

METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO DATA

TECHNICAL FIELD

- 5 The present disclosure relates to data management. In particular, the present disclosure relates to methods and systems for the automated negotiation, enforcement, and auditing of data-sharing agreements between different entities.

BACKGROUND

10

In the contemporary digital landscape, enterprises frequently engage in data-sharing agreements to enhance operational efficiency, drive innovation, and gain competitive advantages. However, managing these agreements poses significant challenges, particularly in ensuring compliance with stringent privacy regulations like the European
15 Union General Data Protection Regulation (GDPR) and mitigating biases in shared datasets. Traditional methods of managing data-sharing agreements are often manual, time-consuming, and prone to human error, leading to potential breaches of compliance and ethical standards.

20

SUMMARY

25

The present disclosure introduces a decentralized AI system that autonomously manages the entire lifecycle of data-sharing agreements between organizational entities. The advent of blockchain technology and AI offers promising avenues to
25 address the challenges of managing data-sharing agreements. Blockchain's, or other similar distributed ledger technical framework's immutable ledger provides a transparent and secure method for recording transactions, while AI can automate and optimize various aspects of data management. Integrating these technologies can revolutionize the lifecycle management of data-sharing agreements, ensuring dynamic
30 compliance and ethical data handling. The system leverages blockchain-backed smart contracts and AI agents to negotiate, enforce, and audit data-sharing terms dynamically. Key features of the system include:

1. Smart Contract Integration: Utilizing blockchain technology, the system establishes smart contracts that automatically adjust terms based on real-time data usage patterns.

2. Privacy Protection and Bias Mitigation: AI agents conduct real-time analysis of data flows to detect and correct privacy violations and biases in shared datasets.

3. Self-Healing Compliance: The system automatically rectifies compliance breaches by revoking access or anonymizing data, ensuring continuous adherence to regulations like the GDPR.

The present disclosure provides a robust framework for secure, compliant, and ethical data sharing between enterprises, addressing the limitations of traditional data contract management methods.

According to a first aspect of the present disclosure a method of controlling access to data stored in a data repository is provided. The method comprises: negotiating by a set of artificial intelligence agents to generate a set of smart contract terms; performing a compliance check on the smart contract terms against a data regulation; if the compliance check is successful, deploying a smart contract comprising the set of smart contract terms; and controlling access to the data stored in the data repository using the smart contract.

In an embodiment, controlling access to the data stored in the data repository using the smart contract comprises an artificial intelligence agent of the set of artificial intelligence agents granting a user access to the data stored in the data repository based on the smart contract.

In an embodiment, controlling access to the data stored in the data repository using the smart contract comprises an artificial intelligence agent of the set of artificial intelligence agents monitoring user actions on performed on the data stored in the data repository and if a user action violates a term of the set of smart contract terms, denying access by the user to the data stored in the data repository.

In an embodiment, controlling access to the data stored in the data repository using the smart contract comprises an artificial intelligence agent of the set of artificial intelligence agents performing a transformation on the data stored in the data repository and providing transformed data to a user.

5

In an embodiment, the transformation is defined by a term of the set of smart contract terms.

10 In an embodiment, the negotiating by the set of artificial intelligence agents to generate a set of smart contract terms is based on data sensitivity, data usage purposes and data access permissions.

15 In an embodiment, controlling access to the data stored in the data repository using the smart contract comprises detecting a data privacy violation and triggering a data privacy protection mechanism in response to detecting the data privacy violation.

20 In an embodiment, controlling access to the data stored in the data repository using the smart contract comprises detecting bias in data accessed from the data repository and initiating a bias mitigation process in response to detecting bias in data accessed from the data repository.

25 In an embodiment, controlling access to the data stored in the data repository using the smart contract comprises detecting malicious elements in data accessed from the data repository and initiating a malicious data cleansing process in response to detecting malicious elements in data accessed from the data repository.

In an embodiment, deploying the smart contract comprises storing the smart contract on a distributed ledger.

30 In an embodiment, the method further comprises detecting a change in the data regulation and adapting the set of smart contract terms in response to detecting the change in the data regulation.

In an embodiment, the method further comprises comprising updating an audit log indicating data accessed in the data repository.

