INTELLIGENT IDENTITY VERIFICATION AND BACKGROUND CHECKS

INVENTORS:
Frank Bonifacio

TECHNICAL FIELD

1. Implementations relate generally to identity verification procedures. More specifically, implementations relate to methods and systems for providing intelligent identity verification and background checks.

BACKGROUND

2. In today's globalized society, the movement of individuals across national borders has become more prevalent, leading to an increased need for efficient and reliable identity verification and background check systems. Immigration processes, employment verification, and identity authentication are crucial areas that rely heavily on accurate and swift verification methods. However, the existing systems for identity verification are often fragmented, inefficient, and susceptible to errors, creating significant challenges for both individuals and institutions. These challenges are exacerbated by the need to interact with multiple government agencies, each with its own procedures and databases.

3. The current state of the art in identity verification typically involves a combination of biographic data, biometric data, and document verification. However, these methods are often disjointed and lack a unified approach, leading to delays and potential inaccuracies in the verification process. Biometric technologies, such as fingerprinting and facial recognition, while advanced, are not always integrated seamlessly with government databases and other verification systems. This fragmentation results in prolonged processing times and increases the risk of identity fraud, making it difficult for individuals to quickly and securely obtain necessary legal documentation and access to employment opportunities.

4. Additionally, the lack of interoperability between different government and private sector systems poses a significant barrier to efficient identity verification. Many systems are outdated, with limited ability to share and process data across various platforms. This situation is particularly problematic for vulnerable populations, such as asylum seekers and undocumented immigrants, who often face additional scrutiny and bureaucratic hurdles. The inability to efficiently verify their identity and legal status can lead to delays in legal processes, denial of essential services, and challenges in securing employment. Consequently, there is a need in the art for an integrated, intelligent identity verification and background check system that can address these issues.

SUMMARY

5. The appended claims may serve as a summary of this application.

BRIEF DESCRIPTION OF THE DRAWINGS

6. The present disclosure will become better understood from the detailed description and the drawings, wherein:

7. FIG. 1A is a diagram illustrating an exemplary environment in which some embodiments may operate.

8. FIG. 1B is a diagram illustrating an exemplary computer system that may execute instructions to perform some of the methods herein.

9. FIG. 2 is a flow chart illustrating an exemplary method that may be performed in some embodiments.

10. FIG. 3 is a diagram illustrating types of users, participating agencies, and applications related to the intelligent identity verification and background check procedures, in accordance with some embodiments.

11. FIG. 4 is a flow chart illustrating example embodiments of intelligent identity verification and background check procedures.

12. FIG. 5 is a flow chart illustrating example embodiments of intelligent identity verification and background check procedures.

13. FIG. 6 is a diagram illustrating an exemplary computer that may perform processing in some embodiments.

DETAILED DESCRIPTION

14. In this specification, reference is made in detail to specific embodiments of the disclosure.

15. For clarity in explanation, the disclosure has been provided with reference to specific embodiments, however it should be understood that the disclosure is not limited to the described embodiments. On the contrary, the disclosure covers alternatives, modifications, and equivalents as may be included within its scope as defined by any patent claims. The following embodiments of the disclosure are set forth without any loss of generality to, and without imposing limitations on, the disclosure. In the following description, specific details are set forth in order to provide a thorough understanding of the present disclosure. The present disclosure may be practiced without some or all of these specific details. In addition, well known features may not have been described in detail to avoid unnecessarily obscuring the disclosure.

16. In addition, it should be understood that steps of the exemplary methods set forth in this exemplary patent can be performed in different orders than the order presented in this specification. Furthermore, some steps of the exemplary methods may be performed in parallel rather than being performed sequentially. Also, the steps of the exemplary methods may be performed in a network environment in which some steps are performed by different computers in the networked environment.

17. Some embodiments are implemented by a computer system. A computer system may include a processor, a memory, and a non-transitory computer-readable medium. The memory and non-transitory medium may store instructions for performing methods and steps described herein.

18. In one embodiment, the system: receives, from a client device, a request for verification from a user voluntarily submitting to a government background check; obtains personally identifying information (PII) and biometric data from the user via the client device; upon receiving the PII and biometric data from the user, initiates the background check of the user by interfacing with one or more government agencies; processes the PII and biometric data through one or more interconnected databases to verify the user's identity and legal status; generates a clearance status for the user based on the results from the one or more government agencies; upon successful verification, issuing verified identification information for the user associated with at least biometric verification of the user; stores the verified identification information into a database for future retrieval; and provides one or more authorized third parties with the verified identification information and clearance status of the user.

19. Further areas of applicability of the present disclosure will become apparent from the remainder of the detailed description and the claims. The detailed description and specific examples are intended for illustration only and are not intended to limit the scope of the disclosure.

20. FIG. 1A is a diagram illustrating an exemplary environment in which some embodiments may operate. In the exemplary environment 100, a client device 140 is connected to a processing engine 110 and, optionally, a platform 120. The processing engine 110 is connected to the platform 120, and optionally connected to one or more repositories and/or databases, including, e.g., a user repository 130, a government agency repository 132, and/or an identity information repository 134. One or more of the databases may be combined or split into multiple databases. The client device 140 in this environment may be a computer, and the platform 120 and processing engine 110 may be applications or software hosted on a computer or multiple computers which are communicatively coupled via remote server or locally.

21. The exemplary environment 100 is illustrated with only one client device, one processing engine, and one platform, though in practice there may be more or fewer additional client devices, processing engines, and/or platforms. In some embodiments, the client device(s), processing engine, and/or platform may be part of the same computer or device.

22. In an embodiment, the processing engine 110 may perform the exemplary method of FIG. 2 or other method herein and, as a result, provide intelligent identity verification and background checks. In some embodiments, this may be accomplished via communication with the client device, processing engine, platform, and/or other device(s) over a network between the device(s) and an application server or some other network server. In some embodiments, the processing engine 110 is an application, browser extension, or other piece of software hosted on a computer or similar device, or is itself a computer or similar device configured to host an application, browser extension, or other piece of software to perform some of the methods and embodiments herein.

