International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 05 | May 2023 www.irjet.net p-ISSN: 2395-0072

IoT, Big Data and AI Applications in the Law Enforcement and Legal System: A Review

Md. Shahin Kabir[1], Mohammad Nazmul Alam[2]

[1]*Assistant Professor, Department of Law, Raffles University, Neemrana, Rajasthan, India*
[2]*Assistant Professor, Department of Computer Applications, Guru Kashi University, Talwandi Sabo, Bathinda, India*

Abstract - *The use of technology in the legal system is not a new phenomenon. From the invention of the printing press in the 15th century to the development of the internet in the 20th century, technological advancements have played a significant role in shaping the legal system. However, in recent years, the pace of technological development has accelerated, and the latest technologies such as the IoT, big data, and AI are transforming the legal system in unprecedented ways. This paper aims to explore the applications of these technologies in the legal system and the impact they have on legal proceedings. It focuses on the applications of IoT, Big Data, and AI technologies in the legal system. The paper does not provide a detailed analysis of the legal system but rather focuses on the role of these technologies in improving the efficiency and effectiveness of law enforcement and the legal system. The paper provides a comprehensive review of the literature on the use of IoT, Big Data, and AI in the legal system and presents some of the applications, challenges, and opportunities that arise from their implementation including its ethical considerations. We analyze the current state of research on this topic and identify key trends and future directions.*

Keywords: *IoT, Big Data, AI, legal system, challenges, opportunities*

I. INTRODUCTION

In recent years, the integration of the Internet of Things (IoT), Big Data (BD), and Artificial Intelligence (AI) technologies has significantly transformed various sectors, including the legal system. The legal system is a complex and time-consuming process that involves various stakeholders, including judges, lawyers, law enforcement agencies, and citizens. The integration of IoT, Big Data, and AI technologies in the legal system can help streamline the process and make it more efficient and effective.

Research contribution: This paper presents the literature review to study the contemporary status of modern technology approaches in Law enforcement and the legal system. The paper makes the following contributions:

- Present a survey of the current literature on emerging technology in law
- Explain the different applications in law enforcement and the legal system
- Explain the proposed architectural model of legal expert systems
- Discusses the benefits of using the technology in law
- Explain the challenges and opportunities of implementation of the technology in the law field.
- Provides the open issues for future directions in this field.

Organization of the Research: The rest of the paper is organized as follows: Section II explains the literature survey of the current study in this field. Different applications of IoT, Big data, and AI will be presented in section III. We present proposed knowlwdge base architecture of legal expert systems in section IV. Section V presents implementation challenges. Section VI provides the future directions and, we conclude in section VII.

II. LITERATURE REVIEW

A. Literature Selection Process

To have a clear picture of emerging technology in the law environment, this section provides an extensive literature review of the research on IoT, Big data, and AI in law enforcement and legal system. The paper collection strategy consists of three main stages:

Stage 1

Define the keywords to search relevant papers from electronic databases (ProQuest, IEEE Xplorer, and Science Direct). Considering the alternatives and other synonyms of essential components of the keyword, the subsequent searching string was defined: *("IoT" OR "Big Data" OR "AI" OR "Expert Systems" OR "Machine Learning") AND ("Law Enforcement" OR "Legal System" OR "Courtroom")*

Stage 2

Select papers based on the title, publication year, and language written in English. To make sure that only high-quality publications were included in the study, we spotlight journal publications and conference papers

published by Elsevier, IEEE, Springer, ACM, and Wiley. Moreover, opinion-driven reports such as editorials, commentaries, and letters were excluded.

Stage 3

Review the abstracts and full texts of the selected papers to verify the relevance of these papers. The cited information, abstracts, and keywords of the papers were recorded for further analysis. Finally, 20 papers published between 2020 and 2023 were extracted through the three phases, as shown in Table I.