According to a second aspect of the present disclosure a computer readable medium storing processor executable instructions which when executed on a processor cause the processor to carry out a method as set out above is provided.

According to a third aspect of the present disclosure, a computer system for controlling access to data stored in a data repository is provided. The computer system is configured to implement a plurality of artificial intelligence agents which implement a method set out above.

In an embodiment, the computer system further comprises a compliance system configured to monitor compliance of the artificial intelligence agents with a data regulation.

In an embodiment, the compliance system is further configured to update terms of the smart contract in response to a change in the data regulation.

BRIEF DESCRIPTION OF THE DRAWINGS

In the following, embodiments of the present invention will be described as non-limiting examples with reference to the accompanying drawings in which:

FIG.1 is a block diagram showing a system architecture of a system for controlling access to data stored in data repositories according to an embodiment of the present invention;

FIG.2 is a block diagram showing an access control agent system according to an embodiment of the present invention;

FIG.3 is a block diagram showing a compliance system according to an embodiment of the present invention;

FIG.4 is a flow chart showing negotiation of smart contracts by artificial intelligence agents according to an embodiment of the present invention;

- 5 FIG.5 is a flowchart showing a method of monitoring access to data using artificial intelligence agents according to an embodiment of the present invention; and

FIG.6 is a flowchart showing compliance monitoring and rectification carried out by a compliance system according to an embodiment of the present invention.

10

DETAILED DESCRIPTION

The present disclosure relates to a decentralized agentic AI system that automates the lifecycle management of data-sharing agreements. By integrating autonomous AI-driven smart contracts, privacy protection and bias detection mechanisms, and self-healing compliance frameworks, the system ensures secure, ethical, and regulatory-compliant data-sharing practices. The invention addresses key challenges in computational efficiency, security, and fairness, offering a scalable and adaptable solution for enterprises across various industries. The main components of the system include:

15

20

1. A method for dynamic term adjustment in smart contracts using AI agents to monitor dataset usage and enforce data governance laws and regulations.
- 25 2. An AI-driven system that detects and mitigates privacy and bias in datasets used by smart contracts (possibly within a distributed ledger or blockchain environment), and self-healing compliance frameworks to ensure continuous adherence to regulations.
- 30 3. A mathematical model for optimizing access control policies in smart contracts through real-time data analysis.

FIG.1 is a block diagram showing a system architecture of a system for controlling access to data stored in data repositories according to an embodiment of the present invention.

- 5 As shown in FIG.1, the system architecture 100 comprises a blockchain network 102, access control agents 110A and 110B, data repositories 112A and 112B and a compliance system 160.

10 The blockchain network 102 is a decentralized ledger that records all transactions related to data-sharing agreements, ensuring transparency and immutability. The blockchain network 102 stores smart contracts 104. The smart contracts 104 are self-executing and they can be deployed on any blockchain network, distributed ledger network or any equally secure network. While FIG.1 shows a blockchain network 102, it will be appreciated that the smart contracts could be implemented on other types of
15 network and thus a blockchain network is not an essential requirement for this system, as long as the smart contracts can be executed on an immutable network.

The smart contracts 104 are-executing contracts with terms encoded directly into code, deployed on the blockchain network 102.

20

The access control agents 120A and 120B are autonomous entities responsible for negotiating, enforcing, and auditing data-sharing agreements. The data repositories 112A and 112B are secure storage locations for shared datasets, accessible based on permissions defined in the smart contracts 104.

25

The compliance system 160 is component that monitors adherence to privacy laws and ethical guidelines, triggering self-healing actions when necessary.

30 In the system architecture 100 shown in FIG.1, there are two entities: entity A 110A and entity B 110B. Entity A 110A has a data repository 112A and entity B has a data repository 112B. The respective data repositories store data which may include sensitive or confidential data. The system architecture 100 allows data sharing agreements between the entities to be initiated and managed. The system architecture 100 also allows monitoring of any data being ingested in the data repositories based

on predefined properties or attributes of data intended to be stored in the respective data repositories.

