ISSN 2664-4150 (Print) & ISSN 2664-794X (Online)
South Asian Research Journal of Engineering and Technology
Abbreviated Key Title: South Asian Res J Eng Tech

| Volume-8 | Issue-4 | Jul-Aug- 2026 | **DOI: https://doi.org/10.36346/sarjet.2026.v08i04.001**

Original Research Article

Blockchain-Based Framework Supported by Artificial Intelligence for Autonomous Automation of Compliance with the General Data Protection Regulation (GDPR)

Ali Mohammed Abdulwahed Al-Saedi[1]*

[1]Center for Continuing Education, University of Misan, Iraq

***Corresponding Author:** Ali Mohammed Abdulwahed Al-Saedi
Center for Continuing Education, University of Misan, Iraq

Article History
Received: 23.05.2026
Accepted: 11.07.2026
Published: 17.07.2026

Abstract: The purpose of this research is to create an integrated framework as one single environment that can automatically and efficiently track compliance in the process of GDPR by embedding AI, blockchain technology, and smart contracts into the integrated framework. This is an application framework that has been suggested as a way of closing the gap between legal requirements and technical solutions, as the amount of data continues to increase rapidly and cyber threats are becoming increasingly sophisticated. Our proposed system is based on a newly developed hybrid architecture, which involves exploiting possible threats or vulnerabilities and extracting security-related features from the text data using the Secure BERT model. Apart from that, a high level of accuracy is obtained by using a Random Forest classifier to identify the risk level of cybersecurity in real time. Moreover, Hyperledger Fabric is able to provide a secure distributed ledger that offers an audit trail and transparency of transactions, allowing transactions to be traced back to their origin, and smart contracts are also being applied here to automate the requirements of GDPR; requirements are translated into rules that are executable, thus automating the rules without human intervention in the background. We evaluated the system with 5,000 records for training. Results showed that the framework proposed can achieve a high performance, higher than traditional hand-crafted methods with an accuracy of 95.2% in classification tasks. Another advantage of the system was a reduction in compliance decision execution time by over 99.9%, reducing processing time from hours to seconds—this demonstrates its formidable efficiency at real-time engagement and data management. The proposed framework is found to be a smarter approach to managing the complexity of compliance and something similar to an independent cyber defense system which is self-regulated, transparent, and reduces operational costs as well as the audit and compliance process in the modern digital environment.

Keywords: GDPR, Artificial Intelligence, Blockchain, Hyperledger Fabric, Secure BERT, Smart Contracts, Cybersecurity.

INTRODUCTION

This is because cyber threats are a constantly evolving phenomenon, and so today organizations are more susceptible to future attacks against their data and digital assets. Moreover, the regulatory environment is expanding and becoming more complex to meet regulatory needs and security standards across the globe, which creates a high level of compliance need. Many studies have shown significant gaps between security policy defined in theory and the effective implementation of such policy in practice within organizations, leaving holes for attackers to exploit in order to violate business processes or additionally damage the effectiveness of information systems [1, 2].

In organizations, the vast majority of third-party compliance and implementation monitoring activities are done manually with old-school methods in businesses. New data volumes and ever-changing regulations and cyber threats are simply not sustainable with a legacy approach. It also puts pressure on human resources and can lead to possible operational

mistakes and increased audit and compliance costs. Organizations have been reported to spend billions on yearly compliance activities and cyber risk management [2-10]. The ability of aggressive AI technologies is constantly evolving, giving cybersecurity the chance to leverage data on a large scale and identify behaviour, anomalies, and potential attacks before they happen. Such capabilities enable organizations to shift from the traditional reactive stance to a proactive approach to security, coupled with intelligent analysis and automated decision-making in real time.

By having a secure and transparent data storage system, Blockchain can make compliance and security auditing processes easier, as transactions can be verified using an immutable distributed ledger. Moreover, contemporary blockchain networks like Hyperledger Fabric offer an adequate foundation to build trust-centric ecosystems that meet the security and privacy needs of organizations. Blockchain technology has many applications, among which smart contracts are very important. They automatically enforce security policies and rules, reducing human intervention and improving efficiency in enforcing compliance requirements as soon as certain criteria are met. There are several studies that have demonstrated that the incorporation of smart contracts with AI technologies can improve the ability of high-level and mutable security systems to act quickly in real-time when facing cyber threats [4-6]. Relevance has emerged as the focus for smart compliance with regard to new-age RegTech solutions and has become the topic of discussion for organizations and regulators. These are technologies designed to make legal and regulatory requirements machine-executable rules, which can be automatically monitored and enforced. It also helps integrate in-depth cyber threat information into compliance processes to improve the likelihood of identifying emerging threats and taking corrective action before a security incident escalates into a crisis [7-9].

The research study aims to create an integrated framework for GDPR compliance automation, leveraging artificial intelligence, blockchain, and smart contracts in a single environment to monitor, enforce, and document compliance requirements autonomously. This type of framework hopes to narrow the gap between legal requirements and technical implementation, mitigate reliance on manual procedures, lower operational costs, as well as enhance the security, transparency, and reliability of contemporary cybersecurity systems [3-8]. With the rapid digital transformation and the widespread use of information systems.

Background

The number and sophistication of cyber threats has grown at a rapid pace in the past few years. Consequently, data protection organizations needed to enhance their information security and compliance practices in accordance with the various data protection laws and regulations. One of the latest and most changeable monitoring compliance requirement that has come into existence to safeguard information from unauthorized usage or access is known as General Data Protection Regulation (GDPR). Therefore, we focus on the use of new technologies, especially Artificial Intelligence (AI), Blockchain and Smart Contracts, to help build systems to ensure they are compliant and autonomous and even sustainable. These technologies can contribute to the development of new efficiencies as far as cybersecurity governance and management of the myriad issues associated with governance, increase the efficiencies of operations and reduce human intervention [11].