23. The client device 140 is a device with a display configured to present information to a user of the device who is a user of the platform 120. In some embodiments, the client device presents information in the form of a visual UI with multiple selectable UI elements or components. In some embodiments, the client device 140 is configured to send and receive signals and/or information to the processing engine 110 and/or platform 120. In some embodiments, the client device is a computing device capable of hosting and executing one or more applications or other programs capable of sending and/or receiving information. In some embodiments, the client device may be a computer desktop or laptop, mobile phone, virtual assistant, virtual reality or augmented reality device, wearable, or any other suitable device capable of sending and receiving information. In some embodiments, the processing engine 110 and/or platform 120 may be hosted in whole or in part as an application or web service executed on the client device 140. In some embodiments, one or more of the platform 120, processing engine 110, and client device 140 may be the same device. In some embodiments, the client device 140 is associated with a first user account within a platform, and one or more additional client device(s) may be associated with additional user account(s) within the platform.

24. In some embodiments, optional repositories can include a user repository 130, government agency repository 132, and/or identity information repository 134. The optional repositories function to store and/or maintain, respectively, information relating to users within a platform and their corresponding user accounts and/or profiles; information related to participating government agencies and their background check procedures; and identity information relating to the identities and clearance statuses of users. The optional database(s) may also store and/or maintain any other suitable information for the processing engine 110 or platform 120 to perform elements of the methods and systems herein. In some embodiments, the optional database(s) can be queried by one or more components of system 100 (e.g., by the processing engine 110), and specific stored data in the database(s) can be retrieved.

25. Platform 120 is a platform configured to provide intelligent identity verification and background checks for volunteering users in relation to the systems and methods herein. The platform 120 may present a user with one or more user interfaces or interface components which facilitate the submission of user information and data.

26. FIG. 1B is a diagram illustrating an exemplary computer system 140 with software modules that may execute some of the functionality described herein. In some embodiments, the modules illustrated are components of the processing engine 110.

27. Receiving module 152 functions to receive, from a client device, a request for verification from a user voluntarily submitting to a government background check, and obtain personally PII and biometric data from the user via the client device.

28. Background check module 154 functions to, upon receiving the PII and biometric data from the user, initiate the background check of the user by interfacing with one or more government agencies.

29. Verification module 156 functions to process the PII and biometric data through one or more interconnected databases to verify the user’s identity and legal status.

30. Clearance status module 158 functions to generate a clearance status for the user based on the results from the one or more government agencies.

31. Issuance module 160 functions to, upon successful verification, issue verified identification information for the user associated with at least biometric verification of the user.

32. Storage module 162 functions to store the verified identification information into a database for future retrieval.

33. Providing module 164 functions to provide one or more authorized third parties with the verified identification information and clearance status of the user.

34. The above modules and their functions will be described in further detail in relation to an exemplary method below.

35. FIG. 2 is a flow chart illustrating an exemplary method that may be performed in some embodiments.

36. At step 210, the system receives, from a client device, a request for verification from a user voluntarily submitting to a government background check. In various embodiments, the client device may be, e.g., a mobile device such as a smartphone or tablet, a computing device such as a laptop, a device within a kiosk, or a device within a dedicated verification room. The client device acts as the interface between the user and the verification system. For example, a user may initiate a verification request using a smartphone application designed for this purpose. This application can guide the user through the necessary steps to request verification. Alternatively, the user may use a computing device such as a laptop or desktop computer to access a web portal dedicated to the verification process. In another embodiment, the client device could be a device within a kiosk. These kiosks can be strategically located in places such as government buildings, community centers, airports, or even large employers' premises. For instance, a user at an immigration office could use a kiosk to submit their verification request. Additionally, the client device could be a device within a dedicated verification room, which might be found in immigration buildings, refugee centers, or large multinational corporate offices.

37. In various embodiments, the user is associated with a group of individuals representing one or more of: legal immigrants, undocumented immigrants, asylum seekers, and/or persons seeking identity verification for other reasons. Each such group presents unique challenges and requirements, and the systems and methods herein are designed to accommodate these differences through tailored verification processes.

38. Legal immigrants often need to verify their status for employment, travel, and legal purposes. For example, in some embodiments, a legal immigrant applying for a job may use the system to submit a verification request. The system can ensure that they meet the legal requirements for employment, and inform a specific employer or one or more prospective employers of the clearance status through the steps outlined below. This process can help employers quickly verify the legal work eligibility of potential hires, streamlining the onboarding process and reducing the risk of hiring individuals without proper authorization.

39. In some embodiments, undocumented immigrants (i.e., illegal aliens) might seek verification as part of a regularization process or to access essential services. For instance, in some embodiments, a government amnesty program might use the system to help undocumented individuals regularize their status. By submitting their PII and biometric data, these individuals can undergo a background check to determine their eligibility for legal status adjustment. The system interfaces with multiple government agencies to verify the individual's history and ensure they meet the criteria set forth by the amnesty program. This process provides a structured path for undocumented immigrants to gain legal status and access opportunities previously unavailable to them.

40. In some embodiments, asylum seekers represent another group which may be served by the system. These individuals often flee persecution and seek refuge in a new country, requiring thorough background checks to confirm their identities and assess their asylum claims. For example, an asylum seeker arriving at a refugee center can use a dedicated verification room to provide their PII and biometric data. The system processes this information through interconnected databases, including international agencies and local immigration authorities, to verify the individual's identity and check for any potential security concerns. This comprehensive verification process supports the asylum application by providing credible, verified information to decision-makers.

41. In various embodiments, persons seeking identity verification through the system may encompass a broad range of individuals who may need to establish or confirm their identity for various reasons, such as, for example, opening a bank account, enrolling in educational programs, or accessing government services. For instance, a person who has lost their identification documents might use the system to re-establish their identity. By providing PII and biometric data, the system can verify their identity against existing records in multiple databases. Once verified, the system issues new identification information, allowing the individual to regain access to essential services and opportunities.

42. In some embodiments, when a user submits a request for verification, the client device captures and transmits the request to the central verification system. In some embodiments, this transmission involves secure communication protocols to protect the user's information and submitted data. In some embodiments, once the request for verification is received, the system logs the request and assigns a unique identifier to the user's profile. This identifier can be used to track the user’s verification status throughout the entire process.

43. At step 220, the system obtains PII and biometric data from the user via the client device. In the context of the verification system described, PII refers to any data that could potentially be used to identify a specific individual. In various embodiments, PII may include one or more of the following from a user: full legal name, date of birth, address, social security number or equivalent, passport number, driver’s license number, phone number, email address, photographs or other images, employment information, medical records or screening results, and/or educational records. In this context, biometric data can refer to unique physical or behavioral characters of an individual that can be used to identify them. In various embodiments, biometric data may include, for example, fingerprints, facial recognition data, retinal scans, iris scans, voice recognition, DNA information, gait recognition, behavioral biometrics, or any other biometric data.