FIG.2 is a block diagram showing an access control agent system according to an embodiment of the present invention. The access control agent system 120 is a computer system with memory that stores computer program modules which implement data access control methods according to embodiments of the present invention. The access control agent system 120 corresponds to the access control agent 120A of entity A or the access control agent 120B of entity B shown in FIG.1

The access control agent system 120 comprises a processor 130, a working memory 132, an input interface 134, an output interface 136, and program storage 140. The processor 130 may be implemented as one or more central processing unit (CPU) chips. The program storage 140 is a non-volatile storage device such as a hard disk drive which stores computer program modules. The computer program modules are loaded into the working memory 132 for execution by the processor 130. The input interface 134 is an interface which allows data to be received by the access control agent system 120, for example commands or requests for data, communications between the access control agent and the blockchain 102 and smart contracts 104, and communications between the access control agent and the compliance system 160. The input interface 134 may be a wireless network interface such as a Wi-Fi or Bluetooth interface, alternatively it may be a wired interface. The output interface 136 outputs data from the repository which may be transformed as described in more detail below.

The program storage 140 stores negotiation module 142, a monitoring module 144, a bias mitigation module 146, a privacy protection module 148, a privacy audit module 150 and a term adjustment module 152. The computer program modules cause the processor 130 to execute various data access control processing which is described in more detail below. The program storage 140 may be referred to in some contexts as computer readable storage media and/or non-transitory computer readable media. As depicted in FIG.2, the computer program modules are distinct modules which perform respective functions implemented by the access control agent system 120. It will be appreciated that the boundaries between these modules are exemplary only,

and that alternative embodiments may merge modules or impose an alternative decomposition of functionality of modules. For example, the modules discussed herein may be decomposed into sub-modules to be executed as multiple computer processes, and, optionally, on multiple computers. Moreover, alternative embodiments may
5 combine multiple instances of a particular module or sub-module. It will also be appreciated that, while a software implementation of the computer program modules is described herein, these may alternatively be implemented as one or more hardware modules (such as field-programmable gate array(s) or application-specific integrated circuit(s)) comprising circuitry which implements equivalent functionality to that
10 implemented in software.

Although the access control agent system 120 is described with reference to a computer, it should be appreciated that the access control agent system 120 may be formed by two or more computers in communication with each other that collaborate
15 to perform a task. For example, but not by way of limitation, an application may be partitioned in such a way as to permit concurrent and/or parallel processing of the instructions of the application. Alternatively, the data processed by the application may be partitioned in such a way as to permit concurrent and/or parallel processing of different portions of a data set by the two or more computers. In an embodiment,
20 virtualization software may be employed by the access control agent system 120 to provide the functionality of a number of servers that is not directly bound to the number of computers in the access control agent system 120. In an embodiment, the functionality disclosed above may be provided by executing the application and/or applications in a cloud computing environment. Cloud computing may comprise
25 providing computing services via a network connection using dynamically scalable computing resources. A cloud computing environment may be established by an enterprise and/or may be hired on an as-needed basis from a third party provider.

FIG.3 is a block diagram showing a compliance system according to an embodiment
30 of the present invention. The compliance system 160 is a computer system with memory that stores computer program modules which implement data compliance monitoring and control methods according to embodiments of the present invention.

The compliance system 160 comprises a processor 170, a working memory 172, an input interface 174, an output interface 176, and program storage 180. The processor 170 may be implemented as one or more central processing unit (CPU) chips. The program storage 180 is a non-volatile storage device such as a hard disk drive which stores computer program modules. The computer program modules are loaded into the working memory 172 for execution by the processor 170. The input interface 174 is an interface which allows data to be received by the compliance system 120, for example data relating to data regulations, communications between the compliance system 160 and the blockchain 102 and smart contracts 104, and communications between the compliance system 160 and access control agents. The input interface 134 may be a wireless network interface such as a Wi-Fi or Bluetooth interface, alternatively it may be a wired interface. The output interface 136 outputs data such as audit data.