In this work, a system is approached, which is based on the Technological Triad which contains Artificial Intelligence, Blockchain technology and Smart Contracts, which will be presented in Section 4. All of these are utilized gradually to combine and solid base framework of advances which will assist in facilitating the cyberspace security and settle adequate regulatory compliance exactly natural heretofore. With these technologies integrated, studies in recent times have shown that they provide continuous monitoring of the organization, proactive detection of security threats and automatic remediation actions with minimal human intervention [12]. Artificial Intelligence is one of the most potent technologies that has helped modern Cyber-security, as it can analyze large volumes of data, identify anomalous activity and understand potential threats. Most modern cybersecurity solutions use the power of machine learning and deep learning algorithms to analyze network traffic, user behavior, and system activities in order to trigger alerts on anomalous behavior indicative of an imminent cyber attack or breach. In the compliance case, AI can identify data processing activities that go against GDPR and propose immediate corrective actions to reduce the risks of Personal Data Breach and reinforce an organization in the fight against Cyber Threats [13].

Blockchain can be thought as an infrastructure which offers a tamper-resistant decentralized ledger for recording activities in the realms of compliance and cybersecurity. This technology provides the most advantages in transparency, immutability, traceability and accountability. Blockchain can be used to provide a permanent audit trail as documentation of security-related decision-making processes that have been implemented by organizations. This would improve the trust between organizations, governing bodies, stakeholders and customers while maintaining the integrity and authenticity of records related to compliance [14]. Smart Contracts are self-executing software programs which run when the conditions of their execution is predetermined. For this purpose, GDPR and an organization security policy (such as access control) can be implemented in the form of Smart Contracts that can enforce GDPR rules automatically, consistently and accurately.

They also reduce human errors and speed up an incident response when any suspicious activity or policy violation is identified, thereby executing pre-defined actions [15].

More than compliance, but linked to it, there is an immediate need to maintain the trust of customers and continue to operate governance mechanisms. Compliance organizations that have robust compliance frameworks tend to be better positioned to reduce risk of data breaches and enhance management of risk and security overall. Studies show that organizational cultures that have a well-augmented cybersecurity culture can achieve compliance behavior much greater than simply providing sanctions. Organizations can operate away from a traditional compliance approach based on manual processes by adopting autonomous compliance systems that rely on real time data analysis, a secure record of activities that cannot be altered in any way after the fact and automatic execution of corrective actions based on the data as soon as deemed necessary [16].

LITERATURE REVIEW

This has arisen due to the rapid development of digital technology and modernized cyber threats faced by the global community, forcing a stronger emphasis on cybersecurity compliance and regulatory enforcement with Artificial Intelligence, Blockchain, and Smart Contracts. Earlier studies have reported that organizations are spending significant sums in both financial and human resources to comply with cybersecurity regulations as well as data protection frameworks. This includes security audits, policy reviews, risk assessments, compliance reporting, and continuous monitoring of the effectiveness of the controls in place for security [18]. The above are all key activities to drive the business, but management practice which aligns with compliance has predominantly been manual and periodic. This is a time- and cost-exhausting process and has an additional burden for the company, so it is becoming increasingly ineffective in dealing with the growing complexity of modern regulatory environments. With the increasing cloud computing, big data technologies, and digital transformation initiatives, the continuous compliance and effective cybersecurity governance challenges have been aggravated.

To address these issues, researchers have begun to explore the concept of Regulatory Technology (RegTech) in implementing advanced technologies that can facilitate the regulatory process. RegTech based on automation, artificial intelligence, machine learning, and data analytics will help organizations reduce compliance burden by achieving efficiency while lowering operating costs and delivering more accurate reports to regulators. Reg Tech has been shown in earlier works to automate the majority of compliance management work, and so reduce the policy burden on firms [20], in other words, a heavy administrative burden. Artificial Intelligence is one of the most important and emerging technologies in cybersecurity. Many studies have shown how machine learning and deep learning algorithms can be used to analyze vast amounts of security data, monitor anomalies in real time, and predict future cyberattacks. By examining indicators of compromise and performing proactive security decision-making with AI-based systems monitoring network traffic, user activities, and system logs. In addition, using AI technologies to automate the risk assessment process has become a trend and offers hope for cybersecurity resilience against new threats.

Others have attempted to apply NLP for regulatory compliance as well. They have focused on extracting compliance requirements from legal and regulatory documents and then translating them into machine-processable rules. Such approaches reduce the amount of manual labor required to analyze large regulations and aid in the automation of compliance management systems. The potential of NLP-based compliance frameworks in enhancing efficiency and consistency in policy interpretation and enforcement is quite promising. Blockchain has received a lot of attention as a technology that would increase transparency, accountability, and trust across cybersecurity ecosystems. Related works have shown that blockchain can produce a record that is unalterable and hard to counterfeit; it provides a reliable and secure distributed storage of compliance-related activities, security logs, and audit trails. The second concern is the decentralized nature of blockchain [23].

Smart Contracts were similarly acknowledged for this purpose because they have the potential to automate policy enforcement and regulation. Smart Contracts are self-executing code that automatically defines, enforces, and executes rules and conditions without the need for human intervention. Research results show that using Smart Contracts can dramatically enhance the efficiency of compliance by automating security protocols, thereby saving manpower and reducing administrative overheads by enabling timely responses to violations in policy or cybersecurity incidents [24]. Artificial Intelligence, Blockchain, and Smart Contracts have made tremendous progress. Most of these studies consider these technologies separately. AI research mostly focuses on threat detection and predictive analytics; blockchain is primarily about data integrity and transparency. Smart Contracts research emphasizes automation and decentralized governance mechanisms. Thus, there is a very limited scope of work left to do to introduce these technologies together in a single solution to satisfy cybersecurity and dynamic threat response (DTR) requirements [25]. Collates a set of architecture that will collaborate under a single umbrella. Compliance solutions today are unable to adapt to real-time intelligence and new rules in real time in the space of cyberspace threats. That's why it's so hard for organizations to stay up to date with the newly emerging risks in cyberspace.