44. In some embodiments, the client device, whether, e.g., a mobile phone, tablet, laptop, kiosk, or a dedicated verification room device, serves as the primary user interface for data collection. The system prompts the user to enter their PII, such as full name, date of birth, address, social security number, and contact details, ensuring that all essential information is captured efficiently and accurately. In some embodiments, to obtain biometric data, the client device leverages various built-in or connected sensors and/or peripherals. For instance, mobile devices and tablets equipped with fingerprint scanners and facial recognition cameras can capture biometric data directly from the user. In some embodiments, the system guides the user through the process of scanning their fingerprints or taking a facial photo, ensuring that the data collected is of high quality and suitable for verification purposes. Additionally, in some embodiments, the client device may request the user to perform specific actions, such as, e.g., looking into the camera for a retinal scan or speaking a phrase for voice recognition, depending on the available biometric modalities.

45. In some embodiments, in environments where dedicated devices are used, such as kiosks or verification rooms, the system can utilize more advanced biometric capture technologies. Kiosks may include, for example, integrated fingerprint scanners, high-resolution cameras for facial and retinal scans, and document scanners for capturing images of identification documents. Verification rooms in immigration offices or refugee centers may be equipped with specialized devices like iris scanners and DNA sampling kits, providing a controlled environment for comprehensive biometric data collection. In some embodiments, trained personnel may be on hand to assist users with biometric data collection in these settings.

46. In some embodiments, once the PII and biometric data are captured, the client device securely transmits this information to the central verification system. For example, the transmission process may use encryption protocols, such as SSL/TLS, to protect the data from interception or unauthorized access. The system then stores the data in a secure database, where it can be processed and cross-referenced with existing records in government and private sector databases.

47. At step 230, the system, upon receiving the PII and biometric data from the user, initiates the background check of the user by interfacing with one or more government agencies. In some embodiments, the system leverages secure communication channels to connect with databases and systems managed by various government agencies.

48. In some embodiments, the system employs APIs (Application Programming Interfaces) and other integration methods to establish real-time connections with the databases of agencies such as the Department of Defense (DOD), Department of Justice (DOJ), Department of Homeland Security (DHS), Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), and Immigrations and Customs Enforcement (ICE), among others. These connections allow the system to query the databases and retrieve relevant information about the user, such as, e.g., criminal records, immigration status, employment history, and other pertinent data. The system may also interface with state and/or municipal police databases to gather local-level information.

49. In some embodiments, during this process, the system sends encrypted requests containing the user's PII and biometric data to the respective agencies. Each agency processes the request according to its protocols and returns the relevant data to the system. For example, the FBI may provide criminal background information, while DHS could offer data regarding the user's immigration status and any previous interactions with immigration services. The system ensures that all data exchanged during this process is encrypted and handled according to strict data privacy and security standards to prevent unauthorized access or breaches. In some embodiments, once the background check data is retrieved from the various agencies, the system compiles and analyzes the information to generate a comprehensive profile of the user. This profile may include, for example, verified identity details, legal status, and any other relevant information necessary for further processing.

50. In some embodiments, the system facilitates one or more medical screenings or tests required by the one or more government agencies, ensuring that users comply with health-related prerequisites that may be necessary for, e.g., legal status verification, employment, or immigration processes. For example, in the context of immigration, certain countries require immigrants and asylum seekers to undergo medical screenings to check for communicable diseases, vaccination status, and overall health fitness. An immigrant applying for a visa might need to demonstrate they are free from specific diseases such as tuberculosis or hepatitis. The system facilitates these medical screenings by coordinating with authorized healthcare providers and ensuring the results are securely transmitted to the relevant government agencies.

51. In some embodiments, the system can integrate with healthcare databases and electronic health record (EHR) systems to streamline the medical screening process. When a user is required to undergo a medical test, the system generates a referral to a participating medical facility, where the user can complete the necessary screenings. The medical facility then submits the results directly to the system, which securely stores and processes the medical data. For instance, a visa applicant may receive a referral for a chest X-ray to screen for tuberculosis, and the results are automatically uploaded to the system once the screening is complete.

52. In some embodiments, the system ensures that medical screenings are conducted in compliance with privacy regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, or equivalent regulations in other countries. All medical data collected is encrypted and access-controlled, ensuring that only authorized personnel and systems can view or use this information. For example, an asylum seeker undergoing mandatory health checks will have their medical results securely transmitted and stored, accessible only to the immigration authorities handling their case.

53. At step 240, the system processes the PII and biometric data through one or more interconnected databases to verify the user's identity and legal status. In some embodiments, The interconnected databases include both internal and external sources, encompassing, e.g., government databases, private sector records, and specialized verification services. In some embodiments, the system employs advanced algorithms and data matching techniques to cross-reference the user's information across these diverse datasets.

54. In some embodiments, the system first conducts internal verification by comparing the user's PII and biometric data against previously stored records within its own secure database. This initial check helps to identify any inconsistencies or duplicates within the system. For example, the system may compare the user's fingerprints or facial recognition data with existing records to ensure that the user has not previously submitted fraudulent information or attempted multiple verifications under different identities.

55. Following the internal check, the system interfaces with external government databases. In various embodiments, this includes querying immigration records, criminal databases, and other governmental registries. The system uses secure APIs to send encrypted requests to these databases, retrieving detailed information about the user's immigration status, criminal history, and any other relevant data. For example, an interface with the

DHS database might confirm the user’s legal immigration status, while an interface with the FBI database could reveal any criminal records.

56. In some embodiments, in addition to government databases, the system also accesses private sector databases and specialized verification services. This may include, e.g., employment records, educational qualifications, and other identity verification services that provide additional layers of confirmation. In some embodiments, by integrating data from multiple sources, the system can create a comprehensive and reliable profile of the user. In some embodiments, advanced data analytics and machine learning algorithms are employed to detect anomalies and ensure that the collected data accurately represents the user’s identity and legal status.

57. In some embodiments, the system provides real-time status updates to the user via the client device during the background check process, enhancing transparency and user engagement. Real-time status updates can be delivered through various communication methods depending on the client device being used. For example, if the user is using a mobile phone, updates may be provided through push notifications within, e.g., the verification app, SMS messages, or email alerts. These notifications can inform the user of significant milestones in the verification process, such as the receipt of their data, the initiation of checks by different government agencies, and the completion of various verification stages. On a kiosk or dedicated verification room device, status updates might be displayed on the screen during the session or printed on a receipt that the user can take with them. For example, the screen might show a progress bar indicating the current stage of the background check, along with estimated times for each step. This visual feedback helps users understand where they are in the process and what to expect next. In some embodiments, the system can provide detailed status updates through a secure web portal accessible from any internet-enabled device. Users can log into the portal to view a comprehensive timeline of their background check, including which agencies have been contacted, the results received, and any pending actions. In some embodiments, this portal may also offer a secure messaging feature, allowing users to ask questions or seek clarification on specific aspects of their verification process.

