

SYSTEM AND METHOD FOR PROCESSING A LOAN APPLICATION

FIELD OF INVENTION

[001] The present disclosure relates to systems and methods for processing a loan application.

BACKGROUND

[002] Financial institutions, such as banks, provide various types of loans to individuals and business entities. In particular, micro loans are small monetary loans provided to individuals and small business entities. For small businesses, such loans are designed to help them gain access to funding and can be used for the purchase of equipment or meet working capital requirements. For individuals, micro loans may financially enable people who typically lack collateral, steady employment and a verifiable credit history, and thus do not fall under the requirements in normal banking regulations.

[003] Typically, financial institutions that provide such micro loans are small. Two important issues faced by such institutions are operational costs and risk assessment and minimization. Controlling operational costs is important for small financial institutions as their scale of operations is small and they wish to realize profits. In particular, the operational costs of such institutions need to be minimized as the size of loans are small and they may incur losses when operational costs exceed interest earnings. Risk assessment is an important consideration because such institutions need to ensure the ability of loan repayment from individuals who do not have steady employment and a verifiable credit history.

[004] A need therefore exists to provide a method and system for processing a loan that seeks to address at least some of the above problems.

SUMMARY

[005] According to a first aspect of the present invention, there is provided a system for processing a loan application comprising: a processor; and a memory unit communicatively coupled to the processor, wherein the memory unit is configured to receive a loan request from an applicant and evaluation data specific to the applicant for providing an assessment of the loan request; and wherein the processor is configured to: analyse the evaluation data to determine a plurality of evaluation scores specific to the applicant; and determine an outcome of the loan request based on the evaluation scores, wherein the evaluation scores comprise a risk score determined based on the applicant's credit risk and behaviour risk, wherein the processor may be further configured to determine the behaviour risk based on behaviour data associated with the applicant in connection with the loan request and video data submitted by the applicant as evaluation data.

[006]

[007] In an embodiment, the processor may be further configured to update the behaviour risk based on a determination whether the applicant is a returning customer.

[008] In an embodiment, the processor may be further configured to update the behaviour risk based on at least one of an email analysis, a search analysis and a demographic data analysis.

[009] In an embodiment, the search analysis may comprise a search of an identity of the applicant and a search of a lifestyle of the applicant.

[0010] In an embodiment, the processor may be further configured to analyse the demographic data based on at least one of a verification of the applicant's data provided by a third-party and an assessment based on the applicant's past history.

[0011] In an embodiment, the processor may be further configured to determine the credit risk based on at least the applicant's credit data, and wherein the processor may be further configured to update the credit risk based on the determination whether the applicant is a returning customer.

[0012] In an embodiment, the processor may be further configured to perform a data deduplication following the determination whether the applicant is a returning customer.

[0013] In an embodiment, the evaluation scores may further comprise a document verification score and a facial recognition score.

[0014] In an embodiment, the processor may be further configured to determine the document verification score based on one or more documents provided by the applicant as evaluation data, and check whether the one or more documents have been tampered with.

[0015] In an embodiment, the processor may be further configured to determine the facial recognition score based on a comparison of a first facial image detected from one or more documents provided by the applicant as evaluation data and a second facial image extracted from video data submitted by the applicant as evaluation data.

[0016] In an embodiment, the processor may be further configured to determine an outcome of the loan request based on a weighted model combining the risk score, document verification score and facial recognition score.

[0017] According to a second aspect of the present invention, there is provided an automated method for processing a loan application, the method comprising: receiving, via a user device, a loan request from an applicant; obtaining evaluation data specific to the applicant for providing an assessment of the loan request; analysing the evaluation data to determine a plurality of evaluation scores specific to the applicant; determining an outcome of the loan request based on the evaluation scores, wherein the evaluation scores comprise a risk score determined based on the applicant's credit risk and behaviour risk, and wherein the behaviour risk may be determined based on behaviour data exhibited by the applicant in connection with the loan request and video data submitted by the applicant as evaluation data..

[0018]

[0019] In an embodiment, the behaviour risk may be updated based on a determination whether the applicant is a returning customer.

[0020] In an embodiment, the method may further comprise updating the behaviour risk based on at least one of an email analysis, a search analysis and a demographic data analysis.

[0021] In an embodiment, the demographic data analysis may comprise at least one of a verification of the applicant's data provided by a third-party and an assessment based on the applicant's past history.

[0022] In an embodiment, the credit risk may be determined based on at least the applicant's credit data, and wherein the credit risk is updated based on the determination whether the applicant is a returning customer.

[0023] In an embodiment, the method may further comprise a data deduplication step following the determination whether the applicant is a returning customer.