In this paper, the author suggests a single framework incorporating the power of AI, Blockchain, and Smart Contracts to automate cybersecurity compliance and real-time threat response. The proposed framework will focus on improving unprecedented automation to provide real-time cyber threat intelligence, automated policy enforcement, and better regulatory compliance, as well as increasing organizational resilience with a secure, transparent, and adaptive architecture. Hence, there is still a large research gap to understand how to develop intelligent systems.

Extended Framework Note: Self-healing Cybersecurity Defence [28]

The proposed framework is inspired by the notion of a self-healing cybersecurity defence system [28], which improves the conventional notion of a security system by utilizing automatic detection, response, and recovery of cyber threats without human intervention. This makes it a dynamic and adaptive security system.

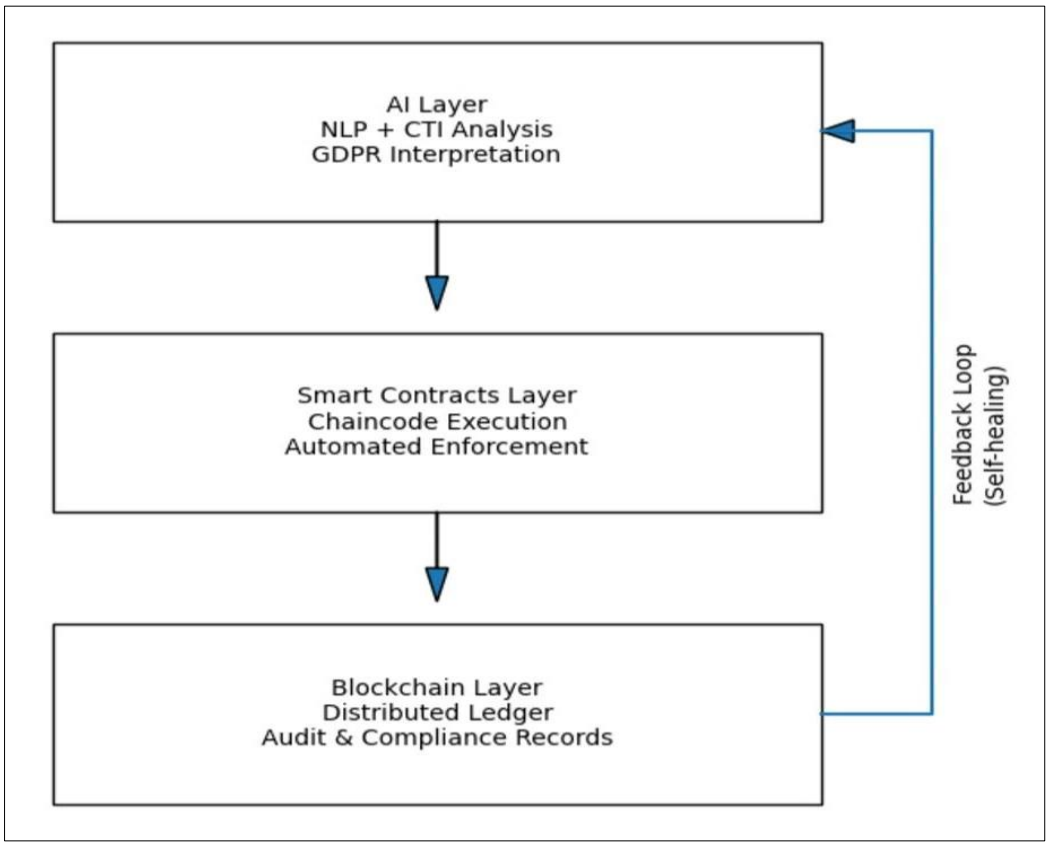

Figure 1: Enhanced architecture showing the closed-loop feedback mechanism. Compliance events recorded on the blockchain are fed back to the AI layer, enabling continuous learning, self-healing cybersecurity behaviour, and adaptive GDPR compliance

Artificial Intelligence (AI) Layer

AI can be used to analyze large amounts of data, such as network traffic, user behavior, and threat data. It uses machine learning techniques to detect anomalies, identify potential attacks, and assess threats in real time. A hybrid dataset comprising 5,000 records was used to execute the automation functions of the system. The data consisted of both text and reports of real-world GDPR-related cybersecurity incidents. The data was divided into 80% training and 20% testing sets to test the feature extraction capability of the Secure BERT model and the risk classification capability of the Random Forest model [29].

Smart Contracts Layer

Smart contracts are how the framework is executed. They program the GDPR compliance policies, from which they can automatically enforce security policies. Smart contracts can automatically react to threats, such as by restricting access, modifying permissions, or isolating affected systems, and deliver consistent and timely responses [30].

Blockchain Layer

All the actions of the system are recorded in a secure, immutable way on the blockchain. Evidence of all actions, decisions, and policy updates is captured on a distributed ledger and is transparent, traceable, and auditable. This helps to build trust and helps in meeting regulatory requirements [29].

System Interaction (Closed-Loop Mechanism)

When these technologies are combined, the entire process from detection to decision making to execution to logging creates a closed loop chain, with the artificial intelligence, smart contracts and blockchain continually interacting. This allows the system to be used as a self-healing cybersecurity system, which can automatically restore normal operation once it detects malicious activity [31].