58. In some embodiments, the system conducts an immigration certification process, wherein the certification process comprises one or more steps to facilitate legal migration by enabling the user to obtain legal documentation. In some embodiments, the legal documentation may be, for example, a pre-green card document or a green card document. In some embodiments, the immigration certification process begins with a thorough verification of the user’s identity and legal status, leveraging the collected PII and biometric data. Once the user's identity is confirmed and any preliminary background checks are completed, the system initiates the specific steps required to obtain legal migration documentation. For example, a user seeking a pre-green card document will be guided through the process of submitting necessary forms, providing supporting documents such as employment verification or sponsorship letters, and undergoing any additional biometric screenings required by immigration authorities. In some embodiments, the system integrates with immigration databases and government portals to facilitate the submission and tracking of the user's application. This may include real-time data sharing and updates, ensuring that the user's application status is current and any required actions are promptly communicated. For instance, if an immigration authority requires additional information or documentation, the system can immediately notify the user, providing instructions on how to submit the required materials through the integrated platform. In some embodiments, as part of the certification process, the system may also schedule and manage appointments for the user, such as interviews with immigration officials or medical examinations required for the green card application. By coordinating these activities, the system helps ensure that the user completes all necessary steps efficiently and within the required timelines. For example, the system can automatically book an appointment for a biometric interview at a local immigration office and provide the user with detailed instructions on what to bring and expect during the interview.

59. In some embodiments, once all required steps are completed and the user's application is approved, the system facilitates the issuance of the legal documentation. This can include, for example, generating a digital version of the pre-green card or green card document that the user can access through their client device, as well as coordinating the delivery of physical documents. The system ensures that these documents are securely stored and easily retrievable for future use.

60. In some embodiments, the user may be identified as a refugee from one of the countries on a list of designated countries, and the system may thereafter ensure that the background check further includes an additional review of the user through a security advisory opinion process. Such measures are designed to address the heightened security concerns associated with refugees from certain regions or countries. This additional review ensures that the verification process meets stringent security standards and provides a thorough assessment of the individual's background. In some embodiments, when the system identifies a user as a refugee from a designated country, it triggers the security advisory opinion (SAO) process. This process involves a more detailed and rigorous examination of the user’s background, leveraging intelligence and security databases from multiple agencies. The designated countries are typically those identified by government agencies as requiring extra scrutiny due to heightened security risks, such as ongoing conflicts or high levels of terrorist activity. During the SAO process, the system interfaces with specialized databases and security services, including international intelligence agencies, counterterrorism units, and other relevant organizations. For example, the system might query databases maintained by the National Counterterrorism Center (NCTC) or Interpol to gather additional intelligence on the individual. This comprehensive data collection helps to identify any potential security threats posed by the user. In some embodiments, the system also facilitates the coordination and communication between various agencies involved in the SAO process. For instance, the system might compile data from immigration records, criminal databases, and international security reports, presenting a unified report to the authorities responsible for making the final determination. Once the additional review is complete, the system updates the user’s clearance status based on the findings of the SAO process. If no significant security threats are identified, the user can proceed with their application for asylum or other immigration benefits. Conversely, if potential issues are flagged, the system provides detailed reports and recommendations for further action, such as additional interviews or security measures.

61. At step 250, the system generates a clearance status for the user based on the results from the one or more government agencies. In some embodiments, the system synthesizes the data obtained from the various government agencies, along with internal and external database checks, to determine an overall clearance status that will be used for further actions and decision-making.

62. In various embodiments, the clearance status can take several forms, depending on the results of the background checks and data verifications. For example, a "Clear" status indicates that the user’s identity has been verified without any issues, and their legal status is confirmed as compliant with immigration and legal requirements. Conversely, a "Pending" status may be assigned if certain aspects of the user’s background require further investigation or if additional documentation is needed. A "Failed" status indicates significant discrepancies or issues in the user’s background that prevent successful verification, such as, for example, a criminal record or unresolved immigration status.

63. In some embodiments, to generate the clearance status, the system employs a decision-making algorithm that evaluates the collected data against predefined criteria and thresholds. This algorithm considers various factors, including the presence of any criminal records, immigration violations, or inconsistencies in the biometric data. The algorithm is designed to weigh these factors appropriately, ensuring a balanced and fair assessment of the user's profile. In some embodiments, the system also incorporates feedback mechanisms from the government agencies, allowing for real-time updates and adjustments to the clearance status as new information becomes available.

64. In some embodiments, once the clearance status is generated, it is securely logged into the system's database and associated with the user's profile. The system then prepares this information for dissemination to authorized third parties, such as, e.g., employers, legal immigration services, or other relevant entities.

65. In some cases, the clearance status may represent the user failing the background check via one of the government agencies. In some embodiments, when the user fails the background check, the system provides, to the user, a rejection identifier and instructions for issue rectification. This step ensures that users who do not initially pass the background check are informed of the reasons for their failure and are given a potential pathway or opportunity to address and rectify the issues identified.

66. In some embodiments, when a user fails the background check, the system generates a rejection identifier that is unique to the user's case. This identifier helps track the specific reasons for the failure and the associated details, such as which government agency reported the issue and what aspects of the user's background were problematic. For example, the system might indicate that the user has a criminal record reported by the FBI or an unresolved immigration issue flagged by DHS. The rejection identifier serves as a reference for both the user and the authorities involved in the rectification process. In some embodiments, along with the rejection identifier, the system provides detailed instructions for issue rectification. These instructions are tailored to the specific reasons for the rejection and outline the steps the user must take to address the identified issues. For instance, if the rejection is due to a criminal record, the instructions might include steps for obtaining legal documentation to dispute or clarify the record. If the issue is related to immigration status, the instructions might guide the user through the process of resolving outstanding immigration issues, such as providing additional documentation or attending a follow-up interview.

