UNITED STATES PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
PCT/US25/20835	**03/21/2025 11:53:10 AM Z ET**	**-**

Title of Invention

AI Powered Licensing Enforcement and Compliance System

Application Information

APPLICATION TYPE	International Application (PCT) for filing in the US receiving office	PATENT #	-
CONFIRMATION #	8667	FILED BY	TENG LI
PATENT CENTER #	69682108	FILING DATE	-
CUSTOMER #	–	APPLICANT NAME	NEVERMISSED LICENSED TRUST
CORRESPONDENCE ADDRESS	TENG ZHI LI 2 PRINCES STREET PORT ADELAIDE, AU	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 1

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
xlicense.pdf	14	Specification	303 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
xlicense.pdf	27B1621AF63FF75ACDAFB47715BBF3BB02927665B8866E3B0 CDF8E660418455F380BC40ABEC797F98E088C5CADFDEC45A AB284B40092BBC06CC3F60436E99ADE

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Title

SmartLicense-X: AI Powered Licensing Enforcement and Compliance System

---

Applicant Information:

Full Name: NEVERMISSED LICENSED TRUST
Address: 2 Princes Street, Port Adelaide SA 5015, Australia
Country of Nationality and Residence: Australia

Inventor Information:

Name: TENG ZHI LI
Address: 2 Princes Street, Port Adelaide SA 5015, Australia

Country of Nationality and Residence: Australia

Title of Invention:
SmartLicense-X: AI Powered Licensing Enforcement and Compliance System
Receiving Office:
Specify the receiving office where you intend to file the application.

Table of Contents

Abstract

SmartLicense-X is an AI powered licensing and compliance enforcement system designed to detect, monitor, and regulate unauthorized AI model usage. The system integrates behavioral fraud detection, deception based licensing traps, blockchain smart contract enforcement, and automated regulatory reporting. It prevents AI misuse, detects licensing violations in real time, and applies financial and access penalties using decentralized infrastructure. SmartLicense-X supports compliance enforcement across government agencies, financial institutions, cloud service providers, and regulated AI deployments.

Technical Field

The invention relates to artificial intelligence governance, licensing compliance, fraud detection, and smart contract based enforcement. It applies behavioral AI analytics, federated fraud intelligence, deception driven traps, and blockchain validation to automate licensing control and regulatory enforcement across AI powered systems.

Background of the Invention

As artificial intelligence becomes foundational to financial systems, cybersecurity, carbon markets, and enterprise infrastructure, licensing misuse and AI fraud have increased dramatically. Existing licensing systems are reactive, static, and unable to detect unauthorized model reuse or cloning in real time. This creates regulatory, financial, and operational risk.

Many current tools lack deception based detection techniques, smart contract enforcement, or federated learning based anomaly tracking. Regulators including the Securities and Exchange Commission and oversight authorities under the European Union AI Act now require provable licensing and compliance automation. However, existing solutions fail to deliver such enforceable frameworks.

Summary of the Invention

SmartLicense-X introduces a layered AI enforcement system comprising:

- A real time AI fraud detection engine that applies behavioral anomaly analysis to detect misuse
- Deception based honeypot traps that simulate AI APIs and licensing endpoints to detect unauthorized model access
- A blockchain smart contract licensing enforcement engine that controls access, fee payments, and license status
- A regulatory reporting interface for real time compliance submission to oversight bodies
- A federated AI monitoring network that shares anonymized fraud patterns across enterprise and public infrastructures

The system dynamically enforces AI model licensing across private, public, and hybrid environments. It detects violations, penalizes misuse, and ensures compliance via blockchain enforced contracts and autonomous fraud response.

Detailed Description of the Invention

1. AI Fraud Detection Engine

The AI fraud detection engine continuously monitors model execution behavior, access logs, usage patterns, and API activity to identify unauthorized or cloned deployments.

- Behavioral scoring models compare runtime data against baseline behavior of licensed models
- Federated anomaly detection shares indicators across monitoring nodes
- Violations are detected based on deviations in execution flow, access frequency, or model input response signatures

2. Deception Driven Compliance Traps

SmartLicense-X deploys honeypot models and fake license validation endpoints to lure potential unauthorized users or AI cloners.

