting. Third, the combination of a hybrid AI architecture that includes keyword-based retrieval, semantic matching, local inference, and cloud-based reasoning minimizes the reliance on external models, and therefore increases reliability. Finally, integrated cyber safety tools increase the level of awareness among the general public regarding cyber-fraud and decreases their susceptibility to online fraud.The system architecture consists of several interconnected modules, which include: a natural language user interface; a query classification module; a fuzzy search and semantic retrieval engine; a hybrid AI reasoning pipeline; a centralized legal and cybercrime repository; an RBAC security layer; an audit logging module; and an investigator workflow generator for law enforcement users. Each module is designed to ensure accuracy, transparency, and procedural consistency in order to decrease the likelihood of investigative error and improve legal compliance. LawFort AI was developed with the primary objective of working within Indian legal frameworks. It includes statutory sources like the Information Technology Act and its amended versions, the DPDP Act, CERT-In advisories, the IT Rules 2021, Bharatiya Nyaya Sanhita provisions, and guidelines on digital evidence. The data used by LawFort AI consists of official government repositories, authenticated legal documents, publicly available cyber investigation materials, academic datasets, and curated cybercrime templates. A multi-layered modular structure of the Integration Strategy enables each component of the System to interact with each other using secure API calls (independently), as well as enabling the separate update of models. A compliance-focused design ensures that all data retained is minimal, and encrypted logs are maintained along with pseudonymization of data as per DPDP requirements. The System can support an open scalable deployment across multiple Cloud Platforms or on-premises infrastructure based on the needs of Law Enforcement Environments.

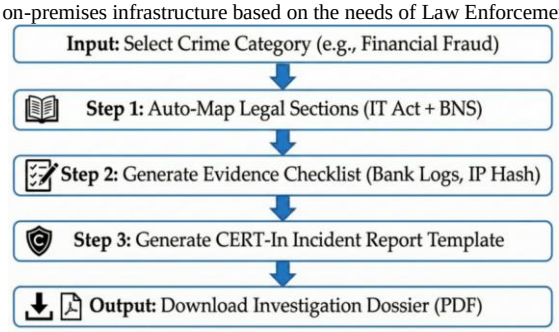


Figure 2: LawFort AI Investigation Workflow

The LawFort AI System provides an automated flow in the investigation of Cyber-Crimes which will integrate Legal Reasoning, Evidence Guidance & Regulatory Documentation as a single Intelligent Framework for the investigation of Cyber-Crime cases. The System is intended to remove manual efforts, procedural mistakes, and delay times that are common when investigating crimes committed using technology. The System also helps to establish the Investigation Process into the Stages of Investigation to ensure Consistency, Accuracy and Legal Compliance from the commencement of the Investigation through to the conclusion of the Case. The first part of the workflow is where the user selects an offense type (e.g., financial fraud) that falls into the crime category selected by the user. The user's selection will establish the context for all subsequent steps in the workflow. It is also designed to allow investigators to provide a high-level definition of the incident rather than requiring them to provide technical or legal definitions in detail. Thus, it provides a high degree of usability regardless of whether the user has extensive experience with legal and/or technical issues related to cybercrime.When the appropriate crime type is selected, LawFort AI will automatically determine the correct applicable legal sections under both the Information Technology Act and Bharatiya Nyaya Sanhita for that specific incident. Through automation, LawFort AI significantly lessens the investigator's dependence upon manual legal interpretation so they have confidence that their investigations start with proper legal footing. Following identification of legal section, LawFort AI creates a digital evidence checklist relevant to the particular case being investigated. This checklist identifies common evidence artifact types necessary for investigations such as bank transaction records, IP address logs, communication metadata, device identifiers and cryptographic hash values. Investigators are provided guidance on what evidence artifact types to collect to support a systematic and legally compliant evidence collection process thus reducing the probability of missing some key forensic element(s) during an investigation. Following generation of digital evidence checklist and selection of appropriate crime type, the workflow continues in automation of creation of an incident report template according to CERT-In guidelines. Automated incident report templates will create consistent formats for documenting all facets of a cyber-incident (for example: Incident Description; Technical Impact; Systems affected; Response measures) thus increasing consistency and adherence to established documentation procedures regarding cyber-incidents and standardizing reporting procedures among investigators and agencies responsible for responses. Upon completion of process, LawFort AI will integrate the mapped legal sections, evidence checklist and incident report template into a single Investigation Dossier document format. The resulting dossier will be generated in PDF format that can be easily stored, shared amongst interested parties and submitted to the appropriate authority (such as judicial bodies, regulatory agencies). Benefits to generating this singular document include; elimination of administrative burdens related to production of additional supporting documentation and maximization of operational efficiency of investigative process. Thus, by integrating Legal Intelligence, Evidence Guidance and Regulatory Compliance through a single pipeline, LawFort AI will increase the level of precision and consistency in investigations, enable scaling of operations and ensure that the platform may adapt to new developments in Cyber Laws and evolving trends in crimes. Therefore, the platform is designed to deliver long-term value to both law enforcement and organizations supporting the legal system.