67. In some embodiments, the system also facilitates communication between the user and the relevant government agencies, helping to streamline the rectification process. Users can use the system to submit additional documents, request appointments, and track the status of their rectification efforts. For example, the system might allow a user to upload court documents that expunge a past criminal conviction or provide additional proof of legal residency. By centralizing these interactions within the system, users benefit from a more organized and efficient process for addressing their background check issues. In various embodiments, the system may allow the user to access all relevant documents to present in person to the one of the government agencies that did not clear the user. For example, the system may compile and provide downloadable copies of all submitted documents, rejection notices, and any additional evidence needed to clarify or resolve discrepancies, allowing the user to bring comprehensive and organized information to their appointment.

68. At step 260, the system, upon successful verification, issues verified identification information for the user associated with at least biometric verification of the user. The verified identification information serves as a robust and reliable credential that can be readily authenticated by authorized third parties. In various embodiments, the verified identification information can be issued in multiple formats depending on the context and requirements. In some embodiments, this includes a physical identification card. In some embodiments, this physical identification card features the user's biometric data, such as, e.g., a photograph or fingerprint. This card may also include traditional identification elements such as the user's name, date of birth, and a unique identification number. In some embodiments, the physical identification card may incorporate a Radio Frequency Identification (RFID) chip to facilitate contactless verification and access control. The RFID chip stores encrypted biometric and identification information that can be read by RFID scanners. In some embodiments, a QR code may be included on the identification card. The QR code can be scanned using various devices such as, e.g., smartphones and dedicated QR scanners, to quickly retrieve the user's encrypted biometric information and identification details. This allows for versatile use across different verification platforms and simplifies the process for both users and verifiers. For example, an employer could scan the QR code during the hiring process to instantly access the applicant's verified identity and legal status. In some embodiments, the card's design may incorporate advanced security features to prevent counterfeiting and unauthorized duplication. These features may include, for example, holographic overlays, microtext, or UV printing.

69. In some embodiments, the system may additionally or alternatively issue digital identification credentials. In some embodiments, these digital credentials can be stored in a secure digital wallet on the user's mobile device. In some embodiments, the digital ID can be accessed via a mobile application and can include biometric verification features such as, e.g., facial recognition or fingerprint authentication to unlock and present the ID.

70. In various embodiments, the issuance of verified identification information involves several steps to ensure accuracy and security. In some embodiments, the system generates the ID based on the confirmed data from the verification process, incorporating the user's biometric data to link the ID unequivocally to the individual. This ID is then encrypted and stored securely within the system's database. For physical IDs, the system may coordinate with a secure printing service to produce the cards, which are then distributed to the user. For digital IDs, the system may facilitate secure downloading and installation onto the user's mobile device.

71. In some embodiments, the system conducts a certification process enabling the user to obtain one or more pieces of legal migration documentation. This ensures that users can transition from verified identity status to acquiring the necessary legal documents required for immigration purposes. For example, an individual who has successfully undergone the verification process and has a "Clear" clearance status may be eligible to apply for a pre-green card document or a full green card. The system facilitates this by guiding the user through the application process, ensuring that all necessary information and documentation are collected and submitted to the relevant immigration authorities. This may include, e.g., filling out forms, uploading supporting documents, and scheduling interviews or additional assessments.

72. In some embodiments, the system integrates with immigration agency databases to streamline the submission and tracking of legal migration documentation. Once the user submits their application, the system tracks the progress and provides real-time updates to the user. For instance, a user applying for a green card can monitor their application's status through the system, receiving notifications about any required actions or milestones reached in the process. This transparency helps users stay informed and engaged throughout the certification process.

73. In some additional embodiments, the certification process may involve additional checks or verifications to ensure the user's eligibility for specific documents. For instance, the system might verify the user's employment history, financial status, or family relationships as part of the application for a family-based visa. An applicant for a work visa may need to provide proof of employment and income, for example, which the system can verify through integrated employment databases and financial records.

74. In some embodiments, this certification process also includes generating and issuing the legal migration documentation once the user has met all requirements. This might involve creating digital or physical documents that are officially recognized by immigration authorities. For example, after completing the certification process, the user might receive a digital copy of their visa or a physical green card, which can be used as proof of their legal status. By incorporating the certification process into the overall verification system, users benefit from a streamlined, comprehensive approach to securing legal migration documentation, ensuring they meet all necessary criteria efficiently and effectively.

75. At step 270, the system stores the verified identification information into a database for future retrieval. In some embodiments, the storage process is designed to prioritize data security and integrity, adhering to strict protocols to prevent unauthorized access or data breaches. In some embodiments, the database used for storing verified identification information is highly secure and resilient, employing encryption techniques to protect sensitive data. Each user's information is stored in an encrypted format, ensuring that only authorized personnel and systems can decrypt and access the data. In some additional embodiments, the database implements robust access controls, audit trails, and regular security assessments.

76. In some embodiments, the system also ensures that the stored identification information is easily retrievable for authorized purposes. When a user or an authorized third party requests verification, the system can quickly retrieve the necessary data from the database and provide the relevant information. This capability can be utilized for various scenarios, such as, e.g., re-verification of identity for employment, legal matters, or other services requiring proof of identity.

77. In some embodiments, the system is designed to support updates and modifications to the stored identification information. As users' circumstances change, such as updating their address, renewing their immigration status, or obtaining new biometric data, the system can incorporate these changes into the database. This dynamic updating process ensures that the stored information remains current and accurate, reflecting the most up-to-date status of the user.

78. In some embodiments, the system integrates with one or more existing government or private sector systems to automatically update the clearance status and verified identification information of the user, ensuring that the user's data remains current and accurate over time. For example, consider a scenario where a user’s immigration status changes due to the approval of a green card application. The system, integrated with the relevant immigration authority’s database, can automatically receive updates about the change in status. Once the green card is approved, the immigration authority’s system updates the user’s status, which is then seamlessly reflected in the verification system. The user’s clearance status and verified identification information are immediately updated to reflect this new legal status, ensuring that any subsequent verifications or checks use the most up-to-date information.

79. Another example involves changes in employment status. If a user changes jobs or updates their employment information in a government or corporate database, the system can automatically incorporate these changes. For instance, the user’s new employer might be required to verify their work authorization status. By integrating with employment databases, the system can detect the new employment details and update the user’s profile accordingly, ensuring that their verified identification information reflects their current employment status.

80. In various embodiments, this automatic updating process may also apply to other critical information such as changes in, e.g., legal name, address, or contact details. For example, if a user legally changes their name and updates this information with the relevant government agency, the integrated system will capture this change and update the user’s identification records. This ensures that the user’s identification information is consistently accurate and reduces the need for manual updates, which can be time-consuming and error-prone.