The program storage 180 stores a compliance monitoring module 182, a remediation module 184, a notification module 186, and an audit module 188. The computer program modules cause the processor 170 to execute various compliance processing which is described in more detail below. The program storage 180 may be referred to in some contexts as computer readable storage media and/or non-transitory computer readable media. As depicted in FIG.3, the computer program modules are distinct modules which perform respective functions implemented by the compliance system 160. It will be appreciated that the boundaries between these modules are exemplary only, and that alternative embodiments may merge modules or impose an alternative decomposition of functionality of modules. For example, the modules discussed herein may be decomposed into sub-modules to be executed as multiple computer processes, and, optionally, on multiple computers. Moreover, alternative embodiments may combine multiple instances of a particular module or sub-module. It will also be appreciated that, while a software implementation of the computer program modules is described herein, these may alternatively be implemented as one or more hardware modules (such as field-programmable gate array(s) or application-specific integrated circuit(s)) comprising circuitry which implements equivalent functionality to that implemented in software.

Although the compliance system 160 is described with reference to a computer, it should be appreciated that the compliance system 160 may be formed by two or more computers in communication with each other that collaborate to perform a task. For example, but not by way of limitation, an application may be partitioned in such a way as to permit concurrent and/or parallel processing of the instructions of the application. Alternatively, the data processed by the application may be partitioned in such a way as to permit concurrent and/or parallel processing of different portions of a data set by the two or more computers. In an embodiment, virtualization software may be employed by the compliance system 160 to provide the functionality of a number of servers that is not directly bound to the number of computers in the compliance system 160. In an embodiment, the functionality disclosed above may be provided by executing the application and/or applications in a cloud computing environment. Cloud computing may comprise providing computing services via a network connection using dynamically scalable computing resources. A cloud computing environment may be established by an enterprise and/or may be hired on an as-needed basis from a third party provider.

FIG.4 is a flow chart showing negotiation of smart contracts by artificial intelligence agents according to an embodiment of the present invention.

The method 400 shown in FIG.4 takes place between artificial intelligence agents representing participating entities such as enterprises.

In step 402, the negotiation starts. In step 404, objectives and constraints are defined.

In steps 406-410, each artificial intelligence agent involved in the negotiation assesses as data sensitivity (step 406), usage purposes (step 408), and access permissions (step 410).

Following the negotiation, in step 412, the compliance system 160 performs a compliance check to confirm adherence to privacy laws and ethical guidelines. If the compliance check is successful, the method moves to step 412. If the compliance check is unsuccessful, the method moves to step 414 in which the terms are revised and the method returns to step 404 in which objectives and constraints are re-defined.

Following a successful compliance check, in step 416, the terms are encoded into a smart contract 104. In step 418, the smart contract 104 is deployed on the blockchain network 102. The negotiation then ends in step 420.

5

Once the smart contract has been deployed on the blockchain, the artificial intelligence agents use the smart contract to automatically enforce the agreed-upon terms, granting or restricting data access as specified. The artificial intelligence agents monitor data usage in real-time to ensure adherence to the contract terms.

10

The smart contracts serve as the backbone of the system, providing a secure and transparent mechanism for enforcing data-sharing terms. Deployed on a blockchain network, these contracts offer the following advantages:

- 15 Immutability: Once deployed, smart contracts cannot be altered, ensuring that the agreed-upon terms remain consistent throughout the contract's lifecycle.

Transparency: All transactions and contract executions are recorded on the blockchain, providing an auditable trail of actions.

20

Automation: Smart contracts automatically execute predefined actions when specific conditions are met, reducing the need for manual intervention.

In the context of this disclosure, smart contracts are utilized to:

25

Define Access Permissions: Specify which entities have access to particular datasets and under what conditions.

30 Set Usage Constraints: Outline permissible data usage conditions. The system ensures that data usage adheres to predefined constraints, such as permissible processing methods, data retention periods, and access levels.

Artificial Intelligence agents continuously monitor data access patterns and flag potential violations, triggering real-time contract modifications if necessary.

The smart contracts define thresholds for data access, such as frequency and volume limits, ensuring that data is not misused beyond agreed-upon terms.

5 It is noted that from the conceptual point of view, smart contracts are self-executing agreements with terms encoded directly into software. While they are most commonly associated with blockchain technology, they can, in fact, be executed independently of a blockchain. In non-blockchain contexts, smart contracts can operate within centralized systems or utilize trusted third parties for execution. For instance,
10 traditional server-client architectures can host smart contracts, where a central authority manages contract execution. This approach can offer advantages in terms of performance and scalability, as it doesn't rely on the distributed consensus mechanisms inherent to blockchains. However, this centralization reintroduces the need for trust in the managing authority and may lack the transparency and
15 immutability that blockchain-based smart contracts provide.