- Simulated API endpoints and licensing servers detect suspicious traffic
- When triggered, the deception engine logs behavior, injects misleading outputs, and flags sources for further enforcement
- Reverse manipulation corrupts adversarial AI models by feeding false learning data, preventing effective model reuse

3. Smart Contract Licensing and Penalty Enforcement

Each AI model instance must validate its license via a blockchain smart contract ledger prior to activation.

- Smart contracts verify signature tokens, model IDs, and usage limits
- If violations are detected, contracts apply penalties such as throttling, key revocation, or financial deductions
- A tamper proof usage log ensures traceable enforcement records

4. Federated Monitoring and Regulatory Compliance

SmartLicense-X enables privacy preserving sharing of fraud signals across AI license networks using federated learning protocols.

- Oversight regulators such as the Securities and Exchange Commission and European AI authorities receive automated compliance reports
- These include model IDs, timestamps, behavioral logs, and licensing history
- Carbon credit registries and fintech fraud monitoring agencies also receive tailored fraud notifications

---

Independent Claims

Claim 1

An artificial intelligence licensing enforcement system comprising:

- An AI fraud detection engine configured to analyze model behavior, access frequency, and anomaly signatures to detect unauthorized model usage
- A deception driven compliance module comprising simulated license endpoints and honeypot APIs to detect AI misuse
- A blockchain based smart contract engine configured to verify licensing credentials, enforce access controls, and log transactions immutably
- An automated penalty system configured to apply financial deductions, model throttling, or access revocation based on policy violations

Claim 2

The system of claim 1, wherein the fraud detection engine applies federated behavioral analysis to monitor AI activity across distributed cloud environments.

Claim 3

The system of claim 1, wherein the deception compliance module simulates license responses to identify unauthorized attempts and activate reverse manipulation countermeasures.

Claim 4

The system of claim 1, wherein the blockchain engine performs real time enforcement of licensing fees, access validation, and penalty execution without manual intervention.

Claim 5

The system of claim 1, wherein the penalty system is integrated with a regulatory notification protocol that sends structured reports to compliance authorities in response

to AI violations.

Flowcharts and Diagrams (Placeholder Descriptions)

Figure 1 illustrates the core enforcement workflow of SmartLicense-X,

showing how AI models are deployed, license keys are validated, fraud signals are monitored, and smart contracts are triggered to enforce penalties or access restrictions.

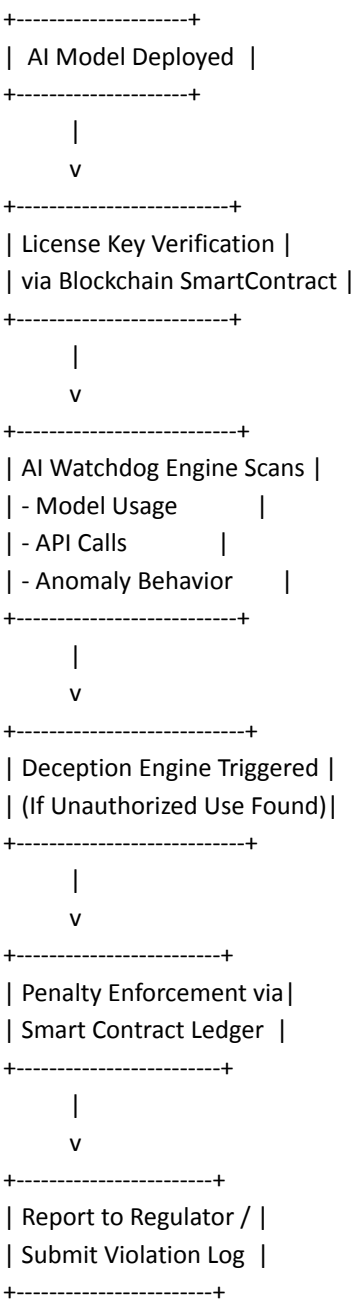


Figure 2 shows the internal structure of the deception-driven fraud detection engine, *including honeypot APIs, simulated model endpoints, behavior logging modules, and adversarial data corruption layers.*