81. At step 280, the system provides one or more authorized third parties with the verified identification information and clearance status of the user. In some embodiments, the system facilitates the secure transmission of verified identification information and clearance status to authorized third parties through encrypted communication channels. Each request for information is carefully validated to ensure that only entities with the appropriate permissions can access the data. This process involves verifying the credentials and authorization levels of the requesting party before granting access to the user’s information. The use of encryption protocols such as SSL/TLS ensures that the data remains confidential and protected from interception during transmission.

82. In some embodiments, authorized third parties can access the verified identification information and clearance status through various means, depending on the integration and technical capabilities of the receiving system. For instance, employers might integrate the system's API into their human resources software to automatically verify the identity and legal status of job applicants. Immigration authorities may access the data through a secure web portal, allowing them to quickly retrieve and review the necessary information for processing applications. Legal institutions and service providers can similarly utilize web interfaces or direct API access to obtain verification data, streamlining their operations and reducing the need for manual checks.

83. In various embodiments, the provision of verified identification information and clearance status also includes mechanisms for auditing and tracking access requests. In some embodiments, each access request is logged with details such as the requesting entity, the information accessed, and the time of access. In some embodiments, users may be notified of access requests, providing them with visibility into who is accessing their information and for what purpose.

84. In some embodiments where the user has been successfully verified and cleared, the system can automatically submit a job application on behalf of the user to one or more employment opportunities within an employment database upon successful clearance of the user, significantly enhancing the user's ability to secure employment swiftly and efficiently. This feature leverages the verified identity and legal status of the user to streamline their entry into the job market. In some embodiments, once the user has been cleared through the verification process, the system automatically generates a job application profile using the verified PII and biometric data. This profile may include essential information such as, e.g., the user's name, contact details, legal status, work authorization, educational background, and any relevant employment history. The system ensures that this information is formatted according to the standards required by various employment databases, facilitating seamless integration. In some embodiments, the system then interfaces with multiple employment databases and job portals to submit the user's application to a range of suitable job opportunities. These databases might include general job search engines, industry-specific employment platforms, and direct employer databases. For instance, the system can target job opportunities in sectors like healthcare, construction, technology, or domestic services, depending on the user's qualifications and preferences. This broad submission increases the chances of the user finding employment quickly.

85. In some embodiments, the system can customize job applications to match the specific requirements and preferences of different employers. For example, if a user has specific skills or certifications relevant to certain job postings, the system can highlight these in the application. In some embodiments, to keep the user informed and engaged, the system provides real-time updates on the status of their job applications. For example, users can receive notifications about application submissions, interview requests, and job offers through the client device.

86. In some embodiments, the system incorporates artificial intelligence (AI) technology to enhance the background check process. For example, by utilizing machine learning (ML) algorithms and natural language processing, the system can efficiently analyze large datasets, identify patterns, and extract meaningful insights from user-provided data and external databases. This AI-driven approach enables the system to detect anomalies and inconsistencies that may not be readily apparent through traditional methods, thereby improving the reliability of identity verification and background checks.

87. In some embodiments, the system applies AI technology to perform predictive analysis. For example, by examining historical data and identifying trends, the AI can assess the likelihood of certain outcomes, such as the potential for a user to have undisclosed information relevant to their background check. This predictive capability allows the system to flag cases for further investigation, providing an additional layer of security and accuracy in the verification process.

88. In some embodiments, the AI technology may also facilitate real-time decision-making during the background check. For example, in some embodiments, as the system processes PII and biometric data, AI algorithms can analyze the information against a set of predefined criteria and thresholds. This continuous analysis ensures that any discrepancies or red flags are immediately identified and addressed. For example, in some embodiments, if the system detects a mismatch between the user’s PII and the data retrieved from a government database, the AI can automatically initiate additional verification steps or notify human operators for further review.

89. In some embodiments, the system employs biometric recognition technologies, including facial recognition, fingerprint analysis, and iris scanning, all enhanced by deep learning algorithms that improve accuracy and reduce false positives. In some embodiments, the

AI continuously refines its recognition models by learning from new data, ensuring that the system stays current with the latest advancements in biometric technology. This ensures accuracy and security in identity verification, particularly when used on devices with integrated biometric hardware, such as, e.g., smartphones and kiosks.

90. In some embodiments, the system is compatible with popular mobile platforms, including, e.g., iOS and Android, enabling users to conduct background checks and identity verification directly from their mobile device. In some embodiments, by leveraging the device's built-in security features, the system can ensure that all transactions are protected against unauthorized access. The use of mobile device-specific APIs allows the system to seamlessly integrate with the device's hardware, ensuring that the user experience is intuitive and secure.

91. FIG. 3 is a diagram illustrating types of users, participating agencies, and applications related to the intelligent identity verification and background check procedures, in accordance with some embodiments. FIG. 3 provides a high-level overview of the various components and interactions involved in the verification system. It outlines the categories of individuals who may use the system, the participating agencies involved in the verification process, and the applications that can benefit from the verification results.

92. The first element, labeled "WHO" (302), specifies the groups of individuals who are the primary users of the verification system. These can include, e.g.: legal aliens, i.e., individuals who are legally residing in a country but are not citizens; undocumented immigrants, individuals who are residing in a country without legal authorization; asylum seekers, individuals who have fled their home country and are seeking protection and legal status in another country; and anyone seeking identification, which includes individuals who need official identification for various purposes, such as those who may have lost their identification documents or require re-verification of their identity.

93. The second element, labeled "PARTICIPATING AGENCIES" (304), lists the government entities that the system interfaces with to conduct thorough background checks and verify the users' information. These agencies may include the Department of Defense (DOD), the Department of Justice (DOJ), the Department of Homeland Security (DHS), the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), state police, and/or municipal or local police. These agencies provide access to critical data and intelligence, ensuring that the verification process is comprehensive and reliable. The system's ability to connect with multiple agencies allows for a thorough cross-referencing of user information, thereby enhancing the accuracy and security of the verification process.

94. [0123] The third element, labeled "APPLICATIONS" (306), enumerates the primary applications of the verification system's results. These applications may include, e.g.: legal immigration, which assists individuals in obtaining legal immigration status such as visas, green cards, or citizenship; dating sites, which provide secure verification for users of online dating platforms, ensuring the authenticity of user profiles and enhancing safety; and labor/employment, which facilitates the employment process by verifying the legal status and identity of job applicants, thereby aiding employers in making informed hiring decisions.