B. Overview of Existing Research on IoT, Big Data, and AI in Legal System

The paper [1] discusses the potential use of big data analytics in the legal industry, specifically in litigation. It highlights the benefits of using big data tools for tracking cases and predicting the success rate of appeals, which can help clients, make informed decisions about whether to continue with a case or cut their losses. The paper also suggests that big data analytics can be used to improve legal research and case preparation, ultimately leading to better outcomes for clients. Overall, the paper contributes to the growing body of literature on the use of big data in the legal industry and provides insights into how this technology can be leveraged to improve legal services. This paper [2] discusses the legal issues related to data protection law in the context of the Internet of Things (IoT) phenomenon. Highlighting the privacy and security risks associated with the use of IoT technologies that often cannot guarantee an acceptable security level. Identifying the main risk for privacy in the IoT as profiling, this allows identifying natural persons through their personal information. Examining the potential consequences for data security and liability in the IoT system allows transferring data, including personal data, on the Internet. Evaluating the technical structure of the blockchain to analyze the law impact and the legal issues on data protection and privacy in the context of the evolving IoT ecosystem. Discussing the new European General Data Protection Regulation (GDPR) that will apply from 25 May 2018 and its introduction of Data Protection Impact Assessment (DPIA), data breach notification, and very high administrative fines in respect of infringements of the Regulation. Providing a correct law analysis to evaluate the risks and prevent the wrong use of personal data and information in the IoT. This paper [3] highlights the need for a legal framework to be established before the IoT is fully operable. Suggesting that a self-regulatory approach may be preferable for establishing this legal framework. Discussing the potential positive and negative impacts of the IoT in various areas, including global trade, healthcare, environmental concerns, and labor standards. Emphasizing the importance of ensuring the security and privacy of users in the IoT, and identifying legal barriers that may stand in the way of the IoT's operation and need to be addressed. This paper [4] discusses the need for a regulatory framework for the Internet of Things (IoT) and highlights the efforts of the European Union in studying the regulatory needs of the IoT. The paper emphasizes the importance of implementing an independently managed decentralized multiple-root system and the establishment of basic governance principles for the IoT. It also suggests that traditional Internet Governance concepts are not suitable for the IoT and that the development of decentralized architectures and the promotion of a shared network of multistakeholder governance for the IoT is needed. Overall, the paper contributes to the ongoing discussion on the regulatory challenges of the IoT. This paper [5] discusses the potential impact of machine learning, a type of artificial intelligence, on the legal profession. It explores how machine learning can improve decision-making in the legal function and how this can benefit businesses. The paper also highlights the need for corporate legal strategists to drive and sustain change in the intersection of law, business, and technology. Overall, the paper aims to bring attention to the relevance of today's transformations to the legal function and encourage business leaders to elevate lawyers to contribute further to corporate strategies and operations. The contributions of this paper [6] are: Identifying the legal challenges of the Internet of Things (IoT) concerning cybersecurity. Highlighting the security concerns regarding consumers' use of IoT devices such as enabling unauthorized access, misuse of personal identification, and expediting attacks on other systems. Addressing the legal challenges that would impede the development, growth, adoption, and use of IoT technology. Providing a comprehensive analysis of the existing security, privacy, and cybersecurity laws. Discussing the potential risks associated with the universality of wireless networks enabling continuous streams of data from smart devices to be sent, processed, and stored in the cloud. This paper [7] discusses the development of computer programs called legal expert systems, which provide advice on the application of the law to a user's particular legal problem. The paper explains the characteristics of expert systems and their importance in the second wave of artificial intelligence research. The paper also discusses the components of a legal expert system, including the inferencing mechanism, knowledge base, application developer interface, user interface, and user-supplied problem facts. The paper's contribution is to provide an overview of the development of legal expert systems and their potential applications in the field of law. The contributions of this paper [8] are: Exploring the complexities and considerations underlying a privacy and cybersecurity regulatory approach for consumer IoT in Part I. Identifying potential regulatory opportunities and models by exploring existing ex-ante cybersecurity and privacy statutes in the United States and the European Union (EU) in Part III. Providing insights into the potential

risks to consumers related to personal privacy, safety issues, and potential for discriminatory data in the field of consumer IoT. Examining how existing products liability, common law civil recovery under contracts or torts schemes, and due process procedures will apply to these products and the data they process. Balancing market needs for innovation with consistent oversight for IoT manufacturers and distributors in the United States. The contributions of this paper [9] are: Defining the field of research of the report, which is the intersection of data protection and Artificial Intelligence (AI). Proposing a regulatory framework for AI based on a values-based approach and risk assessment and management. Highlighting the importance of extending European regulatory leadership in the field of data protection to AI. Emphasizing the historical roots of European data protection in considering the potentially adverse consequences of data processing technologies. The contributions of this paper [10] are: Discussing the use of expert systems as decision aids for law students and lawyers. Surveying some of the expert systems designed for law. Presenting EVIDENT, an expert system for determining the admissibility of evidence. The contributions of this paper [11] are: Investigating the concept of the Internet of Things (IoT) and its pros and cons as used by experts and researchers. Providing recommendations on how to protect privacy and reap the benefits of IoT. Arguing that this study will positively contribute to the academic discussion by looking at one of the most contentious aspects of IoT (privacy challenges) that could slow down its progress. The contributions of this paper [12] are: To explain the connection between law and legal science with the phenomenon of Big Data. To provide a narrow and simple definition of Big Data as the new technical ways, solutions, and methods of producing, collecting, processing, and using data that can change society, including the law. To collect and systematize arguments about the impact of Big Data on law, legal regulation, lawyering, and legal science. The paper [13] explains the impact of Artificial Intelligence on the legal profession. It provides a brief explanation of what Artificial Intelligence is and its history in the legal industry. The paper also discusses the pros and cons of AI in the legal industry and concludes that the advantages of AI outweigh the cons. The contribution of the paper is to provide a comprehensive understanding of the impact of AI on the legal profession for laymen and beginners in the field. The paper [14] provides a basic understanding of IoT devices and their components. Highlighting the challenges that arise when IoT technologies are introduced into the justice system. Discussing the potential increase in IoT investigations and legal cases involving crime, privacy, security, and liabilities. Emphasizing the importance of justice system professionals and law enforcement personnel learning how to deal with electronic evidence collected from IoT devices. The contributions of this paper [15] are: Questioning the "Big Data" paradigm in the legal system. Highlighting the limitations of large-scale data analysis in making behavioral prescriptions using averages without considering the extremes and underlying heterogeneity in beliefs and judgments. Reframing the potential uses of Big Data in the legal system and questioning the widespread optimism about its illusory predictive power. The paper [16] discusses the importance of Case-Based Reasoning (CBR) in legal practice and presents five different paradigms of CBR. It compares them based on various criteria and argues that CBR can supplement rule-based expert systems, improve legal data retrieval systems, and contribute to cognitive science models. The contributions of this paper are to synthesize important CBR research developments, assess the implications of CBR for building law-related expert systems and AI programs to model legal reasoning, and argue that AI/CBR work in the legal domain can make an important contribution to the development of practical systems for the legal profession and to practical and intellectual advances in AI and cognitive modeling. The contributions of this paper [17] are: Examining the changing legal cybersecurity environment in the context of the Internet of Things (IoT). Discussing selected applicable international regulations related to IoT security. Proposing alternative approaches to addressing the security issues arising in the IoT. The main contribution of this paper [18] is to propose the development of a legal expert system for people to solve their legal troubles related to immovable property acquisition. The paper discusses the traditional model of legal reasoning, the proposed approach by expert systems, various logical components, and types of legal inference techniques to automate legal tasks. The paper also highlights the importance of the knowledge base module in expert systems, which consists of information provided by experts and follows either forward-chain or backward-chain inference techniques. The paper [19] introduces Expert Systems in Law and their potential benefits, characterizes them, and differentiates them from Artificial Intelligence. It surveys current projects in Artificial Intelligence and Legal Reasoning and advocates for jurisprudential rigor in building Expert Systems in Law. The paper discusses legal knowledge acquisition, representation, and utilization, identifies directions for further research, and describes an interdisciplinary research project at the University of Oxford. The contributions of this paper [20] are that it discusses legal analysis systems that use AI techniques to solve legal problems, distinguishes between two categories of legal analysis systems, focuses on legal expert systems, proposes an approach that incorporates both rule-based and case-based knowledge representation, and argues that such an approach can form the basis of an effective and useful legal expert system.