[0024] In an embodiment, the document verification score may be determined based on one or more documents provided by the applicant as evaluation data, and wherein analysing the evaluation data comprises checking whether the one or more documents have been tampered with.

[0025] In an embodiment, the facial recognition score may be determined based on a comparison of a first facial image detected from one or more documents provided by the applicant as evaluation data and a second facial image extracted from video data submitted by the applicant as evaluation data.

[0026] In an embodiment, determining an outcome of the loan request may comprise combining the risk score, document verification score and facial recognition score based on a weighted model.

BRIEF DESCRIPTION OF THE DRAWINGS

[0027] The accompanying Figures, where like reference numerals refer to identical or functionally similar elements throughout the separate views and which together with the detailed description below are incorporated in and form part of the specification, serve to illustrate various embodiments and to explain various principles and advantages in accordance with a present embodiment, by way of non-limiting example only.

[0028] Embodiments of the invention are described hereinafter with reference to the following drawings, in which:

[0029] Figure 1 shows a flow chart illustrating an automated method for processing a loan application, according to an example embodiment.

[0030] Figure 2 shows a schematic diagram illustrating the flow of information in a system for processing a loan application, according to an example embodiment.

[0031] Figure 3 shows a schematic diagram of a computer device / system suitable for realizing a facilitator module, according to an example embodiment.

[0032] Figure 4 shows a detailed flow chart illustrating an implementation of the method according to the example embodiments.

DETAILED DESCRIPTION

[0033] Some portions of the description which follows are explicitly or implicitly presented in terms of algorithms and functional or symbolic representations of operations on data within a computer memory. These algorithmic descriptions and functional or symbolic representations are the means used by those skilled in the data processing arts to convey most effectively 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 steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities, such as electrical, magnetic or optical signals capable of being stored, transferred, combined, compared, and otherwise manipulated.

[0034] Unless specifically stated otherwise, and as apparent from the following, it will be appreciated that throughout the present specification, discussions utilizing terms such as “scanning”, “calculating”, “determining”, “replacing”, “generating”, “initializing”, “outputting”, “identifying”, “authorizing”, “verifying” or the like, refer to the action and processes of a computer system, or similar electronic device, that manipulates and transforms data represented as physical quantities within the computer system into other data similarly represented as physical quantities within the computer system or other information storage, transmission or display devices.

[0035] The present specification also discloses apparatus for performing the operations of the methods. Such apparatus may be specially constructed for the required purposes, or may comprise a computer or other device selectively activated or reconfigured by a computer program stored in the computer. The algorithms and

displays presented herein are not inherently related to any particular computer or other apparatus. Various machines may be used with programs in accordance with the teachings herein. Alternatively, the construction of more specialized apparatus to perform the required method steps may be appropriate. The structure of a computer will appear from the description below.

[0036] In addition, the present specification also implicitly discloses a computer program, in that it would be apparent to the person skilled in the art that the individual steps of the method described herein may be put into effect by computer code. The computer program is not intended to be limited to any particular programming language and implementation thereof. It will be appreciated that a variety of programming languages and coding thereof may be used to implement the teachings of the disclosure contained herein. Moreover, the computer program is not intended to be limited to any particular control flow. There are many other variants of the computer program, which can use different control flows without departing from the spirit or scope of the disclosure.

[0037] Furthermore, one or more of the steps of the computer program may be performed in parallel rather than sequentially. Such a computer program may be stored on any computer readable medium. The computer readable medium may include storage devices such as magnetic or optical disks, memory chips, or other storage devices suitable for interfacing with a computer. The computer readable medium may also include a hard-wired medium such as exemplified in the Internet system, or wireless medium such as exemplified in the GSM mobile telephone system. The computer program when loaded and executed on such a computer effectively results in an apparatus that implements the steps of the preferred method.

[0038] Figure 1 shows a flow chart 100 illustrating a method for processing a loan application according to an example embodiment. At step 102, a loan request from an applicant is received via a user device. At step 104, evaluation data specific to the applicant for providing an assessment of the loan request is obtained. At step 106, the evaluation data is analysed to determine a plurality of evaluation scores specific to the applicant. At step 108, an outcome of the loan request is determined based on the evaluation scores, wherein the evaluation scores comprise a risk score determined based on the applicant's credit risk and behaviour risk.

