

A SYSTEM AND METHOD TO REGISTER, IDENTIFY AND AUTHENTICATE ENTITY ON DIGITAL PLATFORM

TECHNICAL FIELD

The present invention pertains to the field of digital security and identity verification, expanding upon the foundational feature established by the previously patented invention (MY Patent No. MY-196087-A) that focused on a system and method for conducting lawsuit over offensive content through telecommunication and networking system. In contrast, the current invention relates to system and methods for registering, identifying, and authenticating entities on digital platforms. The entities in question can include, but are not limited to, individuals, organizations, electronic devices, programs, websites, and browsers. The invention encompasses a centralized approach, leveraging a unified database and a set of protocols, to ensure the legitimacy of entities operating in digital environments, thereby mitigating risks associated with digital corruption and cybercrimes.

BACKGROUND ART

The digital age has revolutionized the manner in which entities communicate and transact, ushering in a new era where activities, ranging from casual interactions to complex business dealings, are facilitated over vast telecommunication and networking systems. Platforms such as social networks, messaging services, forums, and various websites have paved the way for real-time sharing and exchange of information. Despite the benefits of such technological advancements, they have inadvertently given rise to challenges related to identification and authentication of these entities, making the digital realm susceptible to cybercrimes. Cybercrimes,

including but not limited to bullying, defamation, phishing, identity theft, ransomware attacks, fraud and hacking, are alarmingly rampant.

Perpetrators exploit advanced technologies like proxy servers and encryption to cloak their true identities. By routing their activities across multiple countries, they effectively
5 obscure their trails, rendering detection a difficult task. Such deceptive practices not only disrupt virtual platforms but also have tangible repercussions, leading to significant financial losses amounting to billions or trillions of dollars annually for the government, businesses and individuals alike. Given this backdrop, there is an urgent and pressing need for a reliable system that can accurately identify and authenticate
10 online users globally, ensuring the integrity and safety of digital interactions.

In this challenging landscape, prior art US2014337243A1 introduces a unique method for authenticating a user, employing a system that records and compares specific user characteristics, including kinetic motions, during task performance. This authentication occurs within a structured workflow, wherein recorded information associated with the
15 user's interactions, notably their kinetic responses, is compared with a stored user profile. While innovative in its approach to harnessing physical interactions as authentication criteria, the system's application remains significantly limited. It is designed to verify individual user identity based on these unique interaction patterns, lacking a comprehensive approach that accounts for diverse types of entities and more
20 complex authentication scenarios across various digital platforms. Moreover, it does not provide a universal solution for broader cybersecurity challenges, as its verification process is confined to the specifics of user-device interaction within a narrow context.

Similarly, prior art CA2532538A1 presents an apparatus and method for authenticating users specifically when accessing multimedia services. While it proposes a

mechanism for re-using authentication data across different services, it is narrowly focused on multimedia content access, leaving a wide gap in security measures for other forms of digital interactions and services. Its scope is insufficient in the face of diverse cyber threats and complex digital ecosystems, as it does not provide a holistic
5 approach to secure digital identification and authentication across various platforms and entity types.

In this context, the precedent invention, as detailed in MY Patent No. MY-196087-A, provides an innovative approach for conducting electronic lawsuits over offensive content through telecommunication and networking systems. This system offers
10 capabilities like generating reporting links for third-party platforms, identifying and locating defendants based on their network details, and facilitating plaintiff actions through the platform. However, while it laid foundational groundwork in identity detection, it emphasized legal aspects over a broader spectrum of digital interactions and didn't provide a complete solution for registration and real-time authentication
15 across different types of entities prior accessing the digital platform. The present invention seeks to build upon and integrate with this foundational system, introducing enhanced functionalities that cater to entity verification using unique identifiers.