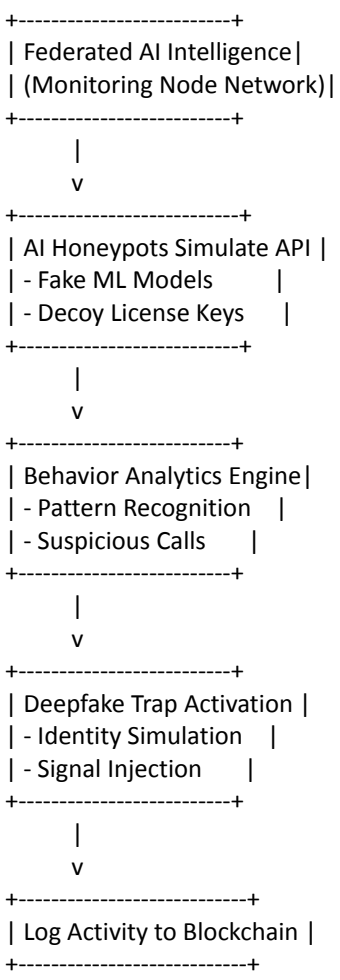
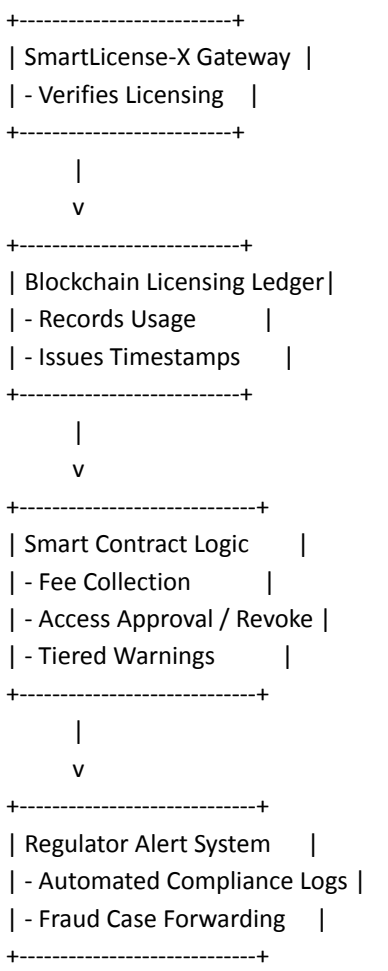


Figure 3 – Blockchain Enforcement Flow

Depicts smart contract logic for license validation, access revocation, tiered penalties, and regulatory alert triggers.



Conclusion

SmartLicense-X provides a foundational platform for AI governance, capable of autonomous licensing enforcement, fraud detection, and regulatory reporting. By combining federated AI monitoring, deception traps, blockchain verification, and smart contract logic, the system delivers enforceable, scalable, and tamper proof AI compliance infrastructure.

Title

SmartLicense-X: AI Powered Licensing Enforcement and Compliance System

---

Applicant Information:

Full Name: NEVERMISSED LICENSED TRUST
Address: 2 Princes Street, Port Adelaide SA 5015, Australia
Country of Nationality and Residence: Australia

Inventor Information:

Name: TENG ZHI LI
Address: 2 Princes Street, Port Adelaide SA 5015, Australia

Country of Nationality and Residence: Australia

Title of Invention:
SmartLicense-X: AI Powered Licensing Enforcement and Compliance System
Receiving Office:
Specify the receiving office where you intend to file the application.

Table of Contents

Abstract

SmartLicense-X is an AI powered licensing and compliance enforcement system designed to detect, monitor, and regulate unauthorized AI model usage. The system integrates behavioral fraud detection, deception based licensing traps, blockchain smart contract enforcement, and automated regulatory reporting. It prevents AI misuse, detects licensing violations in real time, and applies financial and access penalties using decentralized infrastructure. SmartLicense-X supports compliance enforcement across government agencies, financial institutions, cloud service providers, and regulated AI deployments.

Technical Field

The invention relates to artificial intelligence governance, licensing compliance, fraud detection, and smart contract based enforcement. It applies behavioral AI analytics, federated fraud intelligence, deception driven traps, and blockchain validation to automate licensing control and regulatory enforcement across AI powered systems.

Background of the Invention

As artificial intelligence becomes foundational to financial systems, cybersecurity, carbon markets, and enterprise infrastructure, licensing misuse and AI fraud have increased dramatically. Existing licensing systems are reactive, static, and unable to detect unauthorized model reuse or cloning in real time. This creates regulatory, financial, and operational risk.