5. SYSTEM METHODOLOGY

5.1 System Architecture: The LawFort AI architecture is a module-based, scalable, and compliant-based architecture that enables the full integration of all parties involved (users, legal databases, AI models, and specialized police modules). It has been developed as a multi-stage pipeline to ensure the highest possible quality of results (accuracy), complete transparency and role-based user separation.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 674-682

A. User Interaction Layer The User Interaction Layer represents the main entry point into the LawFort AI System for the end-users. It was developed to allow users to interact with the LawFort AI System by submitting legal and cybercrime-related questions in natural language (text-based and/or voice-based). This layer has an emphasis on accessibility and usability to be able to accommodate different types of users (citizens, law students, legal professionals and law enforcement personnel). In addition, it has been developed as a web-based interface with a high degree of responsiveness and intuitiveness to enable users to submit queries, review legal explanations and access system output in a structured way. Voice input capability has also been included to increase accessibility for users who have difficulty with keyboard-based typing or have lower levels of digital literacy. All user submissions are sent to the backend query processing layer via an encrypted channel to provide maximum protection of the user's data. Prior to sending queries to the backend query processing layer, the interaction layer will perform some basic input validation to minimize the possibility of maliciously formatted requests being made to the system and reduce the risk of SQL injection-type attacks. User session information is used to map the current user to one of several predefined roles in accordance with the Role-Based Access Control (RBAC) method. Once a user is mapped to a specific role they will only be provided with features and response options related to their assigned role. With the establishment of a secure and accessible interaction point, this layer provides the foundation for successful human-AI collaboration in the LawFort AI Platform.

B. Query Processing Layer: The Query Processing Layer serves as a connection point to relate the user's query to the AI-based legal reasoning engine. The layer formally represents the user's query to the LawFort AI system using the user's original intended legal context and meaning of their query. Because the target user group for LawFort is so broad (citizens, law students, law enforcement), the system must be capable of recognizing and interpreting user queries in both natural language and non-standard/technical terminology. Following initial text preprocessing to normalize/clean the user query (i.e. noise reduction, punctuation normalizing, removal of stop-words from user query that add little semantic value to the search, spell checking, and conversion of query to standardized syntax/language), the system determines the intent of the user query and classifies it. We utilize a lightweight classifier to categorize each user query as belonging to one of several possible domains (legal information retrieval, cyber crime guidance, procedural investigative workflow, data protection rights, or cyber safety). Once the system has determined the domain(s) the user's query belongs to, the system then determines what steps need to occur in order to process the query and applies role based access control to assure that only those individuals authorized by law enforcement management are allowed to view/utilize the results of specific types of investigations. Additionally, the Query Processing Layer identifies the entity(ies) contained within the users' query (e.g., act names, section numbers, offense category names, procedural stage names, etc.) and identifies them in a manner that allows them to be utilized by either the Legal Information Retrieval Engine or AI Reasoning Module to provide accurate and authoritative responses to the user's query. Through providing a normalized, categorized, and contextually-relevant structure for the user's input, the Query Processing Layer greatly reduces the probability of ambiguous interpretation, increases the reliability of the LawFort AI system, and establishes an environment where the LawFort AI system is able to generate legally compliant responses.

C. Retrieval Engine : The Retrieval Engine provides the primary means of accessing legal documents (the 'lookup' function) and delivers legal information that is contextually correct and accurate through a combination of fuzzy keyword searching and semantic searching techniques using domain-specific vector representations of the legal content. The fuzzy searching will allow the system to retrieve legal documents that have been queried with misspelled words, partial word searches, colloquialisms, etc., thus providing a very high degree of coverage initially, while the semantic searching will attempt to capture the true meaning of the query in order to provide the user with legal documents that are applicable to their query regardless of whether the document uses the same terminology. The semantic searching layer will also be able to identify legal documents that contain the same underlying intent as the query, but use different wording. The Retrieval Engine can operate over repositories of curated and updated cyber laws of India, procedural laws of India and regulatory guidelines of India to ensure that the legal documents retrieved from the system are legally correct and pertinent to the query made by the user. The system will rank the legal documents retrieved according to a relevance score that takes into account the semantic similarity and lexical confidence associated with each of the retrieved documents. This ranking will enable the system to select the legal documents that are most relevant to the query and to establish confidence levels to ensure that the selected legal documents will be used to generate responses to the user's questions. Through the balance of recall and precision, the Retrieval Engine enables the transition from query expressions that are understandable to laypersons and formal legal documents, thus improving accessibility, consistency and reliability for users who include citizens, legal practitioners and law enforcement personnel.

D. Hybrid AI Engine : The Hybrid AI Engine is the central intelligence unit of LawFort AI which generates reason, interpretation, and responds to inputs. The Hybrid AI Engine has a multi-layered structure where three complementary types of reasoning modules have been integrated into the Hybrid AI Engine. These include a transformer-based model; an Explainable AI (XAI); and large language models that reside in cloud storage. The transformer-based model allows for the secure processing of sensitive legal and investigative information in an offline manner, allowing this type of data to be processed locally with no data transmitted out of the device or network. The XAI component of the Hybrid AI Engine allows for the structured and transparent nature of the decision-making process of the system through the creation of decision pathways; rules-based explanations; and justification links to legal principles. As such, this component enhances the trustworthiness, accountability, and explainability of the output generated by the system. Large language models in cloud storage are used for more advanced natural language processing functions, such as linguistically simplifying complex legal concepts; creating summaries of long documents; and explaining the context of complex legal issues. As such, these components allow for easier comprehension of the responses provided by the Hybrid AI Engine from users who are not experts in the area of law. The Hybrid AI Engine dynamically determines the best method for processing input (i.e., which reasoning mechanism will be utilized), based on several factors including the level of complexity associated with the input query; confidence levels of the reasoning mechanisms selected; the sensitivity of the information being processed; and user access rights to the system. This ability to dynamically determine which reasoning mechanisms to utilize at what time, reduces the risks associated with "hallucinations" (i.e., incorrect interpretations of information), preserves the legal accuracy of the output; ensures that the output is clear and understandable; and produces a reliable and accurate output for use in a variety of applications, including but not limited to, legal, academic, and law enforcement.