TABLE I. ANALYSIS THE LITERATURE SURVEY OF LEGAL SYSTEM

Research paper	Main topic	Technique	Outcomes
Fina. S. et al. [1]	"Big data & litigation: Analyzing the expectation of lawyers to provide big data predictions when advising clients"	Big data	Improve legal research, Make informed decisions about whether to continue with a case or cut their losses.
Fabiano. N. [2]	"Internet of Things and the Legal Issues Related to the Data Protection Law According to the new European General Data Protection Regulation"	IoT	Prevent a mistaken exploit of personal data and information
Weber, Romana [3]	"Internet of Things-Legal Perspectives"	IoT	Identify legal barriers to operating fully IoT service
Weber, Rolf H. [4]	"Internet of things - Need for a new legal environment?"	IoT	Point out regulatory challenges of the IoT
Tung, Kenneth [5]	"AI, the internet of legal things, and lawyers"	Machine learning	Provide intersection law, business, and technology
Chike, Chike Patrick [6]	"The Legal Challenges of Internet of Things"	IoT	Identify legal security and privacy challenges in IoT.
Greenleaf, Graha [7]	"Legal expert systems-robot lawyers? An introduction to knowledge-based applications to law"	Expert systems	Provide an overview of the development of legal expert systems and their potential applications in the field of law
Tschider, Charlotte A [8]	"Regulating the Internet of Things: Discrimination, privacy, and cyber security in the artificial intelligence age"	IoT, AI	Exploring the complexities and considerations underlying a privacy and cyber security regulatory approach for consumer IoT.
Alessandro. M. [9]	"Artificial Intelligence and Data Protection: Challenges and Possible Remedies"	AI	Proposing a regulatory framework for AI based on a values-based approach and risk assessment and management.
Jay. L. [10]	"Expert systems in law: A survey and case study"	Expert systems	Presenting EVIDENT, an expert system for determining the admissibility of evidence.
Sidi Mohamed Sidi Ahmed [11]	"The concept of Internet of Things and its challenges to privacy"	Internet of Things	Providing recommendations on how to protect privacy and reap the benefits of IoT.
ZSOLT ZŐDI [12]	"Law and Legal Science in the Age of Big Data"	Big data	Explore the impact of big data in legal science
Rishabh Srivastava [13]	"Artificial Intelligence in the Legal Industry: A Boon or a Bane for the Legal Profession"	AI	Explore the impact of AI on the legal profession
Felix Uribe [14]	"An Introduction to the Internet of Things (IoT) for Justice System and Law Enforcement Professionals"	IoT	Introduce the uses of IoT in the reinforcement and legal profession
Caryn D. et al.[15]	"The Law and Big Data"	Big data	Point out the illusory predictive power of big data in the legal system.
Ashley, K. D. [16]	"Case-Based Reasoning and its Implications for Legal Expert System"	AI	Develop expert systems for the legal profession
Rolf H. Weber et al.[17]	"Cybersecurity in the Internet of Things: Legal aspects"	IoT	Proposing alternative approaches to addressing the security issues arising in the IoT.

Venkateswarlu Naik. M. et al. [18]	"Building a Legal Expert System for Legal Reasoning in Specific Domain Survey"	Expert systems	Proposing a legal expert system to automate legal tasks.
Susskind, R. E. [19]	"Expert Systems in Law: A Jurisprudential Approach to Artificial Intelligence and Legal Reasoning"	Expert system	Building expert systems in law
Popple, J.[20]	"Legal Expert Systems: The Inadequacy of a Rule-Based Approach"	AI	Focuses on legal expert systems, proposes an approach that incorporates both rule-based and case-based knowledge representation

III. IoT, Big Data, and AI Applications in Legal System

IoT, big data, and AI applications can significantly impact the legal system by improving efficiency, accuracy, and decision-making processes. Here we explain how these technologies are applied in the legal domain [21-23].

A) IoT Application in Legal System

The Internet of Things (IoT) technology has the potential to revolutionize various industries, including the legal domain. Here are some applications of IoT in the legal sector.

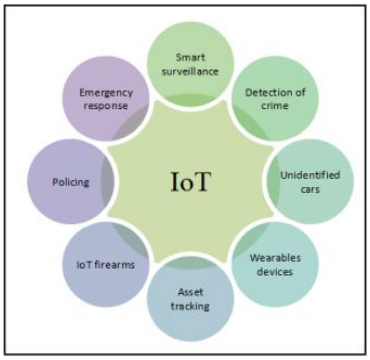

Fig.1. IoT Applications

1) Smart Surveillance

IoT devices such as cameras, sensors, and drones can be used to monitor public spaces, buildings, and critical infrastructure including traffic, providing real-time video feeds and data to law enforcement agencies.

2) Asset tracking

IoT devices can be used to track and manage valuable assets such as vehicles, weapons, and equipment used by law enforcement agencies, helping to prevent theft, loss, or misuse.

3) Crime detection

IoT devices can be used to detect and prevent crime by monitoring and analyzing data from various sources, such as traffic patterns, social media, and public sensors.

4) Emergency response

IoT devices can be used to improve emergency response and management by providing real-time information on natural disasters, accidents, and other critical incidents.

5) Wearables

IoT devices such as wearable technology can be used to monitor the health and safety of law enforcement personnel and provide alerts in case of emergencies.