Many current tools lack deception based detection techniques, smart contract enforcement, or federated learning based anomaly tracking. Regulators including the Securities and Exchange Commission and oversight authorities under the European Union AI Act now require provable licensing and compliance automation. However, existing solutions fail to deliver such enforceable frameworks.

Summary of the Invention

SmartLicense-X introduces a layered AI enforcement system comprising:

- A real time AI fraud detection engine that applies behavioral anomaly analysis to detect misuse
- Deception based honeypot traps that simulate AI APIs and licensing endpoints to detect unauthorized model access
- A blockchain smart contract licensing enforcement engine that controls access, fee payments, and license status
- A regulatory reporting interface for real time compliance submission to oversight bodies
- A federated AI monitoring network that shares anonymized fraud patterns across enterprise and public infrastructures

The system dynamically enforces AI model licensing across private, public, and hybrid environments. It detects violations, penalizes misuse, and ensures compliance via blockchain enforced contracts and autonomous fraud response.

Detailed Description of the Invention

1. AI Fraud Detection Engine

The AI fraud detection engine continuously monitors model execution behavior, access logs, usage patterns, and API activity to identify unauthorized or cloned deployments.

- Behavioral scoring models compare runtime data against baseline behavior of licensed models
- Federated anomaly detection shares indicators across monitoring nodes
- Violations are detected based on deviations in execution flow, access frequency, or model input response signatures

2. Deception Driven Compliance Traps

SmartLicense-X deploys honeypot models and fake license validation endpoints to lure potential unauthorized users or AI cloners.

- Simulated API endpoints and licensing servers detect suspicious traffic
- When triggered, the deception engine logs behavior, injects misleading outputs, and flags sources for further enforcement
- Reverse manipulation corrupts adversarial AI models by feeding false learning data, preventing effective model reuse

3. Smart Contract Licensing and Penalty Enforcement

Each AI model instance must validate its license via a blockchain smart contract ledger prior to activation.

- Smart contracts verify signature tokens, model IDs, and usage limits
- If violations are detected, contracts apply penalties such as throttling, key revocation, or financial deductions
- A tamper proof usage log ensures traceable enforcement records

4. Federated Monitoring and Regulatory Compliance

SmartLicense-X enables privacy preserving sharing of fraud signals across AI license networks using federated learning protocols.

- Oversight regulators such as the Securities and Exchange Commission and European AI authorities receive automated compliance reports
- These include model IDs, timestamps, behavioral logs, and licensing history
- Carbon credit registries and fintech fraud monitoring agencies also receive tailored fraud notifications

---

Independent Claims

Claim 1

An artificial intelligence licensing enforcement system comprising:

- An AI fraud detection engine configured to analyze model behavior, access frequency, and anomaly signatures to detect unauthorized model usage
- A deception driven compliance module comprising simulated license endpoints and honeypot APIs to detect AI misuse
- A blockchain based smart contract engine configured to verify licensing credentials, enforce access controls, and log transactions immutably
- An automated penalty system configured to apply financial deductions, model throttling, or access revocation based on policy violations

Claim 2

The system of claim 1, wherein the fraud detection engine applies federated behavioral analysis to monitor AI activity across distributed cloud environments.

Claim 3

The system of claim 1, wherein the deception compliance module simulates license responses to identify unauthorized attempts and activate reverse manipulation countermeasures.

Claim 4

The system of claim 1, wherein the blockchain engine performs real time enforcement of licensing fees, access validation, and penalty execution without manual intervention.

Claim 5

The system of claim 1, wherein the penalty system is integrated with a regulatory notification protocol that sends structured reports to compliance authorities in response

to AI violations.

Flowcharts and Diagrams (Placeholder Descriptions)

Figure 1 illustrates the core enforcement workflow of SmartLicense-X,

showing how AI models are deployed, license keys are validated, fraud signals are monitored, and smart contracts are triggered to enforce penalties or access restrictions.