E. Response Generator : The Response Generation layer is the layer that transforms (validated) system output into understandable, structured, and appropriate to the user response. It will alter the depth of the explanation; the tone of the explanation; and how the explanation is presented depending upon the role or level of authorized access a user has. For example, the Response Generation layer will simplify legal explanations so they are easier for the public to read/understand, but maintain the legal-technical accuracy/procedure detail for legal professionals/law enforcement personnel. Relevant statutory references, applicable legal sections, and as needed, the Response Generation layer will generate step-by-step procedural guidance to assist the user in making an informed decision. Wherever possible, the Response Generation layer will provide contextual explanations to help bridge the gap between legal terminology and real-world situations, improve interpretability and practical relevance. Ultimately, the Response Generation Layer provides consistent language, consistent structure and consistent with their authorization level for the system outputs to be consistently reliable, consistently understandable and consistently suitable for all user types.

F. Role-Based Access Control & Logging : Role-Based Access Control (RBAC) is utilized throughout the entire Law Fort AI System to restrict User Functionality, Data Accessibility, and Output capabilities by pre-defining specific Roles for Users; i.e. Citizens, Students, Legal Professionals, Law Enforcement Personnel. Features of the Law Fort AI System that are publicly available for informational and educational purposes will only be accessible to Public Users. Additionally, Investigation Workflows, Confidential Legal Guidance, and Evidence Related Modules will only be accessible to Authorized Law Enforcement Personnel to protect against unauthorized disclosure of Sensitive Information. Permissions will be dynamically assigned at runtime allowing the system to modify its Response Depth, Reasoning Transparency, and Feature Availability based on the User's Authorization Level. An Audit Log Mechanism will be implemented to capture all Significant Interactions within the system including Type of Query, Modules Accessed, Access Level Used, Timestamp, and System Action. These Logs will be Securely Stored to Protect the Integrity of the system, Enable Accountability and Traceability, and Meet Compliance Requirements of Federal and State Regulations. As such, this system can be effectively utilized in Legally Sensitive and Operationally Critical Environments. Police Investigation Module. The Police Investigation Module is a Limited Component that will only be accessible by Authorized Law Enforcement Personnel. This module will generate Standardized Investigative Workflows applicable to each Category of Cybercrime, Financial Fraud, Identity Theft, Cyber Stalking, and Data Breaches. In addition, these work flows will provide Step-by-Step Procedural Guidance consistent with the provisions contained in the Information Technology Act, DPDP Act, and CERT-In Directives. Through the standardization of Investigative Processes, Errors in Process will be minimized and Efficiency in Operations will improve.

G. Cyber Safety Module

The Cyber Safety Module was created to improve the general public's knowledge of cyber threats and to help prevent them through a real time support function for online safety and digital rights. As a public user access module that operates separately from the law enforcement modules it does not restrict access while

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 674-682

maintaining the system's integrity. The module uses rule based validation in combination with semantic analysis to identify and analyze suspicious URLS, phishing links, fraudulent email messages and common cyber scams. The system evaluates user input against previously identified threat indicators and cyber crime categories to assist in providing the user with contextually relevant warning messages, suggested precautions and recommended action to take. In addition to assisting in the identification of potential cyber threats the module assists in educating users about good cyber hygiene practice, i.e., the use of secure passwords, safe browsing habits and data privacy protection pursuant to the Digital Personal Data Protection (DPDP) Act. Through the integration of cyber safety best practices along with an explanation of the applicable laws the Cyber Safety Module provides a link between identifying technical cyber threats and understanding the associated legal implications. Ultimately this will lead to less victimization and more informed digital behavior resulting in a safer online environment.

H. Database Layer

The database layer makes up the majority of the "brain" of the LawFort AI system in that it holds all of the structured and validated legal information and cybercrime related information needed to generate workflow and to provide answers to queries asked of the system. The database layer is made up of two main databases: a legal knowledge base (KB) and a cybercrime investigation database. The legal KB contains all authenticated Indian legal materials including; the Information Technology Act, Digital Personal Data Protection Act, Bharatiya Nyaya Sanhita, procedural codes, etc., along with the necessary amendments. All of these legal materials have been indexed and semantically tagged in order to allow for efficient fuzzy matching and similarity-based retrieval. The cybercrime DB has categories of cybercrimes, investigative templates, procedural guides, CERT-IN advisories, and case references (based on publically available and authoritative sources).

This block diagram representing the structural organization of LawFort AI illustrates the primary flow of data throughout the various components of the system. The process begins with the user interface, where the user inputs both text and voice queries. The inputted queries are then directed toward the hybrid query-processing engine, where fuzzy search and semantic similarity models identify relevant legal sections within the internal law repository. Based upon the complexity of the query, the system will trigger one of three AI reasoning paths: local offline AI model, XAI module, or cloud-based LLM inference.

After Relevant Information has been Identified or Generated from the Analysis Engine it will be forwarded to the Formatting and Output Engine to Present the Information to the User in a Format That is Friendly to the User. For Police Users an Additional Chain Connects to the Investigation Workflow Generator and Evidence Handling Module. This Architecture Supports Modularity, Scalability, and Strict Role-Based Access Control.