[0039] Figure 2 shows a schematic diagram illustrating the flow of information in a system 200 for processing a loan application, according to an example embodiment. The system 200 comprises a facilitator module 202, a user device 204, a risk analysis module 206, a facial recognition module 208, a verification module 210 and a decision module 212. The facilitator module 202 is in communication with the user device 204, the risk analysis module 206, the facial recognition module 208 and the verification module 210. The decision module 212 is in communication with the risk analysis module 206, the facial recognition module 208 and the verification module 210. The facilitator module 202, the risk analysis module 206, the facial recognition module 208, the verification module 210 and the decision module 212 may comprise a processor; and a memory unit communicatively coupled to the processor, wherein the memory unit is configured to receive a loan request from an applicant and evaluation data specific to the applicant for providing an assessment of the loan request; and wherein the processor is configured to: analyse the evaluation data to determine a plurality of evaluation scores specific to the applicant; and determine an outcome of the loan request based on the evaluation scores, and wherein the evaluation scores comprise a risk score determined based on the applicant's credit risk and behaviour risk.

[0040] At step A in Figure 2, the facilitator module 202 receives a loan request from an applicant via a user device 204. The applicant may be an individual or a small business entity seeking a loan to finance certain purchases or to meet capital requirements. In the Figure, the loan request may be submitted via an application of the financial institution installed in the user device 204, such as a mobile phone. In an alternate embodiment, the applicant may visit the financial institution's website and submits his loan request via the website.

[0041] At step B, facilitator module 202 obtains evaluation data specific to the applicant for providing an assessment of the loan request. The evaluation data may be provided by the applicant via the user device 204 or uploaded via the financial institution's website. The evaluation data may include at least one of but not limited to: personal data, mobile data, credit data, demographic data, behaviour data and/or video data corresponding to an applicant of the loan request. The video data corresponding to the applicant may include a video selfie of the applicant while the mobile data may include at least one of the following obtained from the user device 204 of the applicant: a plurality of contacts, a plurality of messages, a plurality of call records, an operating system data of the mobile device, a plurality of emails of the applicant and/or a model

of the user device 204. It can be appreciated that the user device 204 may be realised as a mobile phone, a tablet and/or a laptop.

[0042] Credit data may include financial details of the applicant, such as but not limited to at least one of: a monthly income and/or tax contribution of the applicant. Demographic data may include at least one of: age, address, race, gender, employment status, date of birth and/or marital status of the applicant. Personal data may include one or more documents provided by the applicant and may include at least one of: a copy of a passport of the applicant, a copy of the identity card of the applicant, a copy of the driving licence of the applicant and/or a personal account card of the applicant.

[0043] For example, applicant XYZ browses through bank ABC's website using an application on his mobile phone and wishes to obtain a flexible repayment loan scheme. XYZ proceeds to request the flexible repayment loan from bank ABC via the application. XYZ then proceeds to submit a copy of his passport, his personal account number and his latest income statement via the application. XYZ also submits that he is male, 32 years old, Chinese and married with two children via the application. The facilitator module 202, which is in communication with the application, receives the loan request together with copies of his passport, his personal account number and his latest income statement. The facilitator module 202 also receives information that XYZ is male, 32 years old, Chinese and married with two children. The application simultaneously obtains XYZ's contacts, messages, call records, operating system data and the model of his mobile device and transmits the information to the facilitator module 202.

[0044] Subsequently, XYZ takes a video selfie of himself for one minute which includes an audio recording for requesting the loan and stating reasons for the loan request. The video selfie is uploaded via the application and transmitted to the facilitator module 202 for analysis at a later stage.

[0045] At the same time, behavioral data may also be collected by the facilitator module 202 when XYZ enters his personal data in the application. Examples of behavioral data may occur when XYZ enters his age and his marital status and decides to switch suddenly to take a video selfie instead; or XYZ enters information that he was employed for the past six months but deletes and proceeds to change to three months. The facilitator module 202 captures such a behavior of the applicant for analysis at a later stage.

[0046] At step C, the facilitator module 202 transmits the evaluation data to the verification module 210 to verify that the data is genuine. The verification module 210 may determine whether the one or more documents have been tampered by using a set of image processing techniques and machine learning models to detect any kind of image tampering which is not detectable by naked eye. Examples of image tampering can be altering addresses on identify cards or changing the photo to an imposter who is not the applicant. If the one or more documents are found to be tampered, the verification module 210 may prompt the financial institution to manually inspect the documents.

[0047] The verification module 210 may also determine whether the one or more documents are genuine using optical character recognition (OCR) technology. More specifically, OCR technology-based solutions are used to extract specific information from the one or more documents and cross checks with other data (e.g. demographic data) submitted by the applicant. Alternatively or in addition, the verification module 210 may detect a first facial image of the applicant from the one or more documents he has provided as evaluation data . The verification module 210 thus may use the first facial image to compare and verify with the applicant's video selfie to determine that the one or more documents are genuine. Alternatively, the verification module 210 may extract the applicant's name and address from the one or more documents and verifies with the name and address provided by the applicant during submission of the loan request to determine that the one or more documents are genuine.

