Jaya Veeranjaneya Reddy B, 2026, 14:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Clause Guard : An app that lets users to detect loopholes in terms and conditions.

Jaya Veeranjaneya Reddy B[#1], D Nikhil[#2], Ch Rajesh [#3], Mr. C Ram Chandran[#4]

Email: jayveeranjaneya@gmail.com, dabbugottunikhil08@gmail.com
rajeshchennamsetty505@gmail.com.

[#1]23UG Student, Department of Computer Science and Engineering, School of Engineering and Technology,
Dhanalakshmi Srinivasan University, Trichy–621112, Tamil Nadu, India

[#4]Assistant Professor, Department of Computer Science and Engineering,
Dhanalakshmi Srinivasan University, Trichy–621112, Tamil Nadu, India

Abstract : In the rapidly evolving digital ecosystem, users frequently interact with mobile applications, websites, e-commerce platforms, and online services that require acceptance of lengthy Terms and Conditions (T&C), Privacy Policies, and User Agreements. Most users tend to accept these agreements without thoroughly reading or understanding the hidden clauses, legal complexities, data-sharing permissions, subscription traps, liability waivers, and privacy loopholes embedded within them. This creates a significant gap between user awareness and digital consent, often leading to privacy violations, unauthorized data collection, financial exploitation, auto-renewal scams, and misuse of personal information. To address this growing concern, Clause Guard is proposed as an intelligent and user-centric application designed to detect, analyze, and simplify loopholes present in legal agreements of apps and websites. Clause Guard leverages advanced technologies such as Artificial Intelligence (AI), Natural Language Processing (NLP), Machine Learning (ML), and Legal Text Analytics to automatically scan and interpret complex legal documents in real time. The application identifies potentially harmful, suspicious, or manipulative clauses and categorizes them based on risk level, transparency, and user impact. It highlights critical sections related to data privacy, third-party data sharing, hidden charges, subscription auto-renewals, liability disclaimers, intellectual property rights, tracking permissions, and consent manipulation practices. By converting complicated legal terminology into simple and understandable language, the platform enhances digital literacy and empowers users to make informed decisions before accepting agreements.

Keywords- Artificial Intelligence, Deep Learning, NLP, Data Security, Explainable AI.

I. INTRODUCTION

In today's digitally connected world, users rely heavily on mobile applications, websites, social media platforms, cloud services, and e-commerce systems for communication, entertainment, banking, education, and business activities. Before accessing these services, users are usually required to accept lengthy **Terms and Conditions (T&C)** and **Privacy Policies**. However, these legal agreements are often written in complex legal language, making them difficult for ordinary users to understand. As a result, most individuals accept these policies without carefully reading them, unknowingly granting permissions that may compromise their privacy, security, and consumer rights.

This lack of awareness has become a major issue in the modern digital environment. Many organizations include hidden clauses related to excessive data collection, third-party data sharing, auto-renewal subscriptions, targeted advertising, tracking permissions, liability limitations, and consent manipulation techniques within their agreements. Such

loopholes can expose users to privacy breaches, financial risks, unethical data exploitation, and cyber threats. With the rapid growth of digital platforms and online services, there is an increasing need for a smart solution that can help users identify and understand these hidden risks before accepting any agreement.

To address this challenge, **Clause Guard** is introduced as an innovative AI-powered application designed to detect loopholes and risky clauses in the Terms and Conditions of apps and websites. The application acts as a digital legal assistant that scans, analyzes, and simplifies complicated legal documents into user-friendly summaries. By utilizing advanced technologies such as **Artificial Intelligence (AI)**, **Natural Language Processing (NLP)**, **Machine Learning (ML)**, and **Text Mining**, Clause Guard can automatically identify suspicious, misleading, or potentially harmful clauses in real time.

The system focuses on enhancing digital transparency and promoting informed consent by highlighting critical information related to data privacy, user rights, hidden charges, subscription policies, cookie tracking, and security permissions. It categorizes clauses based on risk level and provides alerts or warnings whenever a policy contains potentially dangerous or unethical terms. This enables users to make informed decisions about whether to accept or reject an agreement.

