November 2023

INFINITY PAY

SAHIL ARORA
Visa

“INFINITY PAY”

VISA

INVENTOR(S):

SAHIL ARORA

TECHNICAL FIELD

[0001] The present disclosure pertains to the field of contactless payment systems and biometric authentication. More specifically, it relates to a novel system and method for enabling secure contactless payments using biometric identification, even in situations where the user's primary device is unavailable. This innovative solution incorporates a combination of machine learning, neural networks, blockchain technology, and interconnected IoT devices to facilitate seamless and secure transactions.

BACKGROUND

[0002] In the contemporary landscape of financial transactions, contactless payment systems have become increasingly prevalent, offering users the convenience of quick and secure payments without the need for physical cash or traditional payment cards. However, these systems are not without their limitations, which primarily revolve around their dependence on a user's personal device, such as a smartphone or smartwatch, for both user identification and payment authorization.

[0003] Typically, when a user wishes to make a contactless payment, their device plays a pivotal role in facilitating the transaction. It not only stores their payment credentials but also acts as a communication gateway between the user, the point of sale (POS) device, and the payment network. While this setup has revolutionized the way people make payments, it is not without its shortcomings.

[0004] One significant drawback of current contactless payment systems is their vulnerability to device-related issues. When a user's primary device is unavailable due to reasons such as a dead battery, loss, or simply being forgotten at home, they are left stranded without the ability to make payments, even in emergency situations. This limitation is further exacerbated by the reliance on the device's internet connection for transaction processing, which may not always be available, especially in remote or off-grid locations.

[0005] Moreover, the existing contactless payment systems, while efficient in many regards, have been critiqued for their security vulnerabilities. Traditional payment cards, for instance, are susceptible to theft, fraud, and unauthorized use. Although some modern systems have integrated biometric authentication methods, they often fall short in providing a comprehensive solution that ensures both user convenience and robust security.

[0006] Thus, there is a need for a system and a method to address these pressing issues and revolutionize the landscape of contactless payments.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate exemplary embodiments and, together with the description, explain the disclosed principles. In the figures, the left-most digit(s) of a reference number identifies the figure in which the reference number first appears. The same numbers are used throughout the figures to reference features and components. Some embodiments of device or system and/or methods in accordance with embodiments of the present subject matter are now described, by way of example only, and with reference to the accompanying figures, in which:

[0008] **Fig. 1** illustrates an enrollment phase for a system, in accordance with an embodiment of the present disclosure.

[0009] **Fig. 2** illustrates a transaction phase of the system that demonstrates the working of the system, in accordance with an embodiment of the present disclosure.

[0010] The figures depict embodiments of the disclosure for purposes of illustration only. One skilled in the art will readily recognize from the following description that alternative embodiments of the structures and methods illustrated herein may be employed without departing from the principles of the disclosure described herein.

DESCRIPTION OF THE DISCLOSURE

[0011] It is to be understood that the present disclosure may assume various alternative variations and step sequences, except where expressly specified to the contrary. It is also to be understood that the specific devices and processes illustrated in the attached drawings and described in the following specification are simply exemplary and non-limiting embodiments or aspects. Hence, specific dimensions and other physical characteristics related to the embodiments or aspects disclosed herein are not to be considered as limiting.

[0012] In the present document, the word “exemplary” is used herein to mean “serving as an example, instance, or illustration.” Any embodiment or implementation of the present subject matter described herein as “exemplary” is not necessarily to be construed as preferred or advantageous over other embodiments.

[0013] While the disclosure is susceptible to various modifications and alternative forms, specific embodiment thereof has been shown by way of example in the drawings and will be described in detail below. It should be understood, however that it is not intended to limit the disclosure to the particular forms disclosed, but on the contrary, the disclosure is to cover all modifications, equivalents, and alternative falling within the spirit and the scope of the disclosure.

[0014] The terms “comprise”, “comprising”, or any other variations thereof, are intended to cover a non-exclusive inclusion, such that a setup, device, or method that comprises a list of components or steps does not include only those components or steps but may include other components or steps not expressly listed or inherent to such setup or device or method. In other words, one or more elements in a device or system or apparatus proceeded by “comprises… a” does not, without more constraints, preclude the existence of other elements or additional elements in the device or system or apparatus.