Given the above, there's a necessity for a solution that bridges these gaps – one that isn't solely focused on one aspect of the challenge but seeks to provide a
20 comprehensive, real-time, and centralized system for digital identification and authentication for diverse entities operating in the digital realm, ensuring security, transparency, and accuracy. The present invention emerges as this bridge, integrating the strengths of previous solutions while addressing their limitations, thereby offering a robust framework for the modern digital era. It proposes a comprehensive, real-time,
25 and centralized system for digital identification and authentication of entities via unique

identifiers, enhancing the safety and integrity of digital communications and transactions across various platforms.

Therefore, the present invention integrates with the innovative aspects of the original patented invention and also significantly extends its functionalities. It embarks on
5 providing a centralized, real-time solution for digital identification and authentication, crucially mitigating risks associated with digital corruption and other forms of cybercrimes.

SUMMARY OF THE INVENTION

The present invention discloses a comprehensive solution to the challenges in the
10 digital security era, particularly focusing on the identification and authentication of various entities operating online.

The invention is distinguished by its centralized system and method for registration, identification and authentication of entities including but not limited to individuals, organizations, electronic devices, programs, websites, and browsers, ensuring a wide-
15 ranging application. Unlike the system described in MY Patent No. MY-196087-A that partially addressed the feature of detecting the identity and location of the alleged offender, this present invention provides a more detailed framework equipped with several key modules that work in synergy to ensure a secure digital environment.

The system operates under the governance of organizations such as government
20 body or its intermediary agencies, or, private organizations, to ensure compliance with legal standards and enhancing trust among users.

This disclosure describes a system to register, identify and authenticate entity on digital platform, comprising a registration and identification module configured to collect, verify, and store identifying information of entities; an identifier generator or

capturer configured to create, assign or capture a unique identifier to each registered entity; a registry database configured to maintain comprehensive of registered entities, including their assigned unique identifier and collected identifying information; an authentication module that cross-references entered unique identifier with the
5 corresponding details in the registry database to verify entities' identities during access attempts on digital platform; a digital footprint capturer configured to record online activities of the entity, establishing a behaviour log for each; a notification module that triggers alerts to the recognized entity of the unique identifier in cases of unusual activity suggesting potential cyber threats; and a platform that facilitates requests for
10 entity authentication confirmations, entity information retrievals, and submissions of suspected fraudulent activities or other potential cyber threats by other entities.

In addition to that, this disclosure also describes a method for registering, identifying, and authenticating an entity on digital platform, comprising the steps of registering and identifying an entity seeking registration, wherein said entity provides its associated
15 details; generating or capturing a unique identifier specific to the registered entity; storing the registered entity's detailed information and its unique identifier in a registry database; authenticating the entity by cross-referencing the provided unique identifier with the details stored in the registry database; capturing and logging a digital footprint of the entity during its online interactions on a digital platform, wherein the digital
20 footprint comprises records of the entity's online activities; and facilitating request for confirming entity authentication confirmations, entity information retrievals, and submissions of report related to suspected fraudulent activities or other potential cyber threats by other entities.

In summary, the present invention represents a significant advancement in
25 cybersecurity, providing a system and method for entity registration and

authentication. By bridging the gaps left by earlier prior arts, it establishes a new standard in digital security protocols, ensuring a safer online environment for all entities involved.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

- 5 In the following detailed description, the embodiments described are not meant to be limiting. Other embodiments may be utilized, and other changes may be made, without departing from the spirit or scope of the subject matter presented herein.

While this invention is described in terms of the best mode for achieving this invention's objectives, it will be appreciated by those skilled in the art that variations may be
10 accomplished in view of these teachings without deviating from the spirit or scope of the present invention.