II. RELATED WORK

Several browser extensions and privacy-focused applications have also been introduced to enhance digital transparency. Tools like automated cookie analyzers, permission trackers, and privacy assistants notify users about excessive permissions requested by websites or mobile applications. These tools contribute to online security awareness by warning users about suspicious tracking activities and unsafe data-sharing practices. However, their functionality is generally limited to permission monitoring and does not include comprehensive legal clause analysis or risk-based classification.

Research in the field of **Legal Technology (LegalTech)** has further accelerated the development of intelligent contract analysis systems. AI-powered legal review tools are capable of performing document classification, contract comparison, anomaly detection, and legal compliance verification. Many enterprise-level solutions are used by law firms and organizations to automate contract management processes. Despite their efficiency, such systems are often expensive, complex, and designed primarily for legal professionals rather than general users. They may not specifically focus on consumer-oriented digital agreements such as website terms and conditions or app privacy policies.

Recent advancements in **Machine Learning (ML)** and **Explainable Artificial Intelligence (XAI)** have enabled the creation of more transparent and interpretable decision-making systems. Researchers have proposed models capable of assigning risk scores to legal clauses and detecting deceptive patterns in online agreements. Some studies also explore sentiment analysis and behavioral prediction techniques to identify manipulative language intended to influence user consent. These approaches are highly relevant to Clause Guard, as they provide the technical foundation for automated loophole detection and intelligent risk assessment.

Although existing systems contribute significantly toward legal automation and privacy protection, there remains a major gap in providing a unified, user-friendly, and real-time solution capable of detecting loopholes, simplifying legal content, categorizing risks, and educating users simultaneously. Most current applications either focus solely on readability, compliance verification, or permission tracking. Clause Guard addresses these limitations by combining AI-driven clause detection, semantic analysis, privacy risk assessment, legal simplification, and transparency scoring into a single integrated platform designed specifically for ordinary internet users.

Therefore, the proposed system builds upon previous advancements in AI, NLP, cybersecurity, and LegalTech while introducing a more comprehensive and accessible approach

International Journal of Science, Engineering and Technology
An Open Access Journal

for protecting users against hidden digital exploitation and unfair online agreements.

III. PROPOSED SYSTEM

The proposed system consists of multiple interconnected modules that work together to provide efficient loophole detection and legal simplification. The first module is the **Document Collection and Extraction Module**, which gathers Terms and Conditions and Privacy Policy content from websites or mobile applications. This module supports automated text extraction from URLs, web pages, and uploaded documents.

The second module is the **Natural Language Processing Engine**, which preprocesses and analyzes the extracted text using tokenization, stop-word removal, stemming, named entity recognition, and semantic analysis. This module identifies important legal patterns and classifies clauses into categories such as privacy risks, payment policies, tracking permissions, user obligations, and liability terms.

The third module is the **Risk Detection and Classification Module**, where machine learning algorithms analyze suspicious patterns and assign risk scores to individual clauses. The system compares detected content with a predefined database of known deceptive practices, unfair contractual terms, and privacy violations. Clauses that indicate potential exploitation or unethical practices are highlighted using warning indicators and transparency ratings.

Another important component is the **Legal Simplification Module**, which converts complicated legal language into simple and user-friendly explanations. This feature ensures that users without legal knowledge can easily understand the meaning and consequences of specific clauses. The application also generates summarized insights, recommendations, and alert notifications for high-risk agreements.

The proposed system further includes a **User Interface and Dashboard Module**, which provides an interactive environment where users can upload agreements, view clause analysis reports, monitor privacy scores, and receive personalized security recommendations. The application can also function as a browser extension or mobile assistant to perform instant analysis while users browse websites or install applications.

Additionally, Clause Guard supports compliance analysis based on regulations such as **GDPR (General Data Protection Regulation)** and other digital privacy standards. This enables users to identify whether a platform follows ethical data-handling practices and legal compliance requirements. The system continuously improves its detection capability through machine learning-based model training and database updates.