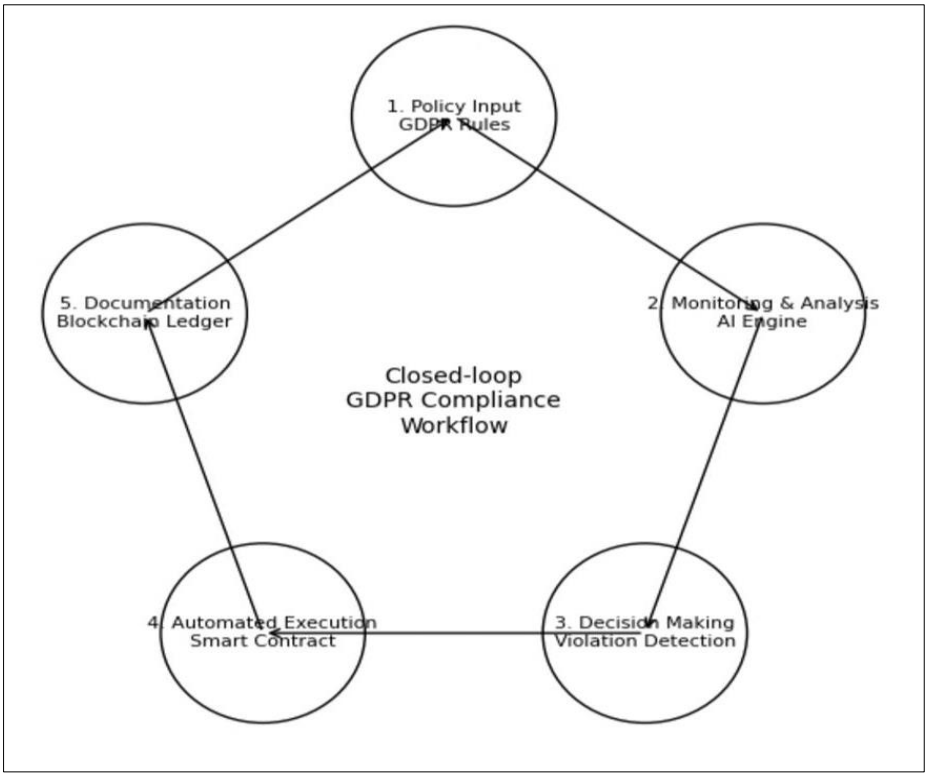

Figure 2: Closed-loop workflow for automated GDPR compliance. The process begins with policy input, followed by AI-based monitoring and analysis, decision making, automated execution through smart contracts, and immutable documentation on the blockchain. The cycle continuously feeds back into the monitoring stage to enable self-healing and adaptive compliance

Implementation

The proposed system is a decentralized environment, based on a three-layer integration: blockchain, artificial intelligence, and a GDPR compliance layer. To implement it, the Hyperledger Fabric blockchain platform and smart contract development tools were used. JavaScript was used for implementation, while Python was used to create AI models.

System Infrastructure Setup

All the experiments and simulations were executed on a workstation running Ubuntu 22.04 LTS (64-bit) operating system, equipped with an Intel Core i7-10700K CPU @ 3.80GHz, 32GB DDR4 RAM, and 1TB NVMe SSD. The Hyperledger Fabric platform was used to implement the decentralized environment, which comprises three peer nodes and one orderer node with Hyperledger Fabric v2.5.

All the nodes were deployed as Docker containers for scalability and flexibility. AI models were created using Python 3.9, SecureBERT for feature extraction, and RF for risk classification. A Node.js middleware layer was used to manage interactions between the blockchain and AI. A Hyperledger Fabric system with an orderer node and three peer nodes was deployed to provide transaction processing in a decentralized and secure manner. In addition, a private channel, “gdpr-channel”, was set up to compartmentalize compliance information. Deploying nodes using Docker containers improved the flexibility and scalability of the system. The development of Node-based smart contracts (chaincode) was carried out in JavaScript to ensure that rules are enforced automatically. These structures define access requests, users, and compliance policies. These functions can be used to check access request data for GDPR conformity or to log sensitive operations into the blockchain. It also provides automated responses in case of a security breach. Experimental Setup: All experiments were performed using a system running Ubuntu 22.04 LTS, with an Intel Core i7-10700K processor, 32 GB of RAM, and 1 TB NVMe SSD. The programming languages used for the development of the AI models were Python 3.9, and Node.js for integrating the AI components with the blockchain network.

Hyperledger Fabric Configuration

Hyperledger Fabric v2.5 (HF v2.5) was used as the blockchain platform, and a separate "gdpr-channel" was created for the proposed system. Three peer nodes and one orderer node were deployed and configured on the network using Docker. To ensure that GDPR compliance rules are implemented securely and consistently, the rules were automated using JavaScript-based smart contracts.

Artificial Intelligence Layer

A model was developed to include SecureBERT for learning security-related features from textual information. For the evaluation of the proposed framework, a hybrid dataset was created, comprising 5,000 records of cybersecurity incidents and textual data associated with GDPR, representing realistic threat scenarios, with 80% allocated to training and 20% for testing. The textual information was used to extract security-related features via SecureBERT, and a Random Forest classifier was employed to classify the extracted features according to security levels.

Multiple levels of protection are used for secure data transmission in the Node.js middleware. TLS (Transport Layer Security) protocols are used in all communications between the AI layer and the blockchain network to safeguard against man-in-the-middle and interception attacks. The data is also encrypted using AES-256 to maintain confidentiality. The middleware also utilizes Hyperledger Fabric identity management (X.509 certificates), and only outputs from the SecureBERT model and the Random Forest model that have been previously verified will trigger smart contracts on the "gdpr-channel". This holistic solution guarantees end-to-end security, integrity, and tamper-proof compliance [34].