Figure 3: Basic Block Diagram of LawFort AI System

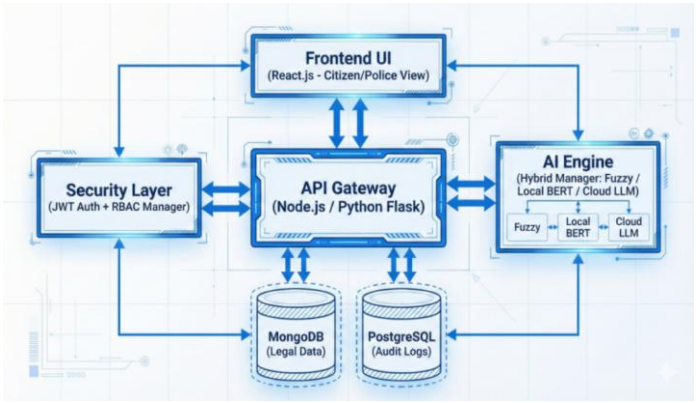


Figure 4 – System Architecture of LawFort AI

5.2 Technologies Used

Legal technology used to achieve goals of reliable legal answers, fast and accurate responses, and legal and secure access to information.

a) Artificial Intelligence and NLP Technologies: Transformer-based models like Bert, LEGAL-BERT, and DistilBERT provide contextual understanding of text relating to legal and cybercrime domains. These models were adapted from their original form to enable them to understand statutory language; legal terms; and procedural narratives common to India's cyber laws. The system employs named entity recognition (NER) to identify key legal entities which include act names, section numbers, organizations, digital artifacts, and timelines that assist in the structured interpretation of unstructured legal text. Legal documents & user queries are embedded into a high dimensional vector space utilizing semantic embeddings to support similarity-based retrieval. Finally, a hybrid query interpretation methodology is employed to combine machine learning inference with rule-based legal logic & constrain probabilistic model outputs within predefined legal rules and statutory bounds to ensure doctrinal correctness. b) Hybrid AI Pipeline: A hybrid ai pipeline is used to achieve accuracy, explanations, and security through a variety of reasoning and retrieval mechanisms. A fuzzy search engine is used on structured legal databases to find relevant provisions by handling partial matches, spelling variants, and informal phrases. Non-sensitive queries (i.e., privacy-sensitive and/or confidential information) are processed utilizing locally-deployed ai models to avoid exposing externally accessed data & comply with data protection regulations. Xai components are integrated into the system to produce transparent reasoning paths, confidence scores, and justification links between queries & legal results to enhance user trust & auditability. Cloud-based large language model (LLM) APIs are utilized on a selective basis for non-sensitive applications (such as linguistic simplification, summarization, readability enhancements), leverage advanced language capabilities without compromising either privacy or legal integrity. c) Backend and Database: The flexible service-oriented architecture of node.js & python flask supports efficient request handling & modular design of services, along with compatibility between ai services & Web components. Unstructured and semi-structured legal content (statutes, guidelines, advisory documents) is stored in mongodb. Structured data (user roles, access permissions, case metadata, system logs) is managed in PostgreSQL. Role-Based Access Control (RBAC) manages user authentication & authorization across different categories of users at the back end. An extensive audit log recording system captures all interactions in the system, query processing events, & access decisions to support post-incident review, traceability, & legal accountability. d) Web Technologies: React.js is utilized to develop the responsive interaction environment of the frontend of LawFort AI. Secure communication with back-end services is achieved via an api gateway that enforces access control policies & validates requests. Https encryption protects data transmitted over the network. Sessions are secured via JWT-based authentication to prevent unauthorized access. Content presentation is dynamically adjusted based upon user roles such that sensitive investigative features are available only to authorized personnel while providing clarity and simplicity for public users. e) Security and Compliance: Security and Compliance are central considerations in the design of LawFort AI. By implementing principles of data minimization, access control, purpose limitation the platform meets requirements of dpdp act 2023/2025. The platform incorporates support for CERT-In reporting standards to facilitate standardization of cyber incident documentation and regulatory communications. Local caching of data is implemented for controlled processing. Input sanitization is implemented to prevent injection attacks. Continuous monitoring of access is implemented to detect unauthorized or anomalous usage patterns to add overall system resiliency, safeguard digital evidence and support lawful and responsible use of the platform.

5.3 NLP Processing Pipeline: User input is preprocessed via standard techniques (case normalization, noise elimination, lemmatization and spelling correction) in order to make user input consistent with previous examples. Legal Domain Embedding Models are used to create a representation of the user's query that captures more than just similar keywords. A hybrid ranking algorithm based upon both fuzzy matching and semantic similarity is used to rank the relevant legal documents that were returned by the search engine. Depending on the complexity of the question and how sensitive it is, the system will select the best response

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 674-682

method from one of three options: local inference, structured explainable reasoning or use of a cloud based language model. Once selected the best response method, the system generates a response that accurately reflects the users' question, is fully explainable and provides context to the user while limiting risk to the user.