IV. METHODOLOGY

The methodology of the proposed system, **Clause Guard**, is designed to develop an intelligent and automated solution for detecting loopholes, hidden risks, and unfair clauses present in the Terms and Conditions (T&C) and Privacy Policies of websites and mobile applications. The system begins with the collection and extraction of legal documents from websites, applications, or uploaded files using automated text extraction and web scraping techniques. Once the legal content is obtained, preprocessing techniques such as tokenization, stop-word removal, stemming, lemmatization, sentence segmentation, and keyword extraction are applied to clean and convert the raw text into a machine-readable format. After preprocessing, the system utilizes advanced **Natural Language Processing (NLP)** techniques including semantic analysis, Named Entity Recognition (NER), sentiment analysis, dependency parsing, and text classification to identify important legal patterns and clauses related to data sharing, third-party access, hidden charges, auto-renewal subscriptions, tracking permissions, liability disclaimers, and privacy risks. The extracted clauses are then analyzed using **Machine Learning (ML)** algorithms trained on datasets containing fair and unfair contractual practices to classify the detected clauses into low-risk, medium-risk, and high-risk categories. The system assigns risk scores based on factors such as ambiguous

language, manipulative wording, lack of transparency, forced consent mechanisms, and potential data exploitation indicators. To improve user understanding, Clause Guard incorporates an AI-driven legal simplification and summarization module that converts complex legal terminology into plain and user-friendly language while generating concise summaries, alerts, recommendations, and transparency ratings. Additionally, the system verifies whether the analyzed agreements comply with international privacy standards and regulations such as **GDPR (General Data Protection Regulation)** and consumer protection policies. The final analysis results are displayed through an interactive dashboard or browser extension where users can view highlighted risky clauses, privacy scores, warning notifications, and simplified explanations in real time while accessing websites or installing applications. Furthermore, the system continuously updates its loophole database and retrains its machine learning models using newly identified deceptive patterns and user feedback to improve detection accuracy and adaptability against evolving digital policies. By integrating **Artificial Intelligence (AI)**, **Cybersecurity**, **LegalTech**, **Semantic Text Analysis**, **Privacy Risk Detection**, **Explainable AI**, **Automated Legal Document Processing**, and **Digital Privacy Protection**, the methodology of Clause Guard provides an effective and user-centric approach for improving transparency, informed consent, and online security in the modern digital ecosystem.

V. SYSTEM ARCHITECTURE

The system architecture of **Clause Guard** is designed to provide an intelligent, scalable, and automated platform for detecting loopholes and hidden risks in the Terms and Conditions (T&C) and Privacy Policies of websites and mobile applications. The architecture consists of multiple interconnected modules that work together to perform document extraction, legal text processing, risk analysis, clause classification, and user-friendly result visualization. The overall architecture integrates advanced technologies such as **Artificial Intelligence (AI)**, **Natural Language Processing (NLP)**, **Machine Learning (ML)**, and **Cybersecurity Mechanisms** to ensure accurate loophole detection and efficient legal document analysis.

The architecture begins with the **User Interface Layer**, where users interact with the system through a mobile application, web application, or browser extension. Users can upload legal documents, paste URLs, or directly scan website policies in real time. This layer provides features such as policy scanning, clause highlighting, privacy score display, risk alerts, and simplified legal summaries. The interface is designed to be user-friendly and accessible for both technical and non-technical users.

The next component is the **Data Collection and Extraction Layer**, responsible for gathering Terms and Conditions and Privacy Policy documents from websites, apps, and uploaded files. This module uses web scraping, API integration, and document parsing techniques to extract legal text while maintaining the structure and formatting of clauses. The extracted content is temporarily stored in the system database for further processing.

After extraction, the legal content is passed to the **Text Preprocessing Layer**, where the raw text is cleaned and converted into a machine-readable format. This layer performs operations such as tokenization, stop-word removal, stemming, lemmatization, sentence segmentation, and keyword extraction. Preprocessing improves the efficiency and accuracy of subsequent NLP and Machine Learning operations.

The processed text is then forwarded to the **Natural Language Processing (NLP) Engine**, which acts as the core analytical component of the system. This module performs semantic analysis, Named Entity Recognition (NER), text classification, sentiment analysis, and contextual understanding of legal clauses. The NLP engine identifies sensitive and important clauses related to privacy risks, third-party data sharing, subscription traps, hidden charges, liability

Jaya Veeranjaneya Reddy B, 2026, 14:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

limitations, tracking permissions, and user consent mechanisms.