95. FIG. 4 is a flow chart illustrating example embodiments of intelligent identity verification and background check procedures. The flow chart illustrates the process of user verification within the system. It delineates the sequence of actions taken from the initial user interaction to the final dissemination of results to authorized third parties.

96. The first element, labeled "User" (402), represents individuals such as, e.g., undocumented immigrants, asylum seekers, or any person seeking identification. These users initiate the verification process by submitting a request through the system. This step marks the beginning of the verification process, where the user's need for identification or legal status verification prompts them to engage with the system. The second element, labeled "Environment / device" (404), specifies the different environments or devices that users can utilize to interact with the system. These may include, e.g., rooms, smartphones, and kiosks. Each of these environments provides the necessary tools and interfaces for users to submit their personally identifying information (PII) and biometric data. For example, a user in a dedicated verification room might use advanced biometric scanners, while a user with a smartphone might use the device's camera and fingerprint sensor.

97. The third element, labeled "Biographic and identity investigations" (406), encompasses the core verification activities conducted by the system. This may include, for example, FBI biometric checks of fingerprints, photographs, retinal scans, and facial recognition, as well as medical screenings. Additionally, the system may perform checks with US domestic and international intelligence agencies, such as the National Counterterrorism Center and the FBI, to ensure comprehensive background verification. Refugees from designated countries may undergo an additional review through the Security Advisory Opinion process to address heightened security concerns.

98. The fourth element, labeled "Results sent to authorized third parties" (408), describes the final step where the verified results are communicated to relevant entities. These entities may include, for example, the Department of Defense (DOD), Department of Homeland Security (DHS), Department of Justice (DOJ), dating sites, and prospective employers. By providing verified information to these third parties, the system facilitates informed decision-making, whether it be for legal immigration processes, enhancing safety on dating platforms, or aiding employers in hiring decisions. This comprehensive flow ensures that the verification process is thorough, secure, and beneficial to both users and third parties requiring validated information.

99. FIG. 5 is a flow chart illustrating example embodiments of intelligent identity verification and background check procedures. A detailed flowchart is presented which outlines one example process of user verification and subsequent actions within the system. It provides a step-by-step representation from the user's arrival at a physical location to the final stages where verified identification is utilized in various employment sectors.

100. The process begins with the user seeking verification arriving at a physical location, as indicated by step 502. This could be a kiosk, a dedicated room in a police station, or an immigration building. The physical location is equipped with the necessary infrastructure to support the verification process. At step 504, the user interacts with a client device available at the physical location. This client device is equipped with modern biometric indicators and applications that facilitate the collection of the user's personally identifying information (PII) and biometric data. The device could be a specialized kiosk terminal, a mobile application, or any other interface that allows for secure and efficient data entry and biometric capture.

101. Following the data collection, step 506 involves background checks being conducted by interfacing with one or more government agencies. The system securely transmits the user's PII and biometric data to various agencies such as the Department of Defense (DOD), Department of Justice (DOJ), and the Department of Homeland Security (DHS). These agencies perform thorough checks, including criminal background verification, immigration status checks, and any other relevant investigations. This multi-agency interaction ensures a comprehensive review of the user's background, enhancing the reliability of the verification process.

102. At step 508, the system determines whether the user has successfully cleared the verification process. Successful clearance involves obtaining verification from all relevant agencies, confirming that the user's identity and legal status are validated without any discrepancies. If the user passes these checks, they proceed to the certification process outlined in element 510. This process involves steps to facilitate legal migration, such as applying for a pre-green card or green card. The certification process is tailored to ensure that all necessary legal documentation is obtained, allowing the user to potentially gain or regularize their legal status in the country.

103. Once the certification process is completed, the system issues a physical identification card, as depicted in element 512. This card includes advanced features such as RFID chips and facial recognition technology, making it a robust and secure form of identification. The issued card is then entered into a secure database for future retrieval and verification purposes. This step ensures that the user has a tangible, official document that can be used to prove their identity and legal status.

104. [0136] With the physical identification card issued and entered into the database, the user can now clear employment identification checks in various sectors, as shown in element 514. This includes sectors such as medical employment, labor, craftsman roles, and caregiving. The verified identification card enables employers in these sectors to confirm the user's identity and legal status quickly and securely. Employers can verify the issued user ID via biometric scanning, as illustrated in element 516, ensuring that the hiring process is both efficient and compliant with legal requirements. This comprehensive flowchart of one example process demonstrates the integrated approach of the verification system, from initial user interaction to practical applications in employment and legal migration.

105. FIG. 6 is a diagram illustrating an exemplary computer that may perform processing in some embodiments. Exemplary computer 600 may perform operations consistent with some embodiments. The architecture of computer 600 is exemplary. Computers can be implemented in a variety of other ways. A wide variety of computers can be used in accordance with the embodiments herein.

106. Processor 601 may perform computing functions such as running computer programs. The volatile memory 602 may provide temporary storage of data for the processor 601. RAM is one kind of volatile memory. Volatile memory typically requires power to maintain its stored information. Storage 603 provides computer storage for data, instructions, and/or arbitrary information. Non-volatile memory, which can preserve data even when not powered and including disks and flash memory, is an example of storage. Storage 603 may be organized as a file system, database, or in other ways. Data, instructions, and information may be loaded from storage 603 into volatile memory 602 for processing by the processor 601.

107. The computer 600 may include peripherals 605. Peripherals 605 may include input peripherals such as a keyboard, mouse, trackball, video camera, microphone, and other input devices. Peripherals 605 may also include output devices such as a display. Peripherals 605 may include removable media devices such as CD-R and DVD-R recorders / players. Communications device 606 may connect the computer 100 to an external medium. For example, communications device 606 may take the form of a network adapter that provides communications to a network. A computer 600 may also include a variety of other devices 604. The various components of the computer 600 may be connected by a connection medium such as a bus, crossbar, or network.

108. Some portions of the preceding detailed descriptions have been presented in terms of algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations are the ways used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of operations leading to a desired result. The operations are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, combined, compared, and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

109. It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the above discussion, it is appreciated that throughout the description, discussions utilizing terms such as "identifying" or “determining” or "executing" or “performing” or “collecting” or “creating” or “sending” or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage devices.

110. The present disclosure also relates to an apparatus for performing the operations herein. This apparatus may be specially constructed for the intended purposes, or it may comprise a general purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program may be stored in a computer readable storage medium, such as, but not limited to, any type of disk including floppy disks, optical disks, CD-ROMs, and magnetic-optical disks, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, magnetic or optical cards, or any type of media suitable for storing electronic instructions, each coupled to a computer system bus.