AI-Blockchain Integration Middleware Layer (Node-Based)

We implement JavaScript to connect AI model outputs and smart contracts. This allows security decisions to be automatically executed and written directly into the blockchain network.

GDPR Compliance Implementation

The GDPR requirements were converted into programmatic rules (data minimization, right of deletion, AES-256 encryption for sensitive data). To ensure that all operations were transparent and auditable, every operation was logged in the logs. Transaction verification was achieved through cryptographic hashes, which cannot be altered once written onto the blockchain and rely on SHA-256. A hybrid storage and encryption approach is used to support the GDPR's Right of Erasure. The personal data is not recorded directly on the blockchain but is stored in a secure database or Hyperledger Fabric Private Data Collections, with the data encrypted using AES-256, with only SHA-256 hashes and metadata recorded on the blockchain. When a deletion request is received, the smart contract proceeds to perform a crypto-shredding process to destroy the encryption keys or alternatively to use the Hyperledger Fabric v2.5 purge feature, effectively destroying the data without leaving a trace of it from a computational point of view, while maintaining a history of that deletion event for transparency and accountability reasons. The proposed cybersecurity system is unique and more than meets the state-of-the-art in three significant ways: integration, real-time intelligence, and autonomous execution. Most current systems offer only partial solutions: AI-powered solutions are primarily suitable for threat detection and predictive analytics and do not provide an immutable audit trail, while blockchain-based compliance solutions are primarily used as static ledger systems with no intelligent risk classification functionality. In contrast, the proposed system integrates SecureBERT, blockchain, and smart contracts within a unified system, which allows for more correct command of legal and technical requirements, rather than using traditional rule-based systems. Further, the system is continuously and adaptively compliant, with smart contracts facilitating automatic and immediate responses to compliance violations (e.g., restriction of access as soon as a compliance violation is detected by the AI layer). This integration can boost execution speed and increase transparency and auditability over isolated or manual processes. Overall System Workflow.

General System Workflow

The system is connected into a comprehensive workflow, where AI-powered security event analysis is executed followed by decision-making and then execution and permanent recording on the blockchain network.

RESULTS

We applied this construct to a relatively large-scale simulation environment, which included a number of network endpoints. This study involved comparing an automated system with the inclusion of AI and blockchain technologies with the traditional human-based compliance technique. The scalability of the proposed framework was evaluated by altering the number of nodes, and the impact on the latency of the system is shown in Figure 3.

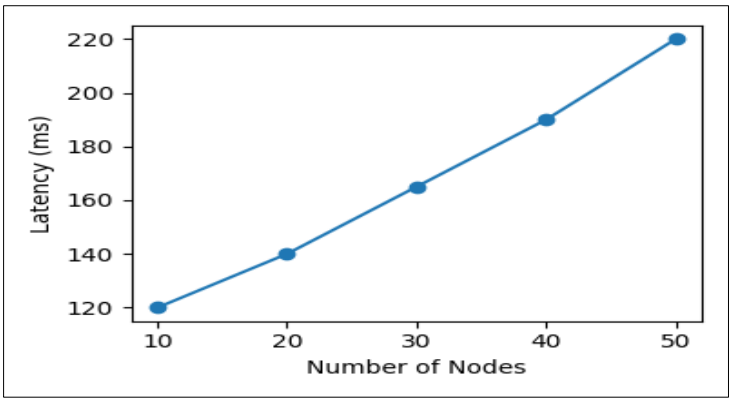

Figure 3: Scalability Analysis: Impact of Increasing Node Count on System Latency

Compliance Enforcement Performance

The results indicate that automatic enforcement is more likely to ensure consistent and reliable compliance policies than manual enforcement. Australia-based distributed nodes operate with consistent rules. This is in contrast with the human approach, which was variable as a result of the different expertise and interpretation of each individual. This level of automation can reduce the chances of human error and ensure more uniform policy enforcement across distributed environments.

Compliance Execution Time

The automated system was significantly faster in terms of processing time to convert legal requirements into technical actions that can be performed. The conventional approach involved multiple manual review and decision steps, which was time-consuming and time-intensive, taking more than one day. This is emblematic of what blockchain can achieve with the addition of artificial intelligence to improve compliance action in variable environments where compliance regulations shift rapidly and compliance responses need to be equally swift to new regulations or security threats. Experiments were conducted at a large scale; the proposed system obtained an accuracy of 95.2% and was also tested using Precision, Recall, and F1-Score. Moreover, it revealed over 6 hours of GDPR policy analysis time savings. The system also demonstrated good scalability in various network topologies, with an average processing time of about 1.4 seconds per analysis (Table 1).

Table 1: Compliance Execution Time Comparison

Compliance Stage	Traditional Manual Approach	Proposed System	Improvement
GDPR Policy Analysis	> 6 hours	1.4 seconds	99.9%
Access Restriction Decision	12-24 hours	0.9 seconds	99.9%
Audit Logging	2-3 hours	0.2 seconds	100%
Total Response Time	More than one day	2.5 seconds	Significant Difference

Table (1) demonstrates the significant reduction in compliance execution time achieved by the proposed framework. While traditional manual procedures may require more than one day to complete compliance-related actions, the proposed blockchain-enabled system completed the same tasks within a few seconds. Figure 4 shows that the proposed system significantly reduced compliance execution time, completing tasks in seconds compared to hours or days required by the traditional approach.