The identified clauses are analyzed in the **Machine Learning-Based Risk Detection Layer**, where trained ML models classify clauses according to their severity and potential risk level. The system compares the extracted clauses against a database of known deceptive patterns, unfair contractual practices, and privacy violations. Risk scores are assigned to each clause based on transparency, ambiguity, manipulation indicators, and data exploitation potential. Clauses are categorized into low-risk, medium-risk, or high-risk groups to help users quickly understand the seriousness of the agreement.

Another important component is the **Legal Simplification and Summarization Layer**, which converts complex legal terminology into plain and understandable language using AI-driven summarization techniques. This module generates concise summaries, warnings, recommendations, and transparency ratings to improve user awareness and digital literacy.
The system also includes a **Compliance Verification Layer** that checks whether the analyzed agreements comply with international standards and regulations such as **GDPR (General Data Protection Regulation)** and digital privacy policies. This module helps users identify unethical or non-compliant practices within online agreements.

All processed information, clause classifications, risk scores, and user interaction data are stored in the **Database Management Layer**, which maintains datasets of legal documents, loophole patterns, user feedback, and machine learning training data. Continuous updates and retraining mechanisms ensure that the system adapts to newly emerging deceptive practices and evolving legal standards.

Finally, the **Result Visualization and Alert Layer** presents the analyzed results to users through dashboards, notifications, highlighted clauses, privacy ratings, and risk indicators. Users receive real-time alerts whenever suspicious or potentially harmful clauses are detected, enabling informed decision-making before accepting agreements.

Thus, the system architecture of Clause Guard combines **AI-powered legal analysis**, **intelligent document processing**, **privacy risk assessment**, and **cybersecurity techniques** into a unified framework that promotes digital transparency, informed consent, and user data protection in modern online platforms
interpretability, and trust in AI-assisted diagnosis. The overall architecture of the proposed system is illustrated in Fig. 1, while the explainability and visualization process using Grad-CAM is shown in Fig. 2

```
clauseguard/
├── backend/
│   ├── app/
│   │   ├── routes/          # API endpoints
│   │   ├── services/        # Risk analysis & document processing
│   │   └── config.py        # Configuration
│   ├── requirements.txt     # Dependencies
│   └── run.py               # Flask server
├── frontend/
│   ├── src/
│   │   ├── components/      # React components
│   │   ├── pages/           # Page layouts
│   │   ├── services/        # API client
│   │   └── index.js         # Entry point
│   └── package.json         # Dependencies
└── README.md
```

VI. RESULTS AND DISCUSSION

The implementation of **Clause Guard** successfully demonstrated the ability to detect loopholes, hidden clauses, and privacy risks present in the Terms and Conditions (T&C) and Privacy Policies of various websites and mobile applications. The system effectively analyzed legal documents using **Artificial Intelligence (AI)**, **Natural Language Processing (NLP)**, and **Machine Learning (ML)** techniques, providing users with simplified explanations, risk classifications, and transparency ratings. The obtained results indicate that the proposed

system can significantly improve user awareness and help individuals make informed decisions before accepting online agreements.

During testing, the application was evaluated using multiple legal documents collected from social media platforms, e-commerce websites, subscription-based services, and mobile applications. The system successfully extracted important legal clauses related to data sharing, third-party access, tracking permissions, hidden subscription policies, liability disclaimers, and auto-renewal conditions. The NLP engine accurately identified legal patterns and semantic relationships within the documents, while the Machine Learning models effectively classified clauses into low-risk, medium-risk, and high-risk categories.

The results showed that Clause Guard achieved high efficiency in detecting potentially harmful clauses that are often ignored by users due to the complexity of legal language. The legal simplification module generated concise and user-friendly explanations, enabling users without legal expertise to understand the meaning and consequences of specific clauses. This feature greatly improved accessibility and enhanced digital awareness among users. The system also generated real-time alerts and warnings whenever suspicious or manipulative clauses were identified, thereby increasing transparency and reducing the chances of uninformed consent.