This description provides comprehensive information regarding system and method to register, identify and authenticate entity, aiming to enhance cybersecurity measures and mitigate potential digital corruption and cybercrimes. In this context, the term
15 "entities" refers to, including, but not limited to individuals, organizations, electronic devices, programs, websites, or browsers within the digital platform. In this context, a "program" refers to any form of coding available on the digital platform, including, but not limited to, software and mobile applications, each of which could potentially serve as a target or medium for cyber activities. Herein, the term "digital platform"
20 encompasses any platform or medium capable of transmitting signals, thereby enabling the transmission and exchange of all forms of data or information. Furthermore, the term "authority" refers to private organizations or government body such as Malaysian Communications and Multimedia Commission (MCMC), or

intermediary agencies such as telecommunications service providers, each playing a role in regulating, overseeing, or facilitating these digital interactions.

As detailed in MY Patent No. MY-196087-A, it involves an approach for conducting electronic lawsuits over offensive content through telecommunication and networking systems by generating reporting links for third-party platforms, identifying and locating defendants based on their network details, and facilitating plaintiff actions through the platform. In the present system, building upon this foundation, a unique identifier is generated or captured for all registered entities. The term "identifier" may include, but is not limited to, codes or any other unique features associated to the entity such as fingerprints and facial recognition. The current invention emphasizes improving the mechanisms for identifying, authenticating and securely managing various entities operating in the digital realm.

Upon initiating registration, entities are required to submit exhaustive identification details that align with standards specified by various national and international laws and regulations. This information is crucial for the accurate identification and subsequent authentication of the entity. The nature of the required information varies depending on the entity involved — whether an individual, an organization, a program, or an electronic device. For individuals or organizations, essential details are derived from government-issued identifications, including identification cards, passports, business registration certificates, and contact information. In the case of electronic devices, "device-specific identifiers" are necessary; these refer to unique details that distinguish each device, encompassing elements such as the International Mobile Equipment Identity (IMEI) and the Integrated Circuit Card Identifier (ICCID). Further, registering an electronic device also necessitates comprehensive information on the characteristic of the device such as the brand, model, serial numbers and other

pertinent data. For programs, details pertaining to the development team and the entire coding structure are necessary. This meticulous collection of data ensures a multi-layered, foolproof system of authentication that is pivotal in safeguarding digital interactions in the vast online environment. Once entities submit these credentials, the
5 system initiates a robust preliminary verification phase. This stage is crucial to ascertain the authenticity and validity of the information provided, acting as the first line of defence against potential digital misconduct.

Following successful and verified registration, a unique identifier is assigned to each entity, establishing its authenticated digital identity. This identifier serves as a digital
10 fingerprint, distinguishable and irreplicable, ensuring that each entity's interactions within the digital space can be individually recognized and tracked. This identifier, either generated randomly or through a precise algorithm, establishes each online identity as unique and secure, akin to a digital fingerprint. The system's advanced capabilities also enable the capture of various identifiers of the digital entity. These
15 identifiers extend beyond traditional codes, encompassing the unique features to the entity comprising a range of biometric data points such as fingerprints and digital facial recognition patterns. By integrating these sophisticated identification methods, the system broadens its security parameters, offering a more comprehensive, multi-faceted approach to digital identity verification and management. This not only fortifies
20 the trust in the interactions occurring within the digital environment but also significantly diminishes the risk of identity theft or fraudulent activities, enhancing the overall integrity of the digital space

This invention also consists of a registry database that is a comprehensive repository of all registered entities, storing their details and respective unique identifiers. It
25 features real-time updating capabilities, ensuring that any changes in an entity's

information are instantaneously reflected within the system. This database, necessary for ensuring accurate and current information, also maintains comprehensive archives, including complete coding and historical data for digital programs.

Validating an entity's authenticity every time it attempts to seek entry into a digital platform, is crucial. Upon each attempt, the system may necessitate the input of the unique identifier into a platform which is a website, mobile application, web application, or desktop application that may be integrated with the existing patented invention, mandating that entities authenticate themselves. This authentication is not a one-off event; it occurs recurrently, specifically each time the device being used to access the digital platform is powered on, thereby maintaining a consistent security check.