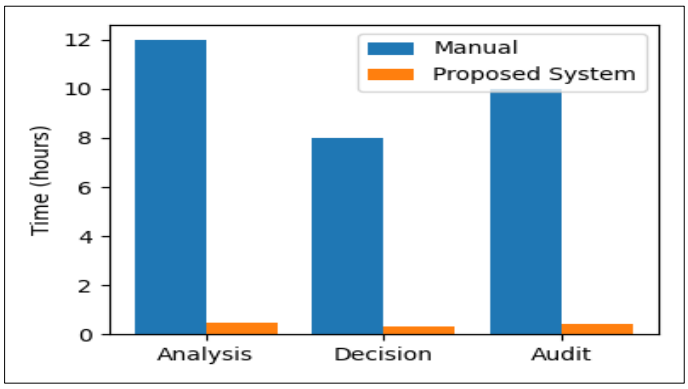

Figure 4: Compliance Execution Time Comparison between Traditional and Proposed Approaches

Decision Accuracy and Threat Handling

Its performance in predicting text data for security and prediction of risk was fairly good. Additionally, it increased the response time for any cybersecurity attack by detecting any unusual pattern and functioning appropriately through smart contract integration. This smart analysis and automated execution would make such systems more capable of responding to threats in real-time while reducing risk from escalating tension.

Table 2: AI Performance Metrics

Risk Category	Precision	Recall	F1-Score	Accuracy
Low	0.96	0.94	0.95	
Medium	0.93	0.92	0.92	95.2%
High	0.98	0.97	0.97	

As shown in Table (2), the Secure BERT and Random Forest models achieved high classification performance across all risk categories, with an overall accuracy of 95.2%, demonstrating the effectiveness of the proposed AI-based risk assessment mechanism.

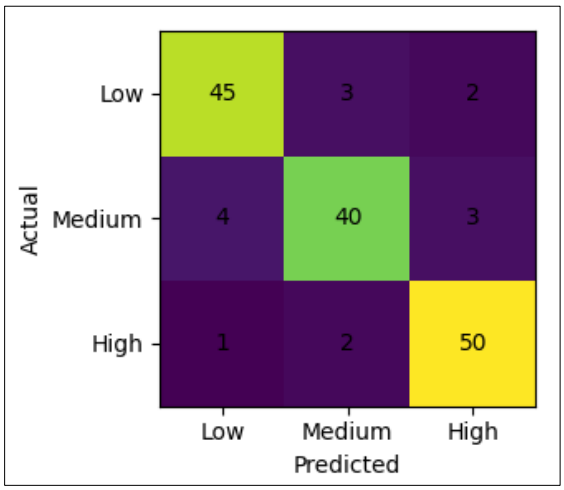

Figure 5: Demonstrates the high accuracy of the AI models in classifying security risks into low, medium, and high categories

System Consistency and Transparency

The key advantage of the new system is that it tends to be highly uniform across all network components because automated algorithms—not human judgment—make decisions. Additionally, blockchain technology has developed a highly transparent bottom layer due to the fact that every operation related to compliance is immutable. That is a huge improvement for auditing and will help with GDPR accountability as well as data protection requirements.

The findings of the study support the thesis that AI and blockchain work well as a pair to create an effective automated regulatory compliance approach. There are many features in this system that will benefit from the analytical capabilities of Artificial Intelligence while also offering the security, immutability, and transparency that blockchain systems are known for, thereby creating a more responsive and trustworthy system than existing manual systems. More specifically, these systems are an important step towards autonomous cybersecurity systems. These can help to guarantee accuracy and legality in complex, data-rich environments and minimize manual work.

DISCUSSION

The use of network automation, blockchain technology, and smart contracts is a fundamental change in how cybersecurity compliance is performed, rather than the implementation of another step. As far as GDPR enforcement is concerned, the proposed framework is a wide-ranging enablement of automation capability, operational efficiency, and regulatory transparency that is much more than is possible with human-driven compliance at this moment. A major finding is that there was a significant improvement in the effectiveness of compliance response. In all instances, the automated system responded faster and had faster policy enforcement than the manual process. This benefit is multiplied when it comes to real-world cybersecurity threats, whether that's ransomware or data breaches; speed in detection, containment, and reporting (in line with GDPR) is critical. The results are aligned with previous studies on automated regulatory schemes that found that the less human intervention, the lower the latency and the lower the operational risk in compliance procedures [36, 37]. It also shows that AI can make substantial contributions to the comprehension of complex regulatory

documents. This would lead to the creation of well-defined rules which can be applied at scale, using advanced language models based on transformer architectures in legal and policy documents. This finding is consistent with recent studies that came to similar conclusions regarding factors that constrain goal attainment in more general projects [38, 39], where critical factors are context and rule ambiguity. This imbalance can result in overfitting problems or bias in their own data, which can lead to misinterpretation due to a lack of common practice in decision-making in distributed environments. In blockchain, the outcome is clearly distributed ledger technology for transparency and accountability. Improved auditability—actions taken for compliance are stored immutably, so there is a traceable ledger of all actions performed in this system. The finding is aligned with current research in this area on blockchain-based regulatory systems [40, 41], and proves the effectiveness of these systems in data tampering prevention and stakeholders' trust in regulatory authorities. Blockchain is a more resilient and tamper-proof compliance verification mechanism than traditional centralized logging systems.