The risk assessment mechanism proved effective in identifying loopholes associated with excessive data collection, invasive tracking permissions, hidden charges, and unfair contractual obligations. The transparency scoring feature allowed users to compare agreements based on their privacy and security risks. Furthermore, the compliance verification module successfully detected whether agreements followed international privacy standards such as **GDPR (General Data Protection Regulation)** and consumer protection guidelines.

The discussion of the obtained results highlights that existing systems primarily focus on legal document summarization or permission tracking, whereas Clause Guard integrates loophole detection, clause classification, legal simplification, and privacy risk assessment within a single platform. This integration provides a more comprehensive solution for protecting users against unethical digital practices and hidden legal exploitation. The use of Explainable AI techniques also improved the interpretability of the system's decisions, allowing users to understand why specific clauses were categorized as risky.

Although the system produced highly promising results, certain challenges were observed during implementation. Some legal documents contained highly ambiguous and context-dependent language, which occasionally affected classification accuracy. Variations in legal writing styles across different websites and applications also created difficulties in standardizing clause analysis. However, continuous Machine Learning model training and database updates can further improve the system's adaptability and detection performance over time.

The results confirm that Clause Guard can serve as an effective tool for enhancing **digital transparency**, **online security**, and **user privacy protection**. The proposed system contributes significantly to the domains of **Cybersecurity**, **LegalTech**, **AI-driven Legal Analysis**, and **Consumer Rights Protection** by helping users identify hidden risks and understand legal agreements more clearly. Future enhancements may include multilingual support, advanced predictive analytics, voice-assisted legal summaries, and integration with enterprise-level compliance monitoring systems.

Overall, the implementation and evaluation of Clause Guard demonstrate that intelligent automation combined with AI-powered legal analysis can play a crucial role in promoting informed consent, ethical digital practices, and safer online interactions in the modern digital ecosystem.

Jaya Veeranjaneya Reddy B, 2026, 14:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

VII. PERFORMANCE EVALUATION AND COMPARATIVE ANALYSIS

The performance evaluation of Clause Guard was conducted to measure the efficiency, accuracy, reliability, and usability of the proposed system in detecting loopholes and hidden risks within the Terms and Conditions (T&C) and Privacy Policies of websites and mobile applications. The evaluation focused on analyzing the system's capability to identify suspicious clauses, simplify legal language, classify risks, and provide real-time alerts using advanced technologies such as Artificial Intelligence (AI), Natural Language Processing (NLP), and Machine Learning (ML).

The system was tested using a large collection of legal agreements obtained from social media applications, e-commerce platforms, subscription-based services, and online websites. Different categories of clauses related to data privacy, third-party data sharing, tracking permissions, hidden subscription policies, liability disclaimers, auto-renewal conditions, and excessive permissions were included in the evaluation dataset. The extracted clauses were manually verified and compared with the system-generated results to measure the accuracy of loophole detection and risk classification.

The performance evaluation demonstrated that Clause Guard achieved high accuracy in identifying risky and manipulative clauses present in legal agreements. The NLP engine effectively processed complex legal language using semantic analysis, Named Entity Recognition (NER), and text classification techniques, while the Machine Learning model accurately categorized clauses into low-risk, medium-risk, and high-risk levels. The system also showed efficient execution time and real-time processing capability, allowing users to receive instant analysis and alerts while accessing websites or installing applications.

The legal simplification module significantly improved readability by converting complicated legal terminology into plain and understandable language. User testing revealed that individuals without legal expertise could understand policy summaries and privacy risks more effectively using Clause Guard compared to traditional legal documents. The transparency scoring and warning notification features further enhanced user awareness and supported informed digital consent.

For comparative analysis, Clause Guard was compared with existing privacy policy analyzers, legal summarization tools, browser-based permission trackers, and conventional compliance verification systems. Existing systems mainly focused on limited functionalities such as document summarization, cookie tracking, or privacy compliance monitoring. Most traditional tools lacked integrated loophole detection, automated risk scoring, semantic interpretation, and user-friendly legal simplification.