6) Policing

The use of IoT devices is assisting law enforcement officers in identifying criminals and tracking their location. City-wide security systems and alarms provide real-time crime information to the police, while access to criminal records through the internet allows officers to quickly gather pertinent information. These technological advancements are contributing to a reduction in crime rates worldwide.

7) IoT firearms

Smart guns that utilize biometrics to verify the user's authorization to operate the firearm are only accessible to legal adults with a gun license. These firearms record the exact location of shots fired and other occurrences during use. Additionally, IoT technology allows for the automatic activation of body cameras in high-pressure situations.

8) Unidentified cars

Drones are increasingly being utilized for surveillance in areas where security personnel may not be present. These devices can monitor suspicious activity, provide details on the location of unknown vehicles, and track criminals. Alarms are also triggered when necessary, alerting authorities to potential threats.

B) *Big data applications in the legal system*

Big data analytics has the potential to transform the legal system by providing valuable insights, improving efficiency, and enhancing decision-making. Here are some applications of big data in legal systems

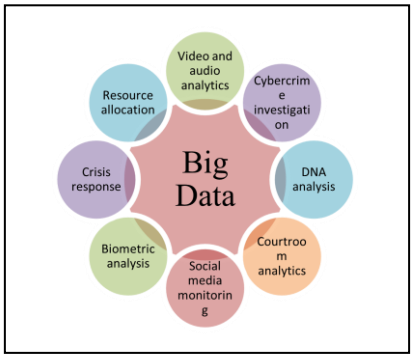

Fig.2. Big Data Applications

1) Video and audio analytics

Law enforcement agencies can use big data tools to analyze vast amounts of video and audio data captured by surveillance cameras and body-worn cameras. This can help identify suspects, gather evidence, and detect potential threats.

2) Cybercrime investigations

Big data can be used to analyze digital evidence, such as computer logs and network traffic, to investigate cybercrimes and track down cybercriminals.

3) DNA analysis

Big data can be used to analyze large amounts of DNA data to identify suspects and match DNA samples from crime scenes to known offenders.

4) Courtroom analytics

Legal systems can use big data to analyze courtroom data, such as case outcomes and judicial decisions, to identify trends and improve the efficiency and fairness of the judicial process.

5) Social media monitoring

Law enforcement agencies can use big data to monitor social media activity to detect potential threats, track down suspects, and gather evidence.

6) Biometric analysis

Big data can be used to analyze biometric data, such as fingerprints and facial recognition, to identify suspects and track down criminals.

7) Crisis response

Law enforcement agencies can use big data to analyze real-time data from multiple sources, such as social media, sensors, and emergency calls, to respond quickly and effectively to crises, such as natural disasters and terrorist attacks.

8) Resource allocation

Law enforcement agencies can use big data to identify areas of high crime rates and allocate resources, such as officers and equipment, accordingly.

C) AI Applications in Legal Systems

We have subdivided AI applications into two categories. Such that expert systems applications and machine learning applications for law enforcement and legal systems. Expert Systems in Law are computer programs that use artificial intelligence techniques to simulate the reasoning and decision-making abilities of human experts in a specific legal domain. They can be designed to perform various tasks that are traditionally done by lawyers and legal professionals, such as legal research, contract management, and decision-making support. On the other hand machine learning is used to predict the crime likely to occur in the future, language translation, and so on. In this section, we explain here some applications of expert systems and machine learning used in law enforcement, the legal system, and in the courtroom.

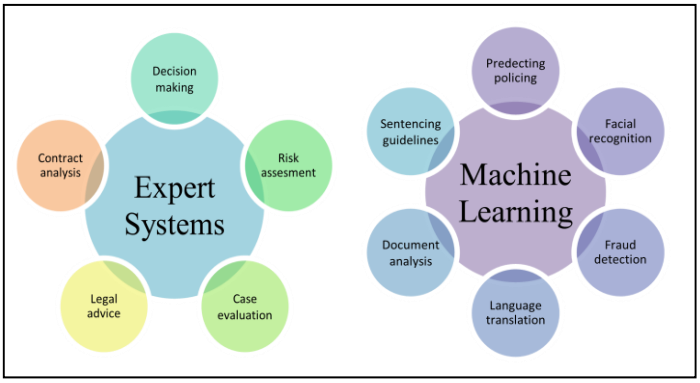

Fig.3. AI Applications

D) Expert systems Applications

1) Legal advice

Expert Systems in Law can be used to provide advice and automate legal research and analysis tasks by identifying relevant cases, statutes, regulations, and other legal sources, and extracting key information from them. ASHSD-II is an expert legal system that combines rule-based and case-based reasoning models to handle disputes related to matrimonial property under English law.

2) Contract analysis

Expert Systems in Law can be used to manage and analyze large volumes of contracts and other legal documents, by organizing them, categorizing them, and extracting relevant data from them. For example, Legislate is a contract management platform powered by a knowledge

graph that uses legal rules to generate lawyer-approved contracts.

3) Decision-making

Expert Systems in Law can assist judges and lawyers in making informed decisions by providing relevant legal information, analyzing legal arguments, and predicting case outcomes based on historical data. For example, JUDGE is an expert legal system that relies on rule-based reasoning to deal with sentencing in criminal cases involving offenses such as murder, assault, and manslaughter.

4) Risk assessment

Expert Systems can help law enforcement agencies to assess and manage risks related to public safety, such as natural disasters, pandemics, and terrorism. They can also provide real-time updates and alerts on potential threats and risks.

5) Case Evaluation

Expert Systems can help law enforcement agencies to manage and analyze large volumes of case data, such as police reports, witness statements, and legal documents. They can also assist in prioritizing cases based on their potential impact and likelihood of resolution.

E) Machine learning Applications

1) *Predictive Policing*

Machine learning algorithms can be trained on historical crime data to predict where crimes are likely to occur in the future. This helps law enforcement to allocate resources more effectively and reduce crime rates.