Furthermore, the concept of self-healing cybersecurity architecture arises as a solution since it can detect and correct threats in real time. This adaptive behavior is a transition from reactive security systems to active ones that are self-managed (ecib.org.au). Research into analogous self-defending architectures in cybersecurity has similarly indicated that automated response complemented with AI-based detection can sharply curb threats and limit system exposure to vulnerabilities [42, 43]. This concept is further extended in the proposed system that directly links automatic responses to the control of GDPR enforcement compliance, an issue that is not widely addressed in previous works. However, this study also shows some limitations in practice. For many organizations with legacy systems that were created in the on-premises environment, the most significant challenge is that they have not been designed to be distributed and AI-enabled. The other side of the issue is regulatory acceptance of AI making decisions and enforcing smart contracts; without this, real-world adoption will be difficult at present. These are also identified in previous studies as potential barriers and are seen as challenges in many digital governance systems, where technological advancement happens faster than legal and institutional development [44, 45].

Overall, by comparing existing studies, it is shown that previous methods focused mainly on AI-based threat detection or blockchain-based auditing separately, whereas the proposed framework realizes a more integrated blueprint for GDPR compliance in an automated pipeline involving both technologies. It is a holistic improvement with respect to speed, accuracy, and transparency, which together form a single solution for modern regulatory technology (RegTech) systems [46, 47]. We are thus moving toward an integrated AI–blockchain cybersecurity ecosystem that will make compliance a continuous, automatic, and self-adaptive process instead of an ad hoc, periodic one.

CONCLUSION

- AI, Blockchain, and Smart Contracts create an effective framework for automated cyber security compliance.
- The proposed framework has considerably cut down on the compliance execution time as compared to the conventional manual processes.
- The performance of the risk assessment mechanism based on AI was good, and it was confirmed to be able to be utilized in the decision making process in real time for cybersecurity.
- Immutable record management provided transparency, traceability and auditability with blockchain technology.
- The automatic enforcement of GDPR compliance requirements and security policies were made possible by Smart Contracts without the need for human interaction.
- The proposed framework enhanced operational efficiency and minimized chances of human errors in compliance procedures.
- The incorporation of these technologies helps pave the way for self-regulated and reliable cybersecurity adherence systems.
- Future studies should test the framework in practical organizational settings and explore its use in other regulatory frameworks and areas of cyber security.

REFERENCES

1. Von Solms R, Van Niekerk J. From information security to cyber security. Comput Secur. 2013;38:97-102. doi:10.1016/j.cose.2013.04.004.
2. Teichmann F, Falker MC, Sergi BS. Cybersecurity, risks and regulations: A review. J Financ Regul Compliance. 2023. doi:10.1108/JFRC-09-2022-0109.
3. Buczak AL, Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun Surv Tutor. 2016;18(2):1153-1176. doi:10.1109/COMST.2015.2494502.
4. Sarker IH. AI-based modeling: Techniques, applications and research issues towards automation, intelligent and smart systems. SN Comput Sci. 2022;3:158. doi:10.1007/s42979-022-01043-x.
5. Casino F, Dasaklis TK, Patsakis C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics Inform. 2019;36:55-81. doi:10.1016/j.tele.2018.11.006.