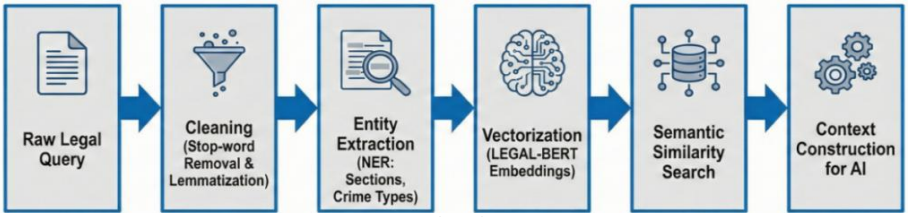


Figure 5 – NLP Pipeline Workflow for Legal Query Processing

5.4 Hybrid Query Interpretation

LawFort AI uses a multi-path hybrid query interpretation method to improve the likelihood of accurate responses while minimizing the risk of "hallucinations" common in many single path AI systems. The initial step is to match the users' query against the internal legal repository using fuzzy string matching. If the confidence level of the match exceeds a pre-defined threshold, the system will provide the applicable statutory provision(s) from the repository. Where there are partial or ambiguous matches, the system invokes a transformer-based local model for contextual analysis on the basis of a curated legal knowledge base (the Legal Knowledge Base). Following this, the system's reasoning layer provides an explanation for its decisions based upon the generation of transparent decision paths and legal rationales. For complex analytical inquiries or procedural summaries for law enforcement use, cloud-based large language models can be selectively invoked. All of the output from LawFort AI passes through a validation layer which ensures that the statutory authority cited is authentic; filters out sensitive information; and restricts access to data consistent with the user's designated role, thereby providing reliable and compliant legal answers.

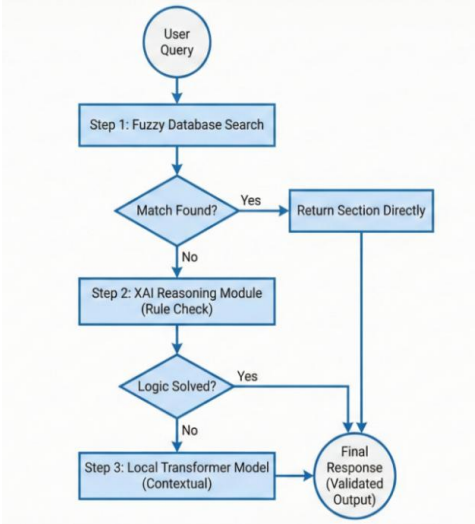


Figure 6– Hybrid Query Decision Flow for AI-Based Legal Assistance

5.5 Role-Based Access Control (RBAC) Model: Role-based Access Control (RBAC), is an important layer of security for the LawFort AI Platform. It is designed to limit how certain users can interact with the systems' features and legal documents that require special authorization. Because the Legal and Investigative aspects of the LawFort AI Platform requires both data protection and adherence to India's data protection legislation, it is crucial that all users be limited to their assigned role when interacting with the systems' features and legal documents. The LawFort AI Platform will classify all users into one of four roles. General Users/Citizens will have access to standard legal information, Cyber Law awareness materials and Cyber Safety Utilities such as Phishing Link Verification. This role is intended to educate the public on legal issues without providing sensitive procedure related data. Students and Researchers will have extended access to Legal Section Interpretations, Case Law References and Structured Learning Materials to assist them in their academic studies and/or legal research. Law Enforcement Officials (LEO's) will be given a highly restrictive and privileged role which will allow them to utilize Investigation Workflow Generators, Evidence Handling and Chain-of-Custody Guidelines, Cyber Crime Classification Modules, and Procedural Checklists specific to India's Cyber Laws and CERT-In Directives. In doing so, the LawFort AI Platform will ensure that only those users who have been properly authorized, will have access to the tools necessary for their investigations. System Governance is the responsibility of Administrative Users and includes, but is not limited to, assigning roles to users, creating police accounts, updating databases, maintaining workflows and monitoring audit logs. The implementation of RBAC is accomplished through a variety of technical controls including JWT Authentication, Encrypted Session Cookies and Database Level Permission Flags which dynamically restrict what queries can be executed and what data can be viewed by each user. All user interactions are logged using a Secure Audit Mechanism which provides Traceability and Accountability. In addition, Data Storage and Access are segregated as required under DPDP Act and provide for the proper processing of data, minimize the exposure of data and segregate data based upon the user's assigned role.

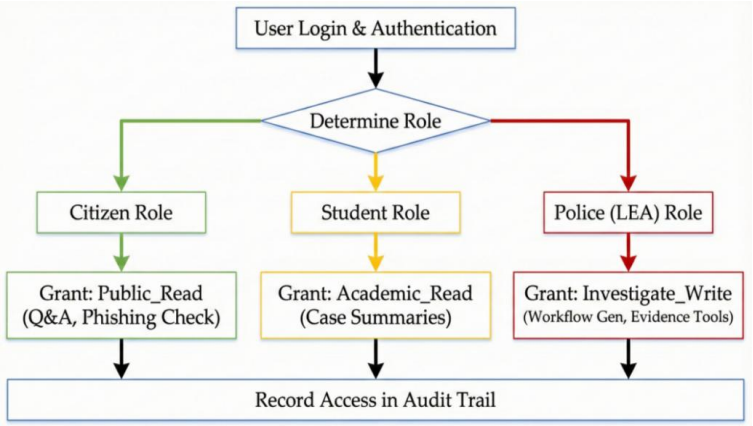


Figure 7 – Role-Based Access Control (RBAC) Flow Diagram

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 674-682

5.6 LLM-Based Legal Interpretation Model: The LLM-based Legal Interpretation Model was developed to support an advanced understanding and contextually based interpretation of legal and cybercrime-related inquiries using natural language. The model uses a large language model that has been fine-tuned to focus on legal domain texts to provide an analysis of user inquiries, determine what legal intent exists within the inquiry and to match the inquiry to the applicable statutes, procedural rules, and regulations. Because the model focuses on the context of the inquiry (i.e., semantic meaning) as opposed to keyword matching, it can interpret inquiries that have some ambiguity, are partially completed, or have been phrased in terms of "everyday" language (which is typical of non-legal users). The model also supports the translation of legal terminology from complex to simple while maintaining doctrinal integrity and statutory applicability. In addition, the model works in conjunction with the retrieval and hybrid AI layers to ensure that the interpretation is supported by verified legal source(s) and validated output(s). Thresholds for confidence and references are used to limit the occurrence of hallucinations and to preclude unsupported legal assertions. Overall, through its design, the LLM-based Legal Interpretation Model supports enhanced access, interpretability, and reliance upon legal assistance, thereby supporting public use, legal practitioner use, and law enforcement authority use of LawFort AI.