[0048] If the verification module 210 determines that the one or more documents are genuine and not been tampered with, the verification module 210 determines a document verification score and transmits to the decision module 212 at step D. The document verification score is determined based on the one or more documents provided by the applicant as evaluation data, and includes checking whether the one or more documents have been tampered with. The documents verification score may be based on a predetermined threshold for tampering the one or more documents.

[0049] Continuing from the above example, the verification module 210 receives the documents including but not limited to the copy of XYZ's identity card, his tax number and his latest bank statement. The verification module 210 proceeds to check if the documents have been tampered and cross check XYZ's details from the copy of his identity card, his tax number and his latest bank statement with the

demographic data he has provided, i.e. male, 32 years old, Chinese, married with two children and employed for the past six months. If the verification module 210 determines that the details are accurate and not tampered, the document verification score may be a five (out of a total of five).

[0050] At step E, the facilitator module 202 transmits video data of the applicant to the facial recognition module 208 to verify a second facial image of the applicant using a facial recognition algorithm. In an example, the facial recognition module 208 may extract the applicant's face from different frames and may build a face recognition model to cross check the face on the identity card uploaded by the applicant. A facial recognition score is determined based on a comparison of the first facial image detected from the one or more documents provided by the applicant as evaluation data and the second facial image extracted from video data submitted by the applicant as evaluation data. In this way, the facial recognition module 208 may prevent an applicant from using documents of another person. Subsequently, the facial recognition module 208 determines the facial recognition score and transmits the score to the decision module 212 at step F.

[0051] The facial recognition module 208 may also analyze an emotional behavior of the applicant based on the video data submitted by the applicant. The facial recognition module 208 may carry out video and audio analysis to identify the different facial expressions and emotions resonated in the voice of the applicant. These emotions and expressions are mapped to the behaviour risk associated with the applicant and may partially determine a risk score of the applicant. In other words, the behaviour risk may be determined based on behaviour data exhibited by the applicant in connection with the loan request and video data submitted by the applicant as evaluation data.

[0052] At step G, the risk analysis module 206 receives the evaluation data for analysis and determines a risk score. The risk score may be determined based on the applicant's credit risk and behaviour risk. The risk analysis module 206 may contain several other models to analyse the evaluation data simultaneously. The risk analysis module 206 may update the behaviour risk based on a determination whether the applicant is a returning customer. Alternatively or in addition, the risk analysis module 206 may update the behaviour risk based on an email analysis, a search analysis and a demographic data analysis. Credit risk may be determined based on at least the applicant's credit data and credit risk may be updated based on the determination

whether the applicant is a returning customer. The returning customer may refer to an applicant who had successfully applied and approved a previous loan which he has already repaid to the financial institution. Credit risk may also be based on the applicant's payment behaviour. For example, the credit risk of applicant XYZ may be updated based on his delay in payment of any existing loans and whether an Enterprise Management Incentive option is available for him even though he had taken a pay day loan.

[0053] The risk analysis module 206 may include an auto survey model including machine learning models to assess the applicant's behaviour risk and credit risk by assessing a possibility that the applicant is genuine in providing his information based on his past history. The risk analysis module 206 may also perform demographic data analysis by verifying the applicant's data with data provided by a third party. In this case, data provided by the third party (such as a network operator) may be used to assess the validity of the information. For example, the risk analysis module 206 checks the address provided by the customer against the address provided by the network operator of the applicant's mobile connection. Other types of third party data may be possible, such as obtaining the applicant's information from a third party (e.g. home cable service provider) where the applicant had provided information for other services and that the third party service providers had verified the applicant's data previously.

[0054] Data deduplication (dedup) is an important step in a loan application process. A fraudulent applicant may request a loan repeatedly until the loan request is approved. For example, an applicant may not be allowed to apply for any loan within a predetermined period using his mobile phone and email address after being rejected for a loan. The fraudulent applicant may thus use a different mobile phone number and a different email address in order to obtain approval of a loan. Therefore, it may be necessary to verify the applicant is not a fraudulent applicant before continuing with further verification or analysis. For example, the risk analysis module 206 may include a dedup model which can perform a data deduplication step after determining whether the applicant is a returning customer. The data deduplication step may include determining a relevance in the identity, mobile phone number and address using the applicant's demographic data. If the risk analysis module 206 determines the applicant is fraudulent, e.g. the applicant had previously applied for the same loan and had been rejected five times, the risk analysis module 206 determines that the applicant does not proceed with the loan process and blocks him. The risk analysis module 206 may also

request that the financial institution perform a manual assessment of the applicant's eligibility for the loan. On the other hand, if the applicant is not fraudulent, the risk analysis module 206 allows the applicant to proceed with the loan application by updating the applicant's credit risk and behaviour risk. It can be appreciated that existing applicants whose loans have been approved are excluded from this (dedup) process.