2) Facial Recognition

Machine learning algorithms can be used to analyze facial features and match them to a database of known individuals. This helps law enforcement to identify suspects and criminals.

3) Document Analysis

Machine learning algorithms can be used to analyze large volumes of legal documents such as contracts, agreements, and court filings. This helps legal professionals to identify relevant information quickly and accurately.

4) Sentencing Guidelines

Machine learning algorithms can be trained on historical sentencing data to predict the likely sentence for a given crime. This helps judges to make more informed decisions when it comes to sentencing criminals.

5) Fraud Detection

Machine learning algorithms can be trained to identify patterns of fraudulent behavior in financial transactions. This helps to prevent financial crimes and protect consumers and businesses alike.

6) Language Translation

Machine learning algorithms can be trained to translate legal documents from one language to another. This helps to improve access to justice for individuals who speak different languages.

E) International Approaches to AI regulations

United Nations Interregional Crime and Justice Research Institute (UNICRI) has published documents that mentioned the timeline of key strategies, action plans, and policy papers on Artificial Intelligence (AI). Figure no.4 explains this section [24].

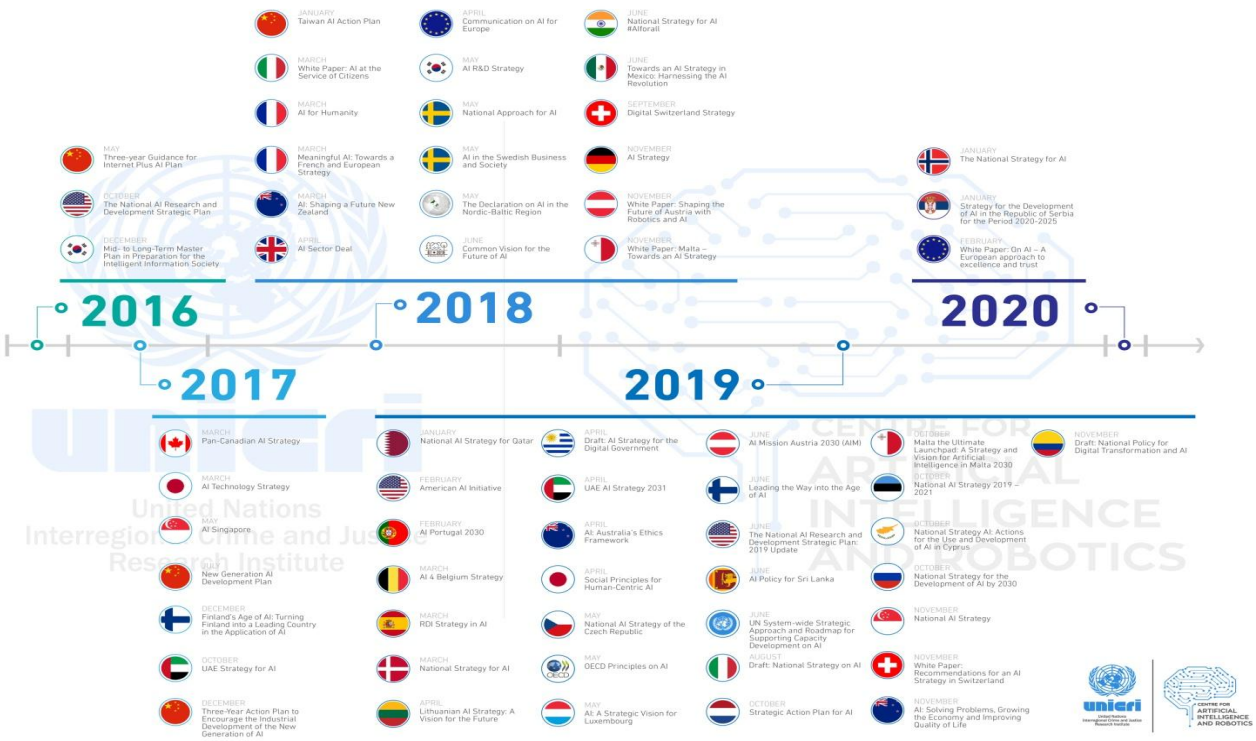

Fig.4. International Approaches to AI Action Plan

IV. PROPOSED KB ARCHITECTURE OF LEGAL EXPERT SYSTEMS (LES)

We have proposed a knowledge base (KB) legal expert systems architecture to develop legal expert systems for use by the non-lawyers and lawyers to get potential benefits in the legal system. Legal expert systems are specialized expert systems that leverage artificial intelligence to simulate the decision-making skills of a human expert in the field of law. These systems rely on a knowledge base, a rule base, and an inference engine to collect, reference, and generate expert knowledge on specific topics within the legal realm. Knowledge gathered and developed by legal Information experts and legal knowledge engineers respectively. It is

important to note that this is recommended for the particular problem domain, not for a general-purpose system in legal aid. Here is the explanation of our proposed legal expert systems architecture [25].

A) Legal knowledge expert

An expert in legal knowledge refers to an individual who possesses the necessary qualifications and experience in the field of law and is authorized to deal with legal aspects such as findings, decisions, recommendations, and other legal matters in an office. Such individuals may include advisors, associate advisors, consultants, solicitors, and other law expert officers.

B) Legal Knowledge Engineer

Coined by Richard Susskind in his book "The End of Lawyers?" in 2008, the term Legal Knowledge Engineer (LKE) is now used in the legal industry to a significant extent.

The LKE is a support role positioned between lawyers and developers and is responsible for facilitating the development of legal tech tools.

C) Inference Engine

An inference engine is a component of an artificial intelligence system that applies logical rules to a knowledge base to deduce new information. Initially, inference engines were components of expert systems, which consisted of a knowledge base and an inference engine.