- More accurate loophole detection using AI-driven semantic analysis
- Real-time identification of hidden risks and manipulative clauses
- Automated risk classification and transparency scoring
- Simplified legal explanations for non-technical users
- Integrated privacy compliance verification
- User-friendly interface with instant alerts and recommendations
- Continuous learning through Machine Learning-based model updates

VIII. FUTURE WORK

One of the major future improvements involves enhancing the **Artificial Intelligence (AI)** and **Machine Learning (ML)** models used for clause detection and risk classification. The current system can be upgraded with advanced **Deep Learning** and **Transformer-based NLP models** such as BERT and GPT-based legal language processing systems to improve contextual understanding of highly complex legal documents. This enhancement will allow the application to identify ambiguous, hidden, and

manipulative clauses with greater precision and reduced false-positive rates.

Another important future update is the implementation of **multilingual support**. At present, many online agreements are available in different regional and international languages, which limits accessibility for global users. Future versions of Clause Guard can incorporate multilingual Natural Language Processing capabilities to analyze legal documents in multiple languages while still providing simplified explanations in the user's preferred language. This feature will significantly improve inclusiveness and global usability.

The system can also be extended with **real-time browser integration and mobile OS-level scanning**. Future updates may allow Clause Guard to automatically analyze Terms and Conditions whenever users install applications, sign up for services, or visit websites. Instant popup notifications and AI-generated privacy warnings can help users make informed decisions without manually uploading documents. Integration with popular browsers and app marketplaces would further improve real-time transparency and online safety.

Another enhancement includes the addition of a **personalized privacy recommendation engine**. Using user behavior analysis and preference settings, the system can provide customized suggestions regarding risky permissions, data-sharing practices, and secure alternatives. Users may also receive comparative privacy ratings between similar applications or services, helping them choose safer digital platforms.

Future work may also include the development of a **Blockchain-based audit and transparency mechanism** for secure storage of analyzed agreements and clause history. Blockchain integration can improve trust, prevent tampering of legal analysis reports, and ensure transparency in privacy evaluations. Additionally, decentralized verification systems can be introduced to improve accountability and authenticity in policy assessments.

REFERENCES

[1] Yann LeCun, Yoshua Bengio, and Geoffrey Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436–444, 2015.
[2] Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," in Proceedings of NAACL-HLT, pp. 4171–4186, 2019.
[3] Ashish Vaswani et al., "Attention Is All You Need," in Advances in Neural Information Processing Systems (NeurIPS), pp. 5998–6008, 2017.
[4] Daniel Jurafsky and James H. Martin, *Speech and Language Processing*, 3rd ed., Pearson, 2021.
[5] Lorrie Faith Cranor, "Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice," Journal on Telecommunications and High Technology Law, vol. 10, no. 2, pp. 273–307, 2012.
[6] Solon Barocas and Andrew D. Selbst, "Big Data's Disparate Impact," California Law Review, vol. 104, no. 3, pp. 671–732, 2016.
[7] Sandra Wachter, Brent Mittelstadt, and Luciano Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation," International Data Privacy Law, vol. 7, no. 2, pp. 76–99, 2017.
[8] European Union, "General Data Protection Regulation (GDPR)," Official Journal of the European Union, Regulation (EU) 2016/679, 2016.
[9] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2010.
[10] Batya Friedman, Peter H. Kahn Jr., and Alan Borning, "Value Sensitive Design and Information Systems," in Human-Computer Interaction and Management Information Systems, pp. 348–372, 2006.
[11] Tom M. Mitchell, *Machine Learning*, McGraw-Hill, 1997.
[12] Ian Goodfellow, Yoshua Bengio, and Aaron Courville, *Deep Learning*, MIT Press, 2016.

ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

[13] Cynthia Dwork, "Differential Privacy," in Proceedings of ICALP, pp. 1–12, 2006.
[14] Karen Yeung, "Algorithmic Regulation: A Critical Interrogation," Regulation & Governance, vol. 12, no. 4, pp. 505–523, 2018.
[15] Luciano Floridi and Josh Cowls, "A Unified Framework of Five Principles for AI in Society," Harvard Data Science Review, vol. 1, no. 1, 2019.