[0055] The risk analysis module 206 may include a credit analysis model to perform credit analysis of the applicant. The credit analysis model may include machine learning algorithms and rule engines. Credit analysis may be performed when the applicant provides his financial and credit information during the loan application process. The risk analysis module 206 extracts information from the credit bureau if information is available for the applicant. The credit analysis model may determine the credit risk of the applicant in this aspect which may partially determine a risk score of the applicant.

[0056] The risk analysis module 206 may include an email analysis model to perform email analysis to determine if there is email fraud. In email fraud, emails are created quickly by the fraudster. These emails are not aged and will adopt the patterns as suggested by email servers. They may also include random numbers. The email analysis model may map email patterns to the observed risk in an existing database to determine the applicant's credit risk. In other words, the risk analysis module 206 may detect fraudulent email identities based on how the applicant handles past emails from email data obtained from the user device 204.

[0057] The risk analysis module 206 may include a search analysis model to perform a search analysis. It is common that people leave traces online by posting advertisements using their mobile numbers or email identifications. Examples include comments on different blogs, respond to sales advertisements. The search analysis model may obtain numbers from the applicant's caller list in their mobile device to search and match with different context if the obtained numbers relate to stores and/or services. The search analysis may include a search of an identity of the applicant and a search of a lifestyle of the applicant.

[0058] In an embodiment for identity search, the applicant's email and mobile number may be searched using different search engines and the results may be analysed as follows. First, a relationship between search results and search keywords is

established. Once the search results are associated with the applicant, a search score is established based on the context of the search results.

[0059] In lifestyle search, the mobile numbers found on the applicant's caller list are searched on different search engines. These numbers are identified with their respective owners / shops / services / escorts etc. which may give an insight into the lifestyle of the applicant. For example, the lifestyle search may determine that the applicant visits certain food and beverage outlets, such as expensive restaurants or pubs. In an embodiment, the lifestyle search may include a social analysis. In this analysis, there may be integration with various social networks to obtain different data points to understand the applicant's behaviour. This may require permission from the various social networks in order to obtain and use such data points.

[0060] It can be appreciated that other types of mobile data may be used for the identity and lifestyle search. An example of mobile data that can be used includes a call list from the applicant's mobile phone. The call list may assist to identify any recent activity of the applicant through a web search and a telephone directory search. In an example, the web search may determine that the applicant is active in certain websites and such websites are associated with a level of risk which may in turn determine the applicant's behaviour risk. The call list may also assist to identify the most frequent numbers which the applicant had communicated, which in turn may assist to track the applicant. For example, if the call list contains a number of an illegal escort agency, the applicant's loan request may be rejected. Another embodiment of mobile data may include a battery life of the applicant's mobile phone. More specifically, the battery life may determine the frequency of discharge. The battery life of the mobile phone may also assist to understand the working style of the applicant based on his phone usage and/or mobile application usage. Mobile data may also include a model of the mobile phone and a year that it was used or purchased. This may determine whether the applicant is unable to buy new one, not able to pay the loan of same or more size equal to price of mobile, which in turn may be used to determine the credit risk of the applicant. In yet another embodiment, mobile data may include location data frequently visited by the applicant. This may assist to identify the places visited by the applicant which can be further analysed to determine his behaviour risk. Mobile data may also include a plurality of photos taken by the applicant during weekdays. The timing of the plurality of photos that are taken may identify the applicant's commitment to work and thus may be used to determine his behaviour risk.

[0061] After the search analysis is completed, the search analysis model may then provide a search analysis score which may be further combined with other scores from other models to determine a risk analysis score.

[0062] Subsequently, the risk analysis module 206 combines the behaviour risk and credit risk from the various models, i.e. credit analysis model, auto survey model, dedup model, email analysis model, search analysis model and behavioural and/or emotional analysis model, to determine the risk score. The risk analysis module 206 may be able to analyse the risk from the different models using a risk algorithm or a deep neural learning network. At step H, the risk score is transmitted to the decision module 212.