D) Explanation facility

Most expert systems come equipped with explanation facilities that allow users to ask why the system asked a specific question or how it reached a particular conclusion. Such questions are answered by referring to the system's goals, the rules being used, and any existing problem data. These facilities enable users to better understand the

reasoning behind the system's decision-making processes and improve their trust in the system.

E) User Interface

A user interface refers to how an expert system interacts with its users. This can include dialog boxes, command prompts, forms, or other input methods. Some expert systems may also interact with other computer applications and not necessarily directly with a human user. The user interface is an essential component of an expert system as it determines the system's ease of use, efficiency, and overall user experience.

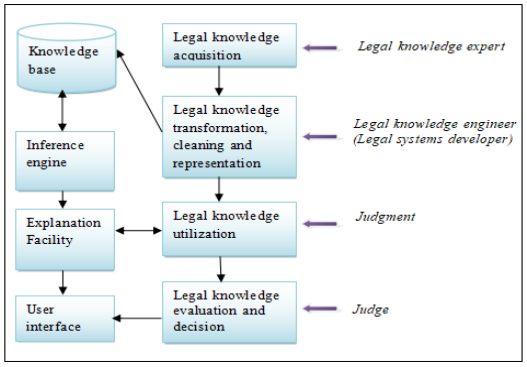

Fig.5. Proposed Legal Expert Systems (LES) Architecture

F) Example of Legal Expert systems

1) The Latent Damage Project

The Latent Damage Project is an expert legal system that utilizes rule-based reasoning to handle limitation periods related to tort, contract, and product liability law under the Latent Damage Act 1986 in the UK.

2) Split-Up

Split-Up is an expert legal system that employs rule-based reasoning to assist with the division of marital assets under the Family Law Act (1975) in Australia.

3) SHYSTER

SHYSTER is an advanced legal expert system that operates primarily on a case-based reasoning approach. It also can function as a hybrid system by integrating rule-based models. Its versatility extends across various legal domains, encompassing Australian copyright law, contract law, personal property, and administrative law.

4) *TAXMAN*

TAXMAN is an AI-powered legal system that utilizes a rule-based approach to conduct fundamental legal reasoning. It functions by categorizing cases according to specific statutory rules within the domain of corporate reorganization law.

V. CHALLENGES AND ETHICAL CONSIDERATIONS

While IoT, Big Data, and AI applications offer numerous benefits for the law enforcement and legal system, they also present several challenges and ethical considerations that need to be addressed. Here are some of the key challenges and ethical considerations [26, 27].

1) Privacy and Data Protection

The increased use of IoT devices and the collection of Big Data raises concerns about privacy rights and data protection. It is crucial to establish clear guidelines on data collection, storage, access, and retention to ensure that personal and sensitive information is adequately protected and only used for legitimate purposes.

2) Bias and Discrimination

AI algorithms can be susceptible to bias, reflecting the biases present in the data used for training. In the law enforcement and legal system, biased algorithms can result in discriminatory practices, profiling, and unfair treatment. It is essential to ensure transparency, accountability, and regular audits of AI systems to mitigate bias and ensure fairness in decision-making processes.

3) Reliability and Accuracy

The reliability and accuracy of IoT devices, Big Data sources, and AI algorithms are paramount in law enforcement and legal system. Inaccurate or unreliable data and algorithms can lead to erroneous judgments, false identifications, and miscarriages of justice. Regular testing, validation, and quality control measures should be in place to minimize errors and ensure the reliability of these technologies.

4) Security and Cyber Threats

IoT devices and interconnected systems can be vulnerable to cyberattacks, posing significant security risks. Breaches and unauthorized access to sensitive law enforcement and legal data can compromise investigations, compromise privacy, and undermine public trust. Robust cybersecurity measures, encryption, and regular updates are essential to safeguard against these threats.

5) Transparency and Explainability

AI algorithms often operate as black boxes, making it challenging to understand their decision-making processes. In the legal system, explainability is crucial for ensuring accountability, allowing individuals to understand how decisions are reached, and challenging them if necessary. Efforts should be made to develop interpretable AI models that can provide transparent explanations for their outputs.

6) Human Oversight and Accountability

While AI systems can automate certain tasks, human oversight, and accountability should remain central in the law enforcement and legal system. Human professionals should be responsible for critical decision-making, reviewing AI-generated outcomes, and addressing any biases or errors that may arise. The legal framework should clearly define the roles, responsibilities, and limitations of AI systems in these domains.

7) Unintended Consequences and Unforeseen Risks

The deployment of IoT, Big Data, and AI technologies can have unintended consequences and unforeseen risks. These include the potential for mission creep, where initially intended purposes of technology may expand beyond their original scope, as well as potential negative impacts on civil liberties and individual rights. Continuous monitoring and evaluation of the technologies' impact should be carried out to mitigate and address such risks.

8) Equitable Access and Technological Divide

The adoption of IoT, Big Data, and AI technologies should not exacerbate existing social inequalities. Ensuring equitable access to these technologies, including access to legal aid and justice systems, is essential to prevent a technological divide and ensure that marginalized communities are not disproportionately disadvantaged.

9) Ethical Use of Facial Recognition

Facial recognition technologies used in law enforcement should be carefully regulated to prevent misuse and abuse. There are concerns regarding mass surveillance, invasion of privacy, and the potential for false identifications. Developing clear guidelines and oversight mechanisms for the ethical use of facial recognition technology is crucial.

10) Accountability and Transparency of Algorithms

In the legal system, it is important to have transparency and accountability regarding the algorithms used. This includes disclosing the criteria, data sources, and decision-making processes involved. Additionally, legal professionals and stakeholders should have the ability to challenge and question the outcomes produced by these algorithms.

11) Regulatory Frameworks

Develop comprehensive and up-to-date regulations that address the unique challenges posed by IoT, Big Data, and AI in the law enforcement and legal context. These regulations should cover areas such as data protection, privacy, algorithmic transparency, and accountability.