It cross-verifies the presented unique identifiers against the registry database, consulting the entity's historical data and current activity parameters archived in the registry database to confirm identity authenticity. This step is crucial in safeguarding against unauthorized access and ensuring a secure digital environment.

A digital footprint capturer records the comprehensive online activities of entities, creating detailed digital footprints that assist the authority in monitoring and analysis for security purposes. It runs continuously in the background, logging all digital activities associated with each unique identifier. Each time an entity accesses the digital platform, it invariably leaves behind a digital footprint. This footprint encompasses a wealth of information, including specifics such as timestamp of access, identifiable details like names, phone numbers, and email addresses, as well as the device technical data including Internet Protocol (IP) addresses and comprehensive device details as recorded in the registry database. Furthermore, it captures the entity's geographical location at the time of access, the variety of services

they engaged with on the digital platform, and the nature of information exchanged during these interactions. This digital footprint is also systematically archived by the authority. The live digital footprint, a real-time data trail, is combined with the registries maintained by the authority. This integration ensures that a holistic view of the entity's activities is available, enhancing the robustness of cybersecurity measures and enabling a more proactive approach to maintaining digital order and integrity.

The advanced notification module which may be integrated within the platform of the earlier patented invention MY Patent No. MY-196087-A, operates by alerting entities whenever there is an unauthorized access attempt or potential impersonation, especially in cases where a device not registered under the entity is being used. These alerts are dispatched directly to the entity's registered devices via the platform. Such prompt notifications allow the entity to take immediate action, such as reporting the incident through the same platform. When this happens, the system immediately flags it for review, tapping into the archived digital footprints and the detailed registration data to investigate the issue comprehensively, thereby preventing potentially fraudulent activities or other potential cyber threats by other entities. This strategy not only blocks unauthorized access but also empowers the entity to maintain control over their digital identity and resources, significantly enhancing the overarching security protocols.

Moreover, the platform facilitates inquiries concerning the authenticity of any entity involved in digital interactions. These inquiries can be directed to the authority via the platform by entering the unique identifier of that entity in question.

Additionally, the unique identifier of a program can be queried with the authority through the platform, enabling individuals to obtain comprehensive details regarding the ownership and/or developers of the program.

Furthermore, any significant threats or violations concerning data integrity are
5 escalated to the higher authority including national security agencies. These agencies are equipped to conduct thorough audits and investigations, tracing the source of the intrusion attempt. Such robust measures reaffirm the system's commitment to proactive security, creating a digital environment where users can operate with confidence and peace of mind.

10 This feature's strength lies in its dual ability to provide peace of mind through transparency and to harness the collective vigilance of all registered entities. It underscores the system's commitment to a collaborative approach in combating digital fraud, unauthorized access, and other forms of cyber threats and crimes. By ensuring that every entity has the means to verify, question, and report, the system fortifies its
15 protective framework, making the digital space a safer place for all its users.

In conclusion, the present invention revolutionizes digital security protocols by establishing a foolproof mechanism that meticulously verifies entities' identities, thereby safeguarding digital platforms from fraudulent activities and security breaches. The system's comprehensive nature, deriving from a combination of advanced
20 technologies and innovative methodologies, marks a significant advancement in cybersecurity solutions.

CLAIMS

1. A system to register, identify and authenticate entity on digital platform, comprising:
 - a registration and identification module configured to collect, verify, and store
 - 5 identifying information of entities;
 - an identifier generator or capturer configured to create, assign or capture a unique identifier for each registered entity;
 - a registry database configured to maintain comprehensive of registered entities, including their unique identifiers and collected identifying information;
 - 10 an authentication module that cross-references unique identifiers with the corresponding details in the registry database to verify entities' identities during access attempts on digital platform;
 - a digital footprint capturer configured to record online activities of the entity, establishing a behaviour log for each;
 - 15 a notification module that triggers alerts to the recognized entity of the unique identifier in cases of unusual activity suggesting potential cyber threats; and
 - a platform that facilitates requests for entity authentication confirmations, entity information retrievals, and submissions of suspected fraudulent activities or other potential cyber threats by other entities.
 - 20
2. The system according to claim 1, wherein said entity comprises of individuals, organizations, electronic devices, programs, websites, or browsers.
3. The system according to claim 1, wherein the registration and identification
- 25 module conducts a validation process requiring submission of official

identification documents or verifiable personal information of individuals and organizations.