In summary, while blockchain provides a decentralized and tamper-proof environment ideal for many smart contract applications, it is not an absolute requirement. Smart contracts can be executed independently of blockchain, though this often involves
20 trade-offs concerning trust, transparency, and security.

FIG.5 is a flowchart showing a method of monitoring access to data using artificial intelligence agents according to an embodiment of the present invention. The method
500 shown in FIG.5 is carried out by the access control agents 120A and 120B shown
25 in FIG.1 after a smart contract corresponding to a data-sharing or data access has been deployed on the blockchain network 102.

As shown in FIG.5, an artificial intelligence agent monitors data flow 504 from a data source 504. This monitoring comprises privacy violation detection 506 and bias
30 detection 514. Techniques such as clustering algorithms and fairness metrics are employed to identify and mitigate biases.

If during privacy violation detection 506, a violation is found in step 508, the method moves to step 510 in which a privacy protection mechanism is triggered. Following the

triggering of a privacy protection mechanism in step 510 the method moves to step 512 and monitoring continues. If no privacy violation is found in step 508, the method moves to step 512 and monitoring continues.

- 5 If during bias detection 514, a bias in the data is found in step 516, the method moves to step 518 in which a bias mitigation process is initiated. Following the initiation of a bias mitigation process in step 518 the method moves to step 512 and monitoring continues. If no bias is found in step 516, the method moves to step 512 and monitoring continues.

10

The system employs AI-powered privacy protection mechanisms and fairness evaluation algorithms to ensure ethical data handling.

- 15 In the bias detection 514 step, the AI agents apply statistical and algorithmic fairness tests, such as disparate impact analysis and counterfactual fairness evaluations, to detect biases in shared datasets. The system leverages techniques such as reweighting, adversarial debiasing, and fair representation learning to mitigate biases in step 518 and enhance equity in downstream decision-making processes.

- 20 Continuous bias auditing is performed using fairness-aware machine learning models to detect evolving biases in data-sharing agreements.

- 25 In some embodiments, the method may comprise detecting malicious data. Here malicious data refers to data capable of poisoning or hijack attacks. This the controlling of access to the computational resource using the smart contract comprises detecting malicious elements in data accessed from the data repository and initiating a malicious data cleansing process in response to detecting malicious elements in data accessed from the data repository

- 30 In the privacy violation detection step 506, to protect personally identifiable information (PII), the system employs data anonymization techniques such as k-anonymity, l-diversity, and t-closeness. AI-powered differential privacy mechanisms ensure that no single data point can be reconstructed from aggregated datasets. The system

dynamically adjusts the privacy budget based on regulatory requirements and organizational risk tolerance, balancing privacy protection and data utility.

The system provides real-time privacy audits. AI agents monitor data-sharing activities in real-time, detecting privacy risks and triggering automated interventions if necessary. The system generates cryptographically verifiable audit logs for regulatory compliance and forensic investigations. Blockchain-integrated privacy enforcement ensures that all data transactions remain transparent and tamper-proof.

In some embodiments, the term adjustment module 152 of the access control agent system 120 functions to dynamically adjust access control policies.

The dynamic adjustment of access control policies can be modeled as follows:

Let $T = \{t_1, t_2, \dots, t_n\}$ represent the set of terms for a smart contract, where each term t_i has associated parameters such as access level (AL_i) and sharing conditions (SC_i). The AI agent monitors dataset usage metrics (MU_j) over time to adjust these parameters. The adjustment is governed by:

$$AL_i^{new} = f(MU_j, T),$$

where f represents the function that maps usage metrics and current terms to new access levels.

To detect biases in datasets used within smart contracts, a bias detection algorithm (BDA_k) is employed:

$$BDA_k = g(D_k, C_l),$$

where D_k represents the dataset of interest, and C_l are context variables such as contract specifications. The function g identifies biases that may affect decision-making fairness. A similar formulation can be applied to privacy protection and fairness optimization.