5.7 Authentication and Role Verification Method : The purpose of the Authentication and Role Verification methodology used by LawFort AI for ensuring the secure, reliable, and controlled access to the system's resources while meeting applicable laws and regulations is addressed by the use of a multi-layered authentication process. In addition to using credential-based login with secure token management, the system will also perform a role verification after an authenticated user has successfully logged into the system to identify the user's authorization level. Users may be classified in a variety of roles such as citizen, student, legal professional, law enforcement etc. The roles identified above have been pre-defined and related to specific system permissions. The validation of user roles is accomplished through an RBAC-based framework, managed centrally across the service layer and application layer. Each incoming request to any function will have the user's role validated prior to access to any feature(s), legal content, or system output. This will allow users to only access what is relevant to their specific responsibilities and classification levels. Only those who are authorized to do so within the law enforcement community will have access to sensitive investigation modules, confidential legal guidance and procedural workflows. Secure methods for managing sessions using token-based authentication and encryption will protect user credentials and session data from being compromised. A user's role will be stored inside the access tokens used for authentication and verified in real time, this will provide the ability to dynamically authorize access to functions and features. All attempts to validate a user's identity and grant/deny them access to the system will also be recorded in the audit logs which will provide traceability, accountability and compliance monitoring. In summary, the use of strong authentication mechanisms combined with strict role validation mechanisms provides LawFort AI a means of securely interacting with users, minimizes the risk of security breaches and provides a responsible method for deploying LawFort AI into a highly regulated environment that contains a significant amount of legal sensitivity.

RESULTS AND VISUAL ANALYSIS

The LawFort AI System was deployed to test a variety of functionalities such as hybrid query interpretation engine, natural language processing (NLP) pipeline, legal retrieval system, phishing detection module, and role based police investigation workflow generator. The testing of the above functionalities produced significant performance with respect to interpreting legal queries, retrieving relevant Indian Cyber Laws sections accurately, and generating workflows based on roles in a controlled environment. This section provides an overview of the outcome of the evaluations of the LawFort AI System, qualitative performance characteristics of the system, and visual representation of the system's output.

Legal Query Interpretation Accuracy

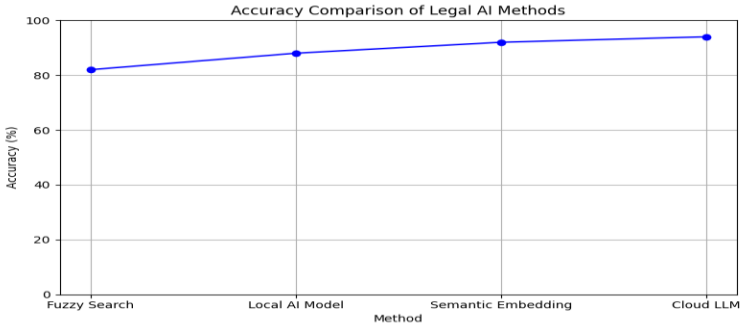


Figure 8: Accuracy Comparison of Legal AI Methods

Performance of Phishing Link Detection Module

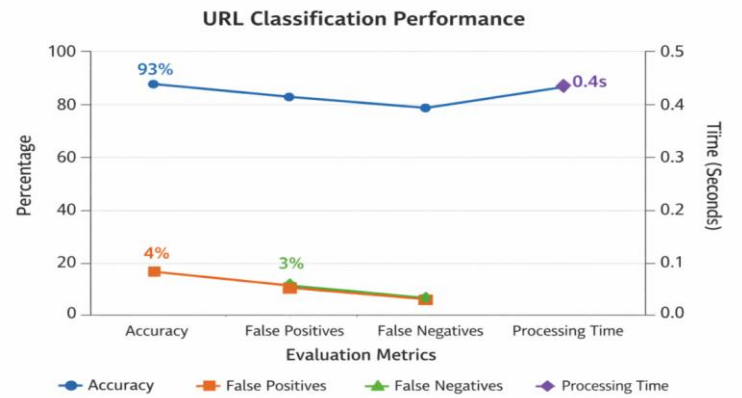


Figure 9: URL Classification Performance Analysis

Query Interpretation

The interpretation of effective queries is key to effective decision support systems that will work in an environment with many variables and/or domain specific information. A comparison of multiple types of query interpretation was done to compare their efficiency. The different query interpretation methods compared were fuzzy search, semantic embeddings, local artificial intelligence models, cloud-based large language models (LLMs) and a hybrid of these query interpretation methods. Fuzzy search provides fast retrieval and is very good at handling misspelled words but it does not have any knowledge about the context. The semantic embeddings are better than fuzzy search because they can find similarities between a query and a document based on semantics and thus are able to retrieve documents from databases in a more efficient manner; however, semantic embeddings do have limitations when dealing with multi-intent queries or ambiguous queries. Local AI models allow for better contextual reasoning and better domain-specific interpretation of queries; however, their ability to perform well is limited by the size and scope of their training data. Cloud-based LLMs provide excellent natural language understanding and explanations for a given input; however, when used as a single entity, they could potentially create inconsistencies and/or hallucinate some output. The hybrid pipeline performed the best in comparison to the other individual pipelines. The reason is due to its ability to combine lexical matching, semantic similarity, contextual reasoning and high level language understanding to obtain a more accurate and consistent interpretation of a query and thereby reduce the amount of ambiguity and/or misclassifications.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 674-682