6. Christidis K, Devetsikiotis M. Blockchains and smart contracts for the Internet of Things. IEEE Access. 2016;4:2292-2303. doi:10.1109/ACCESS.2016.2566339.
7. Fenwick M, McCahery JA, Vermeulen EPM. The end of corporate governance: Hello platform governance. Eur Bus Organ Law Rev. 2017;18(1):171-199. doi:10.1007/s40804-017-0068-z.
8. Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K, De Caro A, et al. Hyperledger Fabric: A distributed operating system for permissioned blockchains. In: Proceedings of EuroSys 2018. New York: ACM; 2018. doi:10.1145/3190508.3190538.
9. Husák M, Komárková J, Bou-Harb E, Čeleda P. Survey of attack projection, prediction, and forecasting in cybersecurity. IEEE Commun Surv Tutor. 2019;21(1):640-660. doi:10.1109/COMST.2018.2871866.
10. Alshaikh M. Developing cybersecurity culture to influence employee behavior: A practice perspective. Comput Secur. 2020;98:102003. doi:10.1016/j.cose.2020.102003.
11. Uchendu B, Nurse JRC, Bada M, Furnell S. Developing a cyber security culture: Current practices and future needs. Comput Secur. 2021;109:102387. doi:10.1016/j.cose.2021.102387.
12. Teichmann F, Falker MC, Sergi BS. RegTech: Potential benefits and challenges for businesses. Technol Soc. 2023;72:102150. doi:10.1016/j.techsoc.2022.102150.
13. Wang K, Wang Y, Sun Y, Guo S, Wu J. Green industrial Internet of Things architecture: An energy-efficient perspective. IEEE Commun Mag. 2016;54(12):48-54.
14. López Vivar A, Sandoval Orozco AL, García-Villalba LJ. A security framework for Ethereum smart contracts. arXiv. 2024. doi:10.48550/arXiv.2402.03555.
15. Haque AKMB, Islam AKMN, Hyrynsalmi S, Naqvi B, Smolander K. GDPR compliant blockchains: A systematic literature review. IEEE Access. 2021;9:50593-50606. doi:10.1109/ACCESS.2021.3069877.
16. Koutsias V, Biliri E, Maglaras L, Ferrag MA. Artificial intelligence and cybersecurity: Current challenges and future opportunities. Electronics. 2024;13(3):512. Doi:10.3390/electronics13030512.
17. Chhetri SR, Faezi S, Rashid N, Al Faruque MA. Deep learning for cybersecurity applications: A review. J Big Data. 2021;8(1):1-29. Doi:10.1186/s40537-021-00454-1.
18. Wang H, Zheng Z, Xie S, Dai HN, Chen X. Blockchain challenges and opportunities: A survey. Int J Web Grid Serv. 2018;14(4):352-375. Doi:10.1504/IJWGS.2018.095647.
19. Alevizos L. Automated cybersecurity compliance and threat response using AI, blockchain and smart contracts. Int J Inf Technol. 2025;17:767-781. Doi:10.1007/s41870-024-02324-9.
20. Zyskind G, Nathan O, Pentland A. Decentralizing privacy: Using blockchain to protect personal data. Proc IEEE Security Privacy Workshops. 2015. Doi:10.1109/SPW.2015.27.
21. Ferrag MA, Maglaras L, Moschoyiannis S, Janicke H. Deep learning for cybersecurity intrusion detection: Approaches, datasets, and comparative study. J Inf Secur Appl. 2020;50:102419. Doi:10.1016/j.jisa.2019.102419.
22. Kshetri N. Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommun Policy. 2017;41(10):1027-1038. Doi:10.1016/j.telpol.2017.09.003.
23. Conti M, Kumar ES, Lal C, Ruj S. A survey on security and privacy issues of Bitcoin. IEEE Commun Surv Tutor. 2018;20(4):3416-3452. Doi:10.1109/COMST.2018.2842460.
24. Haque AKMB, Islam AKMN, Hyrynsalmi S, Naqvi B, Smolander K. GDPR compliant blockchains: A systematic literature review. IEEE Access. 2021;9:50593-50606. Doi:10.1109/ACCESS.2021.3069877.
25. Radanliev P, De Roure D, Nurse JRC, Nicolescu R, Huth M. Cyber risk from IoT technologies in smart cities. Internet Things. 2020;12:100324. Doi:10.1016/j.iot.2020.100324.
26. Devlin J, Chang MW, Lee K, Toutanova K. BERT: Pre-training of deep bidirectional transformers for language understanding. Proc NAACL-HLT. 2019. Doi:10.18653/v1/N19-1423.
27. Breiman L. Random forests. Mach Learn. 2001;45(1):5-32. Doi:10.1023/A:1010933404324.
28. Gonçalves RM, da Silva MM, da Cunha PR. Olympus: A GDPR compliant blockchain system. Int J Inf Secur. 2024;23:1021-1036. Doi:10.1007/s10207-023-00782-z.
29. Mahindrakar A, Joshi KP. Automating GDPR compliance using policy integrated blockchain. Proc IEEE BigDataSecurity/HPSC/IDS. 2020:86-93. Doi:10.1109/BigDataSecurity-HPSC-IDS49724.2020.00026.
30. Greco CM, Tagarelli A. Bringing order into the realm of transformer-based language models for artificial intelligence and law. Artif Intell Law. 2024;32:863-1010. Doi:10.1007/s10506-023-09374-7.
31. Guitton C, Gubelmann R, Karray G, Mayer S, Tamò-Larrieux A. Identifying open-texture in regulations using LLMs. Artif Intell Law. 2025. Doi:10.1007/s10506-025-09450-0.
32. Oham C, Kundu A, Osman I, Ahmed Y, et al. GDPR compliance verification through a user-centric blockchain approach in multi-cloud environment. Comput Electr Eng. 2023;109:108747. Doi:10.1016/j.compeleceng.2023.108747.
33. Drummer D, Neumann D. Is code law? Current legal and technical adoption issues and remedies for blockchain-enabled smart contracts. J Inf Technol. 2020;35(4):337-360. Doi:10.1177/0268396220924669.
34. Finck M. Smart contracts as a form of solely automated processing under the GDPR. Int Data Priv Law. 2019;9(2):78-94. Doi:10.1093/idpl/ipz004.

35. Eszteri D. Blockchain and artificial intelligence: Connecting two distinct technologies to comply with GDPR's data protection by design principle. Masaryk Univ J Law Technol. 2022;16(1):71-94. Doi:10.5817/MUJLT2022-1-3.
36. Liu LC, Sileno G, Van Engers T. Digital enforceable contracts (DEC): Making smart contracts smarter. Legal Knowledge and Information Systems. 2020. Doi:10.3233/FAIA200872.
37. Dwivedi YK, Hughes L, Baabdullah AM, Ribeiro-Navarrete S, Giannakis M, Al-Debei MM, et al. Artificial intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. Int J Inf Manage. 2021;57:101994. Doi:10.1016/j.ijinfomgt.2019.08.002.
38. Voigt P, Von dem Bussche A. The EU General Data Protection Regulation (GDPR): A Practical Guide. Cham: Springer; 2017.
39. Politou E, Alepis E, Patsakis C. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. J Cybersecur. 2018;4(1):tyy001. Doi:10.1093/cybsec/tyy001.
40. Finck M, Pallas F. They who must not be identified—Distinguishing personal from non-personal data under the GDPR. Int Data Priv Law. 2020;10(1):11-36. Doi:10.1093/idpl/ipz026.
41. Zwitter A, Hazenberg J. Decentralized network governance: Blockchain technology and the future of regulation. Front Blockchain. 2020;3:12. Doi:10.3389/fbloc.2020.00012.
42. Dorri A, Kanhere SS, Jurdak R. Blockchain in Internet of Things: Challenges and solutions. arXiv. 2016;arXiv:1608.05187.
43. Xu X, Weber I, Staples M. Architecture for Blockchain Applications. Cham: Springer; 2019. Doi:10.1007/978-3-030-03035-3.
44. Atzori M. Blockchain technology and decentralized governance: Is the state still necessary? J Gov Regul. 2017;6(1):45-62.
45. Romanov V, Bernsmed K, Baiardi F, et al. Privacy-aware blockchain architectures for regulatory compliance and secure auditing. J Inf Secur Appl. 2024.
46. Kshetri N, Voas J. Blockchain-enabled e-voting. IEEE Softw. 2018;35(4):95-99.Doi:10.1109/MS.2018.2801546.
47. Albrecht JP. How the GDPR will change the world. Eur Data Prot Law Rev. 2016;2(3):287-289.