FIG.6 is a flowchart showing compliance monitoring and rectification carried out by a compliance system according to an embodiment of the present invention. The method

600 shown in FIG.6 is carried out by the compliance system 160 shown in FIG.1 acting with the access control agents 120A and 120B.

5 In step 602, the compliance monitoring module 182 of the compliance system 160 is executed to start monitoring. The compliance system 160 continuously monitors for breaches of privacy laws or ethical guidelines.

10 In step 604, a compliance breach is detected. In step 606, the type of breach is determined. As shown in FIG.6 examples of types of breach are an access violation, a data sensitivity issue and a contractual breach. Upon detecting a breach, the system automatically revokes data access or anonymizes sensitive data to restore compliance.

15 The remediation module 184 of the compliance system 160 is executed to rectify the breach and restore compliance. As shown in FIG.6, following an access violation, data access is revoked in step 608; following detection of a data sensitivity issue, data is anonymized in step 610 and following a contractual breach a smart contract is modified in step 612.

20 Following the rectification in step 608-612, the action is logged in step 614. In step 616, the notification module 186 of the compliance system 160 is executed to notify stakeholders.

25 In step 618, the audit record module 188 of the compliance system 160 is executed to update compliance records.

In step 620, the compliance monitoring module 182 of the compliance system 160 is executed to continue monitoring.

30 The compliance system provides automated compliance monitoring. The compliance system continuously tracks changes in global data regulations (e.g., privacy laws like GDPR and CCPA) and adapts contract terms accordingly. AI-powered natural language processing (NLP) models interpret regulatory updates and assess their impact on existing data-sharing agreements. Compliance scores are dynamically

updated, and stakeholders receive automated notifications when contract amendments are required.

As described above, the compliance system also provides for automated remediation of non-compliance. Upon detecting non-compliance, the system initiates corrective actions, such as revoking access, applying data anonymization, or modifying contract terms. Smart contracts may incorporate predefined compliance violation thresholds, ensuring automatic enforcement of corrective measures. Blockchain-based dispute resolution mechanisms facilitate transparent remediation, enabling enterprises to challenge non-compliance determinations.

The decentralized AI system incorporates robust security mechanisms to safeguard data integrity and prevent fraudulent activities.

AI-Powered Threat Detection

AI-driven anomaly detection models continuously monitor system activity, identifying potential security breaches such as unauthorized access, data exfiltration, and insider threats.

Behavioral analytics and zero-trust security principles ensure that only authorized entities can access data-sharing agreements.

Blockchain-Backed Integrity Verification

The system maintains an immutable blockchain ledger that records all contract executions, ensuring verifiable audit trails.

Digital signatures and cryptographic hashing techniques guarantee data integrity, preventing tampering and unauthorized modifications.

Smart contract-based access control enforces strict identity verification, ensuring that only legitimate parties can modify or terminate agreements.

The integration of AI and smart contracts within decentralized data-sharing environments presents unique technical and operational challenges.

Computational Efficiency

5

AI-powered smart contract execution can be computationally intensive, potentially increasing transaction costs and latency. Solution: The system employs lightweight machine learning models and edge computing techniques to optimize computational efficiency.

10

Federated learning approaches enable decentralized AI training without excessive computational overhead.

Security and Privacy Risks

15

Decentralized AI systems are susceptible to adversarial attacks and privacy leakage. Solution: Homomorphic encryption and secure multi-party computation techniques safeguard sensitive data during AI processing. AI-based anomaly detection models proactively identify and mitigate potential security threats.

20

Scalability and Interoperability

Managing large-scale data-sharing agreements across multiple enterprises requires seamless interoperability. Solution: The system employs standardized smart contract templates and API-based integrations to ensure compatibility with diverse enterprise data infrastructures.

The proposed system offers several advantages over traditional data-sharing contract management approaches.

30

Enhanced Compliance and Regulatory Adaptability. AI-powered compliance monitoring ensures real-time adherence to evolving privacy regulations, reducing legal risks. The self-healing mechanism automates regulatory updates, minimizing manual intervention.

Improved Security and Data Integrity. Blockchain-backed audit trails provide verifiable transparency, enhancing trust in data-sharing agreements. Cryptographic integrity verification prevents unauthorized data modifications.