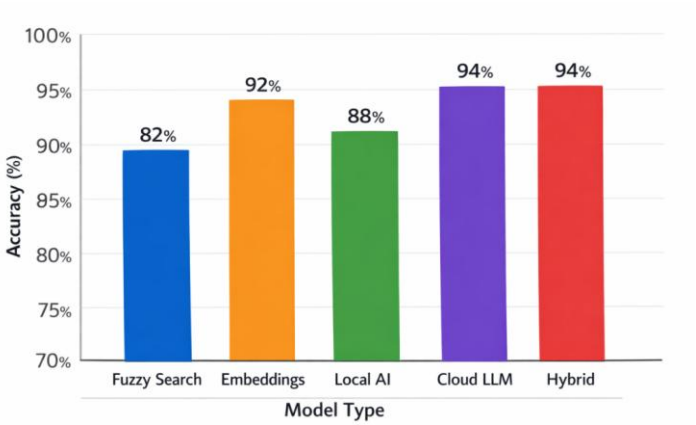
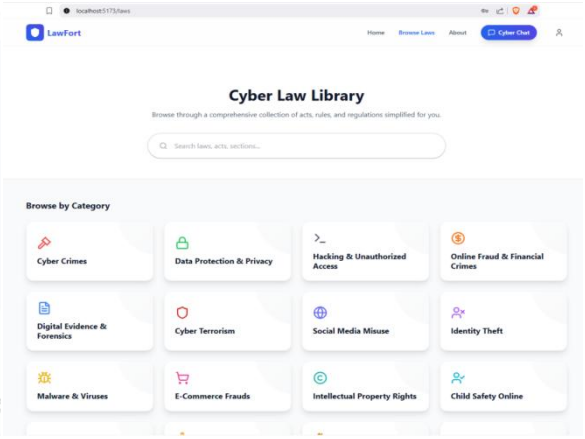
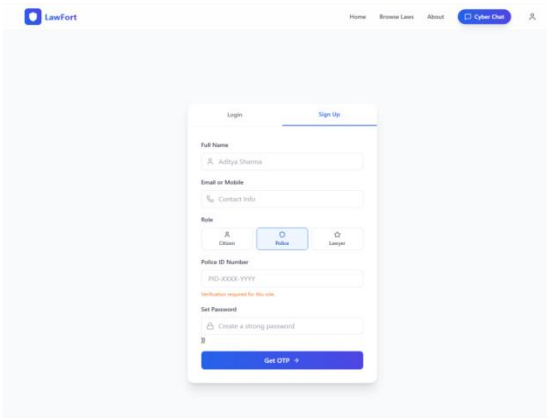
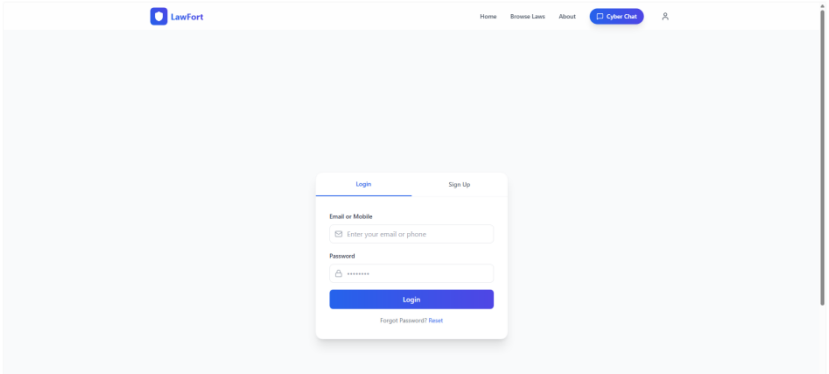


Figure 10: Comparative Performance of AI Models in Legal Query Processing







CONCLUSION AND FUTURE WORK

LawFort AI was created to serve as an intelligent and role-based system to aid in the provision of legal and cyber investigation assistance within the digital governance ecosystem of India. The system is equipped with a hybrid AI based structure which utilizes fuzzy legal search, semantic embeddings, local NLP

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 674-682

models, explainable AI based reasoning and restricted cloud-based LLM's to ensure that the system provides accurate and contextually relevant legal guidance. LawFort AI offers users a variety of options to interact with the system through the use of dynamic natural language interaction and role specific capabilities for citizens, students, legal professionals, and law enforcement officers. Unlike traditional legal portal and rule-based chatbot systems, LawFort AI has been developed to address the major shortcomings associated with existing systems. These include the lack of semantic understanding, the lack of police oriented workflows, inadequate adaptation to new laws such as the DPDP Act 2025, and the lack of support for cybercrime guided investigations. By utilizing a Role Based Access Control (RBAC) model, LawFort AI ensures that there is a complete segregation of general users from police modules. This segregation allows users to safely have access to sensitive investigation workflows, while ensuring that no real-case information is exposed and no confidential information is breached. The Investigation Workflow Generator enables a standardized approach for the cybercrime investigators to follow during the handling of cybercrime cases, and the Phishing Detection Module assists users to enhance their digital safety by identifying malicious URLs. The experimental results demonstrate that the hybrid query engine of LawFort AI improves the accuracy of the queries it processes as compared to single method models. Additionally, user feedback indicates that users are extremely satisfied with regards to the ease of use of the system, clarity of the responses provided by the system and the relevance of the workflows generated by the system. The system was designed using legal compliance and security principles, which clearly demonstrate that an AI-based legal assistant can be both practical and ethical when built with structured constraints, explainability and privacy-by-design principles. Therefore, LawFort AI is providing solutions to bridge the gap between legal complexity and real world usability, supporting legal literacy, cyber awareness and investigative efficiency in a rapidly changing digital legal environment.