12) Ethical Guidelines

Establish clear ethical guidelines and best practices for the development, deployment, and use of IoT, Big Data, and AI technologies in the law enforcement and legal system. These guidelines should prioritize fairness, non-discrimination, accountability, and respect for individual rights.

13) Collaboration and Public Engagement

Foster collaboration and engage with relevant stakeholders, including legal professionals, technologists, civil society organizations, and affected communities. Encourage open dialogue, public consultations, and multi-disciplinary collaborations to ensure that diverse perspectives are considered in the development and implementation of these technologies.

14) Education and Training

Provide adequate education and training to legal professionals, law enforcement officers, and relevant stakeholders on the implications, limitations, and ethical considerations of IoT, Big Data, and AI technologies. This will promote informed decision-making, responsible use, and a better understanding of the potential biases and risks associated with these technologies.

15) Algorithmic Auditing

Establish independent auditing mechanisms to assess the fairness, accuracy, and transparency of AI algorithms used in law enforcement and the legal system. These audits should evaluate the impact of algorithms on different demographic groups, identify biases, and suggest improvements to mitigate any adverse effects.

16) Data Governance and Consent

Implement robust data governance frameworks that ensure informed consent, data minimization, and the secure handling of personal and sensitive information. Individuals should have control over their data, including the ability to access, rectify, and delete their information.

17) Continuous Monitoring and Evaluation

Regularly monitor and evaluate the impact and effectiveness of IoT, Big Data, and AI applications in the law enforcement and legal system. This includes ongoing assessment of their fairness, accuracy, and compliance with ethical guidelines. Any negative consequences should be identified and addressed promptly.

18) International Collaboration

Foster international collaboration and sharing of best practices to address the global nature of IoT, Big Data, and AI technologies in the law enforcement and legal system. This can help establish common standards, promote consistency, and ensure that ethical considerations are upheld across jurisdictions.

By proactively addressing these challenges and ethical considerations, it is possible to harness the potential of

IoT, Big Data, and AI technologies while upholding fundamental rights, fairness, and accountability within the law enforcement and legal system. It requires a multi-stakeholder approach involving policymakers, legal experts, technology developers, civil society organizations, and affected communities.

VI. FUTURE DIRECTIONS

The future of IoT, Big Data, and AI in the legal system looks promising. Emerging technologies, such as natural language processing and machine learning, are expected to transform legal research and decision-making processes. Here are some future directions and applications for these technologies in this domain.

1) *Predictive Policing*
IoT devices, such as sensors and surveillance cameras, can collect real-time data from various sources, including social media, traffic sensors, and crime databases. By analyzing this data using AI algorithms, law enforcement agencies can predict crime hotspots, patterns, and trends, enabling them to deploy resources effectively and prevent criminal activities.

2) Enhanced Surveillance and Public Safety
IoT-enabled devices can provide law enforcement agencies with a wealth of data for surveillance purposes. For example, video cameras equipped with facial recognition technology can help identify suspects or missing persons. Integration with AI algorithms can improve the accuracy and speed of identification, leading to enhanced public safety.

3) Intelligent Traffic Management
IoT devices can be used to collect data on traffic patterns, congestion, and accidents. By analyzing this data using AI and Big in data analytics, law enforcement agencies can optimize traffic flow, improve response times during emergencies, and enhance overall traffic management and safety.

4) Digital Forensics
With the proliferation of connected devices, IoT data can serve as valuable evidence in legal cases. AI and Big Data technologies can be used to analyze massive volumes of digital data, such as emails, social media posts, and communication records, to identify patterns, connections, and evidence relevant to investigations.

5) Smart Prisons and Corrections
IoT devices can be used within correctional facilities to monitor inmate activities, enhance security, and streamline operations. AI algorithms can analyze data from these devices to detect abnormal behavior, identify potential security threats, and improve overall prison management and inmate rehabilitation programs.

6) Legal Research and Case Analysis
AI-powered algorithms can assist legal professionals in conducting comprehensive research, analyzing vast amounts of legal data, and identifying relevant precedents. This can help streamline legal processes, reduce the time and effort required for case preparation, and improve overall efficiency within the legal system.

7) Risk Assessment and Sentencing
AI algorithms can analyze historical data on criminal records, demographics, and socio-economic factors to provide more accurate risk assessments and assist judges in determining appropriate sentences. This can help reduce bias, enhance fairness, and improve consistency in sentencing.

8) Cybersecurity and Data Protection
With the increasing digitization of legal systems, protecting sensitive data from cyber threats becomes crucial. IoT devices can be used to monitor and detect potential security breaches, while AI can help analyze and predict potential vulnerabilities, enabling proactive measures to ensure data privacy and cybersecurity.

9) Virtual Courts and Remote Proceedings
IoT, AI, and Big Data technologies can enable virtual courtrooms and remote proceedings, reducing the need for physical presence and improving access to justice. AI-powered language processing and translation tools can assist in real-time transcription and interpretation, facilitating communication across language barriers.

10) Fraud Detection and Financial Crime Prevention
IoT devices and AI algorithms can be employed to analyze financial transactions, identify patterns, and detect anomalies that may indicate fraud or financial crimes. This can assist law enforcement agencies and financial institutions in preventing and investigating such activities.

These future directions demonstrate the potential of IoT, Big Data, and AI to transform law enforcement and the legal system, enhancing efficiency, effectiveness, and public safety.