4. The system according to claim 1, wherein the registration and identification
5 module conducts a validation process requiring device-specific identifiers, registered entity associated to the electronic device, and characteristics of electronic devices.
5. The system according to claim 1, wherein the registration and identification
10 module conducts a thorough validation process requiring technical details including registered entity associated to the programs, websites or browsers, and relevant components of their source code.
6. The system according to claim 1, wherein the unique identifier generator
15 assigns a non-replicable unique identifier that is accessible to any other entity for verification purposes.
7. The system according to claim 1, wherein the unique identifier capturer is
20 configured to capture the unique features to that entity comprising biometric data including fingerprints, digital facial recognition patterns, and the like.
8. The system according to claim 1, wherein the digital platform operates over the internet or any other networks.

9. The system according to claim 1, wherein the registry database is maintained with real-time data, incorporating immediate updates regarding any changes in the registered entities' status or details.
- 5 10. The system according to claim 1, wherein the digital footprint capturer further captures any one or combination of IP address, geographical location, device information, and history of services accessed by the entity.
- 10 11. The system according to claim 1, wherein the unique identifier associated with each entity is structured for compatibility with the verification procedures, thereby supporting inter-entity authenticity checks.
- 15 12. The system according to claim 1, wherein the platform comprises a website, a mobile application, web application, desktop application or a combination thereof.
- 20 13. The system according to claim 1, wherein the system operates under the auspices of organizations selected from a range comprising private organizations, government bodies, intermediary agencies, or any combination thereof, wherein said entities are responsible for regulating, authorizing, or supervising activities within the system.
- 25 14. A method for registering, identifying, and authenticating an entity on digital platform, comprising the steps of:
registering and identifying an entity seeking registration, wherein said entity provides its associated details;

generating and capturing a unique identifier specific to the registered entity;
storing the registered entity's detailed information and its unique identifier in a
registry database;
authenticating the entity by cross-referencing the provided unique identifier with
5 the details stored in the registry database;
capturing and logging a digital footprint of the entity during its online interactions
on a digital platform, wherein the digital footprint comprises records of the
entity's online activities; and
facilitating request for confirming entity authentication confirmations, entity
10 information retrievals, and submissions of report related to suspected
fraudulent activities or other potential cyber threats by other entities.

15. The system according to claim 14, wherein said entity comprises of individuals,
organizations, electronic devices, programs, websites, or browsers.

15

16. The method according to claim 14, further comprising the step of registering
electronic devices used by the registered entity that enables access to the
digital platform.

20

17. The method according to claim 14, further comprising the step of registering the
entity associated to the program, websites, or browsers;

18. The method according to claim 14, further comprising the step of registering the
program, websites, or browsers by the associated registered entity.

19. The method according to claim 14, further comprising the step of updating the registry database with any revisions or changes of information related to the entities.
- 5 20. The method according to claim 14, further comprising the step of authenticating the entity upon each attempt to access the digital platform via electronic device.
21. The method according to claim 14, wherein the record of the entity's online activities comprises information corresponding to at least one selected from the group consisting of the entity's IP address, geographical location, device
10 information, and history of services accessed.
22. The method according to claim 14, further comprising the step of notifying registered entities regarding unusual activity suggesting potential cyber threats
15 by a notification module.
23. The method according to claim 14, further comprising the step of confirming entity authentication, retrieving entity information and submitting report related to suspected fraudulent activities or other potential cyber threats through a
20 platform.