5

Fairness and Ethical AI Governance. AI-driven bias mitigation techniques ensure equitable data-sharing practices, fostering responsible AI adoption. Privacy-preserving AI methods protect sensitive information while maintaining analytical utility.

- 10 The embodiments disclosed in the present disclosure are applicable across various industries where secure and compliant data sharing is critical.

Financial Services

- 15 Secure data-sharing agreements between banks, insurance companies, and fintech providers for fraud detection, credit scoring, and risk assessment. AI-driven compliance monitoring ensures adherence to financial regulations such as GDPR and PCI-DSS.

Healthcare and Life Sciences

- 20 Privacy-preserving data exchanges between hospitals, research institutions, and pharmaceutical companies for medical research and drug discovery. Differential privacy and federated learning enable secure AI-driven insights without exposing patient data.

- 25 Supply Chain and Logistics

Secure data-sharing frameworks for supply chain partners to enhance transparency, traceability, and operational efficiency. AI-powered contract enforcement ensures compliance with trade regulations and ethical sourcing standards.

- 30 Government and Public Sector

Decentralized AI governance for data-sharing agreements in e-government services, law enforcement, and social programs. Smart contracts facilitate transparent public-sector data transactions while ensuring privacy compliance.

Whilst the foregoing description has described exemplary embodiments, it will be understood by those skilled in the art that many variations of the embodiments can be made within the scope and spirit of the present invention.

CLAIMS

1. A method of controlling access to data stored in a data repository, the method comprising:
 - negotiating by a set of artificial intelligence agents to generate a set of smart contract terms;
 - performing a compliance check on the smart contract terms against a data regulation;
 - if the compliance check is successful, deploying a smart contract comprising the set of smart contract terms; and
 - controlling access to the data stored in the data repository using the smart contract.
2. The method according to claim 1, wherein controlling access to the data stored in the data repository using the smart contract comprises an artificial intelligence agent of the set of artificial intelligence agents granting a user access to the data stored in the data repository based on the smart contract.
3. The method according to claim 1, wherein controlling access to the data stored in the data repository using the smart contract comprises an artificial intelligence agent of the set of artificial intelligence agents monitoring user actions on performed on the data stored in the data repository and if a user action violates a term of the set of smart contract terms, denying access by the user to the data stored in the data repository.
4. The method according to claim 1, wherein controlling access to the data stored in the data repository using the smart contract comprises an artificial intelligence agent of the set of artificial intelligence agents performing a transformation on the data stored in the data repository and providing transformed data to a user.
5. The method according to claim 4, wherein the transformation is defined by a term of the set of smart contract terms.

6. The method according to any preceding claim, wherein the negotiating by the set of artificial intelligence agents to generate a set of smart contract terms is based on data sensitivity, data usage purposes and data access permissions.
7. The method according to any preceding claim, wherein controlling access to the data stored in the data repository using the smart contract comprises detecting a data privacy violation and triggering a data privacy protection mechanism in response to detecting the data privacy violation.
8. The method according to any preceding claim, wherein controlling access to the data stored in the data repository using the smart contract comprises detecting bias in data accessed from the data repository and initiating a bias mitigation process in response to detecting bias in data accessed from the data repository.
9. The method according to any preceding claim, wherein controlling access to the data stored in the data repository using the smart contract comprises detecting malicious elements in data accessed from the data repository and initiating a malicious data cleansing process in response to detecting malicious elements in data accessed from the data repository.
10. The method according to any preceding claim, wherein deploying the smart contract comprises storing the smart contract on a distributed ledger.
11. The method according to any preceding claim, further comprising detecting a change in the data regulation and adapting the set of smart contract terms in response to detecting the change in the data regulation.
12. The method according to any preceding claim, further comprising updating an audit log indicating data accessed in the data repository.
13. A computer readable medium storing processor executable instructions which when executed on a processor cause the processor to carry out a method according to any one of claims 1 to 12.

14. A computer system for controlling access to data stored in a data repository, the computer system configured to implement a plurality of artificial intelligence agents which implement a method according to any one of claims 1 to 12.

15. The computer system according to claim 13, further comprising a compliance system configured to monitor compliance of the artificial intelligence agents with a data regulation.