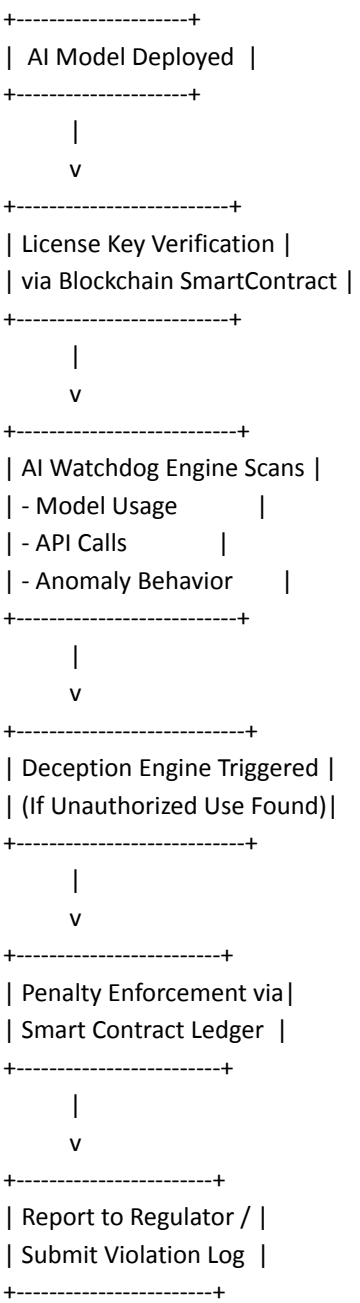


Figure 2 shows the internal structure of the deception-driven fraud detection engine, *including honeypot APIs, simulated model endpoints, behavior logging modules, and adversarial data corruption layers.*

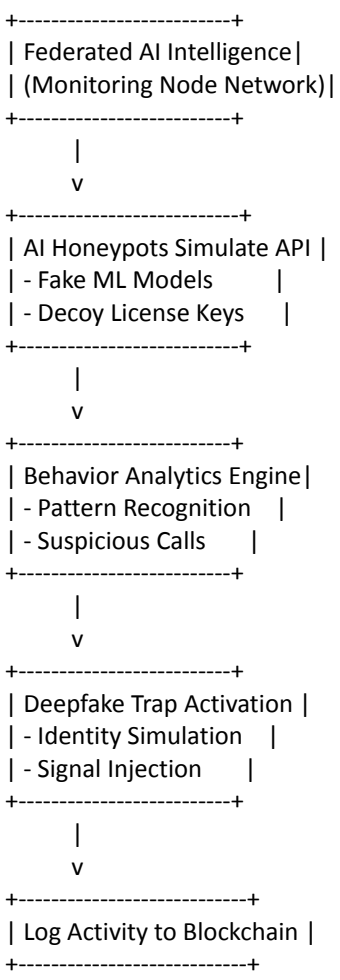
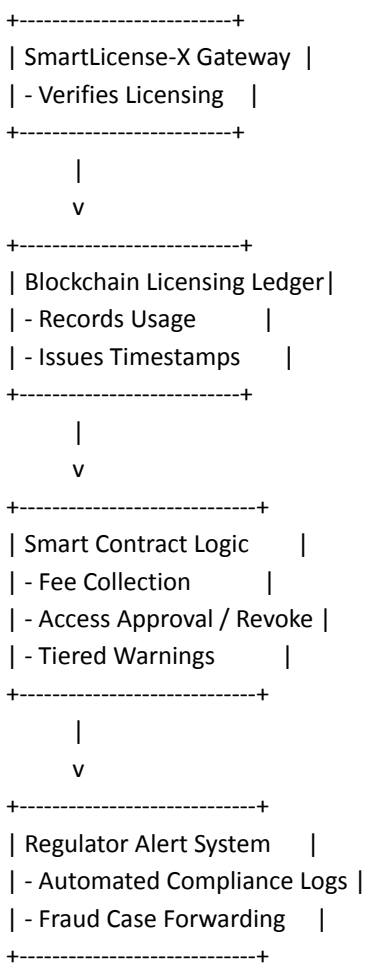


Figure 3 – Blockchain Enforcement Flow

Depicts smart contract logic for license validation, access revocation, tiered penalties, and regulatory alert triggers.



Conclusion

SmartLicense-X provides a foundational platform for AI governance, capable of autonomous licensing enforcement, fraud detection, and regulatory reporting. By combining federated AI monitoring, deception traps, blockchain verification, and smart contract logic, the system delivers enforceable, scalable, and tamper proof AI compliance infrastructure.