[0063] After receiving the risk score, the facial recognition score and the document verification score from the risk analysis module 206, the facial recognition module 208 and the verification module 210 respectively, the decision module 212 combines the results from the different modules and weighs them as per past experience based on a weighted model. As the scores may be inaccurate due to errors (computational or hardware-related) associated with all the modules. The decision module 212 may overcome such errors by using a decision logic algorithm or a deep neural learning network. A trained neural network may be used where the plurality of evaluation scores from the various modules form the inputs of the trained neural network. Previous payment behaviour (default status) may form an output for supervised learning of the trained neural network. The decision module 212 then determines an outcome of the loan request by rejecting or accepting the applicant's loan request.

[0064] In Figure 2, the facilitator module 202, the risk analysis module 206, the facial recognition module 208, the verification module 210 and the decision module 212 are separate modules. It can be appreciated that they can be one single module such that the facial recognition module 208, the verification module 210, the risk analysis module 206 and the decision module 212 may be contained in the facilitator module 202.

[0065] Use of the term “module” herein may be understood to mean a single computing device or a plurality of interconnected computing devices which operate together to perform a particular function. That is, the module may be contained within a single hardware unit or be distributed among several different hardware units. An exemplary computing device which may be operated as a module is described below with reference to Figure 3.

[0066] Figure 3 shows a schematic diagram of a computer device or computer system 300 suitable for realizing the facilitator module 202, the risk analysis module 206, the facial recognition module 208, the verification module 210, and/or the decision module 212. The following description of the computing device 300 is provided by way of example only and is not intended to be limiting.

[0067] As shown in Figure 3, the example computing device 300 includes a processor 304 for executing software routines. Although a single processor is shown for the sake of clarity, the computing device 300 may also include a multi-processor system. The processor 304 is connected to a communication infrastructure 306 for communication with other components of the computing device 300. The communication infrastructure 306 may include, for example, a communications bus, cross-bar, or network.

[0068] The computing device 300 further includes a main memory 308, such as a random access memory (RAM), and a secondary memory 310. The secondary memory 310 may include, for example, a hard disk drive 312, which may be a hard disk drive, a solid state drive or a hybrid drive and/or a removable storage drive 314, which may include a magnetic tape drive, an optical disk drive, a solid state storage drive (such as a USB flash drive, a flash memory device, a solid state drive or a memory card), or the like. The removable storage drive 314 reads from and/or writes to a removable storage unit 318 in a well-known manner. The removable storage unit 318 may include magnetic tape, optical disk, non-volatile memory storage medium, or the like, which is read by and written to by removable storage drive 314. As will be appreciated by persons skilled in the relevant art(s), the removable storage unit 318 includes a computer readable storage medium having stored therein computer executable program code instructions and/or data.

[0069] In an alternative implementation, the secondary memory 310 may additionally or alternatively include other similar means for allowing computer programs or other instructions to be loaded into the computing device 300. Such means can include, for example, a removable storage unit 322 and an interface 320. Examples of a removable storage unit 322 and interface 320 include a program cartridge and cartridge interface (such as that found in video game console devices), a removable memory chip (such as an EPROM or PROM) and associated socket, a removable solid state storage drive (such as a USB flash drive, a flash memory device, a solid state drive or a memory card), and other removable storage units 322 and interfaces 320 which allow software and data to be transferred from the removable storage unit 322 to the computer system 300.

[0070] The computing device 300 also includes at least one communication interface 324. The communication interface 324 allows software and data to be transferred between computing device 300 and external devices via a communication path 326. In various embodiments, the communication interface 324 permits data to be transferred between the computing device 300 and a data communication network, such as a public data or private data communication network. The communication interface 324 may be used to exchange data between different computing devices 300 which such computing devices 300 form part an interconnected computer network. Examples of a communication interface 324 can include a modem, a network interface (such as an Ethernet card), a communication port (such as a serial, parallel, printer, GPIB, IEEE 1394, RJ45, USB), an antenna with associated circuitry and the like. The communication interface 324 may be wired or may be wireless. Software and data transferred via the communication interface 324 are in the form of signals which can be electronic, electromagnetic, optical or other signals capable of being received by communication interface 324. These signals are provided to the communication interface via the communication path 326.

[0071] As shown in Figure 3, the computing device 300 further includes a display interface 302 which performs operations for rendering images to an associated display 330 and an audio interface 332 for performing operations for playing audio content via associated speaker(s) 334.

[0072] As used herein, the term "computer program product" may refer, in part, to removable storage unit 318, removable storage unit 322, a hard disk installed in hard disk drive 312, or a carrier wave carrying software over communication path 326 (wireless link or cable) to communication interface 324. Computer readable storage media refers to any non-transitory tangible storage medium that provides recorded instructions and/or data to the computing device 300 for execution and/or processing. Examples of such storage media include magnetic tape, CD-ROM, DVD, Blu-ray™ Disc, a hard disk drive, a ROM or integrated circuit, a solid state drive (such as a USB flash drive, a flash memory device, a solid state drive or a memory card), a hybrid drive, a magneto-optical disk, or a computer readable card such as a PCMCIA card and the like, whether or not such devices are internal or external of the computing device 300. Examples of transitory or non-tangible computer readable transmission media that may also participate in the provision of software, application programs, instructions and/or data to the computing device 300 include radio or infra-red

transmission channels as well as a network connection to another computer or networked device, and the Internet or Intranets including e-mail transmissions and information recorded on Websites and the like.