111. Various general purpose systems may be used with programs in accordance with the teachings herein, or it may prove convenient to construct a more specialized apparatus to perform the method. The structure for a variety of these systems will appear as set forth in the description above. In addition, the present disclosure is not described with reference to any particular programming language. It will be appreciated that a variety of programming languages may be used to implement the teachings of the disclosure as described herein.

112. The present disclosure may be provided as a computer program product, or software, that may include a machine-readable medium having stored thereon instructions, which may be used to program a computer system (or other electronic devices) to perform a process according to the present disclosure. A machine-readable medium includes any mechanism for storing information in a form readable by a machine (e.g., a computer). For example, a machine-readable (e.g., computer-readable) medium includes a machine (e.g., a computer) readable storage medium such as a read only memory ("ROM"), random access memory ("RAM"), magnetic disk storage media, optical storage media, flash memory devices, etc.

113. In the foregoing disclosure, implementations of the disclosure have been described with reference to specific example implementations thereof. It will be evident that various modifications may be made thereto without departing from the broader spirit and scope of implementations of the disclosure as set forth in the following claims. The disclosure is, accordingly, to be regarded in an illustrative sense rather than a restrictive sense.

CLAIMS

WHAT IS CLAIMED IS:

1. A method comprising:

receiving, from a client device, a request for verification from a user voluntarily submitting to a government background check;

obtaining personally identifying information (PII) and biometric data from the user via the client device;

upon receiving the PII and biometric data from the user, initiating the background check of the user by interfacing with one or more government agencies;

processing the PII and biometric data through one or more interconnected databases to verify the user's identity and legal status;

generating a clearance status for the user based on the results from the one or more government agencies;

upon successful verification, issuing verified identification information for the user associated with at least biometric verification of the user;

storing the verified identification information into a database for future retrieval; and

providing one or more authorized third parties with the verified identification information and clearance status of the user.

2. The method of claim 1, wherein the one or more government agencies comprise one or more of: the Department of Defense (DOD), Department of Justice (DOJ), Department of Homeland Security (DHS), Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), Immigrations and Customs Enforcement (ICE), state police, and municipal police.

3. The method of claim 1, wherein the user is associated with a group of individuals comprising one or more of: legal immigrants, undocumented immigrants, asylum seekers, and persons seeking identity verification.

4. The method of claim 1, wherein the client device comprises one or more of: a mobile device, a kiosk device, or a device within a dedicated verification room.

5. The method of claim 1, further comprising:

facilitating one or more medical screenings or tests required by the one or more government agencies.

6. The method of claim 1, wherein the biometric data obtained from the user comprises at least one of: fingerprints, facial recognition data, and retinal scans.

7. The method of claim 1, further comprising:

conducting a certification process enabling the user to obtain one or more pieces of legal migration documentation.

8. The method of claim 1, wherein the clearance status represents the user failing the background check via one of the government agencies, and further comprising:

providing, to the user, a rejection identifier and instructions for issue rectification.

9. The method of claim 8, further comprising:

allowing the user to access all relevant documents to present in person to the one of the government agencies that did not clear the user.

10. The method of claim 1, wherein the PII and biometric data are obtained from the user via a user interface presented to the user at the client device.

11. The method of claim 1, wherein the one or more authorized third parties are associated with one or more of: legal immigration services, dating sites, and employment verification systems.

12. A system comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors, cause the system to perform operations comprising:

receiving, from a client device, a request for verification from a user voluntarily submitting to a government background check;

obtaining personally identifying information (PII) and biometric data from the user via the client device;

upon receiving the PII and biometric data from the user, initiating the background check of the user by interfacing with one or more government agencies;

processing the PII and biometric data through one or more interconnected databases to verify the user's identity and legal status;

generating a clearance status for the user based on the results from the one or more government agencies;

upon successful verification, issuing verified identification information for the user associated with at least biometric verification of the user;

storing the verified identification information into a database for future retrieval; and

providing one or more authorized third parties with the verified identification information and clearance status of the user.

13. The system of claim 12, wherein issuing the verified identification information for the user comprises issuing a physical identification card.

14. The system of claim 13, wherein the physical identification card includes a machine-readable component to facilitate real-time verification by authorized third parties.

15. The system of claim 12, wherein the instructions further cause the system to perform an operation comprising:

providing real-time status updates to the user via the client device during the background check process.

16. The system of claim 12, wherein the instructions further cause the system to perform an operation comprising:

integrating with one or more existing government or private sector systems to automatically update the clearance status and verified identification information of the user.

17. The system of claim 12, wherein the instructions further cause the system to perform an operation comprising:

conducting an immigration certification process, wherein the certification process comprises one or more steps to facilitate legal migration by enabling the user to obtain legal documentation, the legal documentation comprising one or more of: a pre-green card document or a green card document.

18. The system of claim 12, wherein the user is identified as a refugee from one of the countries on a list of designated countries, and wherein the background check further comprises an additional review of the user through a security advisory opinion process.

19. The system of claim 12, wherein the user has been successfully verified and cleared, and wherein the instructions further cause the system to perform an operation comprising:

automatically submitting a job application on behalf of the user to a plurality of employment opportunities within an employment database upon successful clearance of the user.

20. A non-transitory computer-readable medium containing instructions comprising:

receiving, from a client device, a request for verification from a user voluntarily submitting to a government background check;

obtaining personally identifying information (PII) and biometric data from the user via the client device;

upon receiving the PII and biometric data from the user, initiating the background check of the user by interfacing with one or more government agencies;

processing the PII and biometric data through one or more interconnected databases to verify the user's identity and legal status;

generating a clearance status for the user based on the results from the one or more government agencies;

upon successful verification, issuing verified identification information for the user associated with at least biometric verification of the user;

storing the verified identification information into a database for future retrieval; and

providing one or more authorized third parties with the verified identification information and clearance status of the user.

ABSTRACT

Systems and methods provide intelligent identity verification and background checks for a user. In one embodiment, the system: receives a verification request from a user via a client device; obtains personally identifying information and biometric data; initiates a background check by interfacing with government agencies; processes the information and biometric data through interconnected databases to verify the user’s identity and legal status; generates a clearance status based on the results; issues verified identification information upon successful verification; stores the information in a database for future retrieval; and provides authorized third parties with the verified identification and clearance status.