REFERENCES

[1] Surden, H. (2014). *Machine Learning and Law.* Washington Law Review, 89(1), 87–115.
[2] Moens, M. F., & Vilares, D. (2022). *Legal Text Analytics: From Information Retrieval to Artificial Intelligence.* Cambridge University Press.
[3] P. N, E. P, M. K, S. P. T, S. K. C and S. K. R, "Enhanced QR CODE Scanning and Blockchain Technology for Drug Packaging System," 2024 International Conference on System, Computation, Automation and Networking (ICSCAN), PUDUCHERRY, India, 2024, pp. 1-5, doi: 10.1109/ICSCAN62807.2024.10894169.
[4] Rajput, D. S., & Arora, A. (2020). Cybercrime Detection using NLP and Machine Learning: A Review. *Journal of Cybersecurity and Privacy*, 1(1), 3–18. https://doi.org/10.3390/jcp1010002
[5] Chalkidis, B., Androutsopoulos, I., & Aletras, N. (2021). Neural Legal Judgment Prediction in English. *Artificial Intelligence and Law*, 29(4), 509–539. https://doi.org/10.1007/s10506-021-09296-3
[6] Ministry of Electronics and Information Technology. (2008). *Information Technology Act, 2000 with Amendments.* Government of India. Available at: https://meity.gov.in
[7] Chalkidis, I., Fergadiotis, M., & Aletras, N. (2020). LEGAL-BERT: The Muppets Straight Out of Law School. *arXiv preprint*, arXiv:2010.02559. Available at: https://arxiv.org/abs/2010.02559
[8] Islam, M. R., & Singh, J. (2023). AI-Based Legal Chatbots for Citizen Services: An Empirical Study. *International Journal of Information Management*, 68. https://doi.org/10.1016/j.ijinfomgt.2022.102557
[9] J. P. R, A. A, M. K, P. N, G. V and A. S. S, "Generalized Discriminate Analysis for Classification Algorithms in a Tuned Machine Learning Model for Steganalysis," 2024 International Conference on System, Computation, Automation and Networking (ICSCAN), PUDUCHERRY, India, 2024, pp. 1-5, doi: 10.1109/ICSCAN62807.2024.10894458.
[10] Singh, R., & Sahu, P. (2021). Artificial Intelligence in Law: Indian Perspective. *International Journal of Law and Information Technology*, 29(4), 391–414. https://doi.org/10.1093/ijlit/eaaa032
[11] Angwin, J., Larson, J., & Mattu, S. (2016). Machine Bias: Risk Assessments in Criminal Sentencing. *ProPublica*. Available at: https://www.propublica.org/ article/machine-bias-risk-assessments-in-criminal-sentencing
[12] SpaCy.io. (2024). *Industrial-Strength Natural Language Processing in Python.* Available at: https://spacy.io
[13] Hugging Face. (2024). *Transformers: State-of-the-Art NLP Models.* Available at: https://huggingface.co
[14] National Crime Records Bureau (NCRB). (2023). *Crime in India – Cybercrime Statistics.* Government of India. Available at: https://ncrb.gov.in
[15] Srujan Surya, K. L., Mark K, E., Surya, K., Tej P, C., & Fathima, A. S. (2025). AI-Powered Interactive Legal Chatbot for the Department of Justice. *International Journal of Computer Learning & Intelligence*, 4(4), 809–817. https://doi.org/10.5281/zenodo.15465000
[16] Tandon, U., & Gupta, N. K. (2025). Informational Privacy in the Age of Artificial Intelligence: A Critical Analysis of India's DPDP Act, 2023. *Legal Issues in the Digital Age*, 6(2), 87–117. https://doi.org/10.17323/2713-2749.2025.2.87.117
[17] Surya, N. A. K., Muthulakshimi, V., & Purushothaman, G. (2025). Towards Intelligent Legal Information Retrieval: A Transformer Based Framework. *International Journal of Scientific Research in Engineering and Modernization (IJSREM).* Available at: https://ijsrem.com
[18] N. Palanivel, K. Madhan, A. Venkatvamsi, G. Madhavan, S. B and L. Priya G, "Design and Implementation of Real Time Object Detection using CNN," 2023 International Conference on System, Computation, Automation and Networking (ICSCAN), PUDUCHERRY, India, 2023, pp. 1-5, doi: 10.1109/ICSCAN58655.2023.10394752.
[19] M. R, N. P, N. L. Christy S, M. K, P. N and M. U, "Integrating CNN and Random Forest Algorithm for Multi Satellite Image Compression in Data Mining," 2024 International Conference on System, Computation, Automation and Networking (ICSCAN), PUDUCHERRY, India, 2024, pp. 1-5, doi: 10.1109/ICSCAN62807.2024.10894190.