[0073] The computer programs (also called computer program code) are stored in main memory 308 and/or secondary memory 310. Computer programs can also be received via the communication interface 324. Such computer programs, when executed, enable the computing device 300 to perform one or more features of embodiments discussed herein. In various embodiments, the computer programs, when executed, enable the processor 304 to perform features of the above-described embodiments. Accordingly, such computer programs represent controllers of the computer system 300.

[0074] Software may be stored in a computer program product and loaded into the computing device 300 using the removable storage drive 314, the hard disk drive 312, or the interface 320. Alternatively, the computer program product may be downloaded to the computer system 300 over the communications path 326. The software, when executed by the processor 304, causes the computing device 300 to perform functions of embodiments described herein.

[0075] It is to be understood that the embodiment of Figure 3 is presented merely by way of example. Therefore, in some embodiments one or more features of the computing device 300 may be omitted. Also, in some embodiments, one or more features of the computing device 300 may be combined together. Additionally, in some embodiments, one or more features of the computing device 300 may be split into one or more component parts.

[0076] Figure 4 shows a detailed flow chart 400 illustrating an implementation of the method according to the example embodiments. At step 1, the applicant submits an application for a loan request. At step 2, mobile data of the applicant is obtained from his mobile device for credit risk analysis. At step 3, credit data of the applicant is also obtained for credit risk analysis. At step 4, the applicant provides demographic data for email and search analysis. At step 5, behavioral data of the applicant is obtained for behavioral risk analysis. At step 6, the applicant takes a video selfie of one minute for requesting the loan and stating the reasons for the loan request. At step 7, the applicant uploads the relevant documents for verification analysis. At least some of the above steps may take place substantially concurrently.

[0077] At step 8, the uploaded documents are analyzed to check whether they are tampered with. If the documents are tampered, manual inspection of the documents is performed in step 9. On the other hand, if the documents are not tampered, the identity of the applicant is verified using OCR technology at step 10. At step 11, a document verification score is calculated based on the verification of the applicant's identity. Simultaneously, the applicant's face is detected from the documents at step 12 if the documents are not tampered. At step 13, a face recognition model compares a first facial image of the applicant from the documents and a second facial image taken from the video selfie. At step 14, if the faces are determined to be different after comparison, manual inspection of the documents is performed. On the other hand, if the faces are identical, a facial recognition score is calculated based on the acceptance of the facial images at step 15.

[0078] At step 16, demographic data of the applicant, such as the data provided to a mobile operator, are verified. An auto survey of the applicant's demographic data is also performed at step 17. If the demographic data provided to the mobile operator cannot be verified, the demographic data may be routed for auto survey. At step 18, the demographic data is subjected to an email analysis and a search analysis. At step 19, after the demographic data verification and the email and search analysis are completed, the identity of the applicant is determined to check whether he is a returning customer. If the applicant is determined to be a returning customer, a risk score is updated for the applicant's behavioral risk analysis at step 20. Simultaneously, at step 21, the risk score is also updated for the applicant's credit risk analysis. On the other hand, if the applicant is not a returning customer, data deduplication is carried out at step 22. If data deduplication is absent, i.e. the applicant is not a fraudster, the risk score may also be updated for the applicant's behavioral risk analysis and credit risk analysis at step 23 and step 24 respectively. If data deduplication is present, i.e. the applicant is a fraudster, the applicant is blacklisted at step 25 and the loan request is denied. The applicant's credit risk may also be analyzed based on the applicant's mobile data and the credit data while his behavioral risk may be analyzed using his behavioral data and video selfie. Thereafter, at step 26, the risk score is determined based on the applicant's credit risk and behavioral risk. The risk score, document verification score and the facial recognition score is further routed to a decision logic at step 27 and at step 28, the decision logic determines whether the loan request is accepted or rejected.

[0079] The system and method for processing a loan application as described herein may result in reducing operational costs for financial institutions while minimizing their exposure to risk. It may also improve the turnaround time for a loan request by automating the various processes, such as risk assessment. The automation of risk assessment may allow financial institutions to better understand and mitigate any risk that is associated with the applicant. Unlike traditional loan request applications, the method and system as disclosed herein offer financial institutions a more efficient and faster way of approving or rejecting micro loans for individuals and small business entities.