VII. CONCLUSION

The integration of IoT, big data, and AI in the law enforcement and legal system holds immense potential for transforming these sectors. By leveraging IoT devices and sensors, law enforcement agencies can gather real-time data from various sources, enabling them to monitor and respond to incidents more effectively. Big data analytics

can help extract meaningful insights from large volumes of data, aiding in crime prevention, investigation, and resource allocation. AI technologies, such as machine learning and natural language processing, can automate repetitive tasks, streamline processes, and assist in predictive analysis. This can lead to faster and more accurate decision-making, improved risk assessment, and resource optimization. AI-powered tools can also facilitate legal research, document review, and case management, saving time and reducing costs for legal professionals. However, it is crucial to address certain challenges associated with these technologies. Privacy concerns, data security, and ethical considerations must be carefully addressed to ensure the responsible and lawful use of IoT, big data, and AI in law enforcement and legal system. It is important to strike a balance between the benefits these technologies offer and the protection of civil liberties and individual rights.

On the whole, the application of IoT, big data, and AI has the potential to greatly enhance the effectiveness and efficiency of the law enforcement and legal system. Continued research, development, and collaboration between technology experts, law enforcement agencies, and legal professionals will be essential to maximize the benefits of these technologies while mitigating potential risks.

REFERENCES

[1] Fina, S., & Ng, I. (2017). Big Data & Litigation: Analyzing the Expectation of Lawyers to Provide Big Data Predictions when Advising Clients. *Indian JL & Tech.*, *13*, 1.

[2] Fabiano, N. (2017). Internet of Things and the legal issues related to the data protection law according to the new European General Data Protection Regulation. *Athens JL*, *3*, 201.

[3] Weber, R. H., & Weber, R. (2010). *Internet of things* (Vol. 12). Heidelberg: Springer.

[4] Weber, R. H. (2009). Internet of things–Need for a new legal environment? *Computer law & security review*, *25*(6), 522-527.

[5] Tung, K. (2019). AI, the internet of legal things, and lawyers. *Journal of Management Analytics*, *6*(4), 390-403.

[6] Chike, C. P. (2018). *The Legal Challenges of Internet of Things Mass Communications View project Cybersecurity Law View project*. https://doi.org/10.13140/RG.2.2.31475.84004

[7] Greenleaf, G. (1989, August). Legal Expert Systems–Robot Lawyers?. In *Australian Legal Convention, Sydney*.

[8] Tschider, C. A. (2018). Regulating the internet of things: discrimination, privacy, and cybersecurity in the artificial intelligence age. *Denv. L. Rev.*, *96*, 87.

[9] Artificial Intelligence and data protection.*Council of Europe*

[10] Liebowitz, J. (1986). Expert systems in law: A survey and case study. *Telematics and Informatics*, *3*(4), 263-271.

[11] Sidi Ahmed, S. M., & Zulhuda, S. (2015). The concept of internet of things and its challenges to privacy. *South East Asia Journal of Contemporary Business, Economics and Law*, *8*(4), 1-6.

[12] Ződi, Z. (2017). Law and legal science in the age of big data. *Intersections. East European Journal of Society and Politics*, *3*(2), 69-87.

[13] Srivastava, R. (2018). Artificial Intelligence in the legal industry: A boon or bane for the legal profession. *International Journal of Engineering Trends and Technology*, *64*(3), 131-138.

[14] An Introduction to the Internet of Things(IoT) for Justice System and Law Enforcement Professionals.https://www.uribe.100.com

[15] Devins, C., Felin, T., Kauffman, S., & Koppl, R. (2017). The law and big data. *Cornell JL & Public Policy*, *27*, 357.

[16] Ashley, K. D. (1992). Case-based reasoning and its implications for legal expert systems. *Artificial Intelligence and Law*, *1*(2-3), 113-208.

[17] Weber, R. H., & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. *Computer law & security review*, *32*(5), 715-728.

[18] Naik, V. M., & Lokhanday, S. (2012). Building a legal expert system for legal reasoning in specific domain-A survey. *International Journal of Computer Science & Information Technology*, *4*(5), 175.

[19] Susskind, R. E. (1986). Expert systems in law: A jurisprudential approach to artificial intelligence and legal reasoning. *The modern law review*, *49*(2), 168-194.

[20] Popple, J. (1990, February). Legal expert systems: The inadequacy of a rule-based approach. In *Proceedings of the Thirteenth Australian Computer Science Conference (ACSC-13), Monash University, Melbourne* (pp. 7-9).

[21] TechVidvan. (n.d.). Law Enforcement Applications of IoT. Retrieved May 19, 2023, from https://techvidvan.com/tutorials/law-enforcement-applications-of-iot/

[22] Wisdom Jobs (n.d.). Internet of Things (IoT) Law Enforcement Applications. Retrieved May 19, 2023, from https://www.wisdomjobs.com/e-university/internet-of-things-iot-tutorial-1864/internet-of-things-iot-law-enforcement-applications-25458.html

[23] Alam, M. N., Singh, V., Kaur, M. R., Kabir, M. S. (2023). Big Data: An overview with Legal Aspects and Future Prospects. In *Journal of Emeging Technologies and Innovative Research (Vol. 10, Issue 5)*.https://www.jetir.org/papers/JETIR2305670.pdf

[24] "UNICRI :: United Nations Interregional Crime and Justice Research Institute". *Retrieved from* www.unicri.it.

[25] Legal knowledge engineeir definition. Retrieved May 19, 2023, from http://thelegalknowledgeengineer.co.uk/

[26] Alam, M. N., Kaur, B., & Kabir, M. S. (1994). Tracing the Historical Progression and Analyzing the Broader Implications of IoT: Opportunities and Challenges with Two Case Studies. *networks (eg, 4G, 5G)*, *7*, 8.

[27] Alam, M. N., Kaur, K., Kabir, M. S., Susmi, N. H., & Hussain, S. (2023). UNCOVERING CONSUMER SENTIMENTS AND DINING PREFERENCES: A LEGAL AND ETHICAL CONSIDERATION TO MACHINE LEARNING-BASED SENTIMENT ANALYSIS OF ONLINE RESTAURANT REVIEWS. In *International Journal of Creative Research Thoughts* (Vol. 11, Issue 5). www.ijcrt.orgwww.ijcrt.orgb834