[0080] It will be appreciated by a person skilled in the art that numerous variations and/or modifications may be made to the present invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects to be illustrative and not restrictive.

CLAIMS

1. A system for processing a loan application comprising:
a processor; and
a memory unit communicatively coupled to the processor,
wherein the memory unit is configured to receive a loan request from an applicant and evaluation data specific to the applicant for providing an assessment of the loan request; and
wherein the processor is configured to:
analyse the evaluation data to determine a plurality of evaluation scores specific to the applicant; and
determine an outcome of the loan request based on the evaluation scores,
wherein the evaluation scores comprise a risk score determined based on the applicant's credit risk and behaviour risk; and
wherein the processor is further configured to determine the behaviour risk based on behaviour data associated with the applicant in connection with the loan request and video data submitted by the applicant as evaluation data.
2. The system as claimed in claim 1, wherein the processor is further configured to update the behaviour risk based on a determination whether the applicant is a returning customer.
3. The system as claimed in claim 1 or 2, wherein the processor is further configured to update the behaviour risk based on at least one of an email analysis, a search analysis and a demographic data analysis.
4. The system as claimed in 3, wherein the search analysis comprises a search of an identity of the applicant and a search of a lifestyle of the applicant.
5. The system as claimed in claim 3, wherein the processor is further configured to analyse the demographic data based on at least one of a verification of the applicant's data provided by a third-party and an assessment based on the applicant's past history.

6. The system as claimed in claim 2, wherein the processor is further configured to determine the credit risk based on at least the applicant's credit data, and wherein the processor is further configured to update the credit risk based on the determination whether the applicant is a returning customer.
7. The system as claimed in claim 2, wherein the processor is further configured to perform a data deduplication following the determination whether the applicant is a returning customer.
8. The system as claimed in claim 1, wherein the evaluation scores further comprise a document verification score and a facial recognition score.
9. The system as claimed in claim 8, wherein the processor is further configured to determine the document verification score based on one or more documents provided by the applicant as evaluation data, and check whether the one or more documents have been tampered with.
10. The system as claimed in claim 8, wherein the processor is further configured to determine the facial recognition score based on a comparison of a first facial image detected from one or more documents provided by the applicant as evaluation data and a second facial image extracted from video data submitted by the applicant as evaluation data.
11. The system as claimed in claim 8, wherein the processor is further configured to determine an outcome of the loan request based on a weighted model combining the risk score, document verification score and facial recognition score.
12. An automated method for processing a loan application, the method comprising:
 - receiving, via a user device, a loan request from an applicant;
 - obtaining evaluation data specific to the applicant for providing an assessment of the loan request;
 - analysing the evaluation data to determine a plurality of evaluation scores specific to the applicant;
 - determining an outcome of the loan request based on the evaluation scores,

wherein the evaluation scores comprise a risk score determined based on the applicant's credit risk and behaviour risk; and

wherein the behaviour risk is determined based on behaviour data exhibited by the applicant in connection with the loan request and video data submitted by the applicant as evaluation data.

13. The method as claimed in claim 12, wherein the behaviour risk is updated based on a determination whether the applicant is a returning customer.

14. The method as claimed in claim 12 or 13, the method further comprising:
updating the behaviour risk based on at least one of an email analysis, a search analysis and a demographic data analysis.

15. The method as claimed in 14, wherein the search analysis comprises a search of an identity of the applicant and a search of a lifestyle of the applicant.

16. The method as claimed in claim 14, wherein the demographic data analysis comprises at least one of a verification of the applicant's data provided by a third-party and an assessment based on the applicant's past history.

17. The method as claimed in claim 13, wherein the credit risk is determined based on at least the applicant's credit data, and wherein the credit risk is updated based on the determination whether the applicant is a returning customer.

18. The method as claimed in claim 13, further comprising a data deduplication step following the determination whether the applicant is a returning customer.

19. The method as claimed in claim 12, wherein the evaluation scores further comprise a document verification score and a facial recognition score.

20. The method as claimed in claim 19, wherein the document verification score is determined based on one or more documents provided by the applicant as evaluation data, and wherein analysing the evaluation data comprises checking whether the one or more documents have been tampered with.

21. The method as claimed in claim 19, wherein the facial recognition score is determined based on a comparison of a first facial image detected from one or more documents provided by the applicant as evaluation data and a second facial image extracted from video data submitted by the applicant as evaluation data.

22. The method as claimed in claim 19, wherein determining an outcome of the loan request comprises combining the risk score, document verification score and facial recognition score based on a weighted model.