[0015] The terms “an embodiment”, “embodiment”, “embodiments”, “the embodiment”, “the embodiments”, “one or more embodiments”, “some embodiments”, and “one embodiment” mean “one or more (but not all) embodiments of the disclosure(s)” unless expressly specified otherwise.

[0016] The terms “including”, “comprising”, “having” and variations thereof mean “including but not limited to” unless expressly specified otherwise.

[0017] The present disclosure introduces a groundbreaking feature to revolutionize the landscape of contactless payments. It provides a system and a method for enabling emergency contactless payments through biometric identification, all without relying on a personal device or its internet connection.

[0018] The system disclosed in the disclosure leverages interconnected IoT (Internet of Things) devices with biometric scanners (such as fingerprint scanners or facial recognition cameras) to capture the user's biometric data at the point of payment. This data is processed by neural network-based models for real-time identity verification. Upon successful identification, the system uses a blockchain network to securely carry out the payment transaction, recording it immutably for transparency.

[0019] The system allows users to make contactless payments in emergency situations, even when their primary device is not available. Furthermore, by using biometrics for identification, it provides a highly secure method of user authentication that is difficult to forge, thereby enhancing the overall security of the contactless payment process.

[0020] **Fig. 1** illustrates the enrollment phase of the method disclosed forthwith in the present disclosure. In an embodiment of the present disclosure, the Point of Sale (POS) devices may take as input, the biometric data of the user. The biometric data of the user may include (and is not limited to) facial features, iris, fingerprint scans etc. of the user.

[0021] The biometric data of the user may then be encrypted using advanced cryptographic algorithms to protect sensitive information. The encrypted biometric data and payment details may be stored in a secure cloud server. Services like Amazon S3 may be used for storage due to their robust security measures, scalability, and reliability.

[0022] Deep learning models may be used for biometric verification. Some examples of the same may be Convolutional Neural Networks for facial recognition, Recurrent Neural Networks for voice recognition etc. These models may then be trained using frameworks including but not limited to TensorFlow or PyTorch etc. These models may then be deployed on cloud servers using technologies like AWS SageMaker, Google AI Platform etc.

[0023] In an embodiment, the POS devices as disclosed above may have biometric scanners and these devices may be connected using IOT protocols including but not limited to MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol) etc. which are two popular protocols used to enable communication and data exchange between IoT devices, sensors, systems and even the central server. The technologies that these POS devices may use include Radio-Frequency Identification (RFID), Near Field Communication(NFC) etc. for contactless communication with users' devices.

[0024] **Fig. 2** illustrates the transaction phase of the system and the method disclosed in the disclosure. Besides, the steps of the enrollment phase as already seen above, the transaction phase takes it forward and describes the other aspects of the present disclosure.

[0025] Going back to the Machine Learning Models and Neural Networks as mentioned above, described here is a detailed explanation of the: Machine Learning Models and Neural Networks:

Machine Learning Models and Neural Networks:

• **Input**: The raw biometric data (such as facial images, fingerprints, or voice clips) from the user are the inputs for these models.

• **Processing**: This data is processed through deep learning models. Convolutional Neural Networks (CNNs), in an embodiment, may extract features from input images using convolutional layers, pooling layers, and fully connected layers. These models are trained on a large dataset of similar biometric inputs to learn the distinctive features that can differentiate users.

• **Output**: The output of these models is a set of distinctive features or patterns that uniquely represent the user's biometric data. The idea is to render as output a set of unique distinctive features or patterns of data that are enough to represent the biometric data of the user.

In an embodiment, a verification task is also performed by these models. In the verification task, the model verifies the biometric data of the user. The model receives as input the biometric data of the user, compares it with the data already registered with the model stored in an encrypted form.

In an embodiment, in a verification task, the model may also render as output a confidence score indicating the likelihood that the input biometric data matches the registered data.

[0026] In an embodiment, the POS devices with biometric scanners can be connected using IoT protocols. These POS devices with biometric scanners, serve as a critical bridge between users, the central server, and the payment ecosystem. These devices are designed to enable seamless and secure contactless payments by incorporating various technologies and communication protocols including but not limited to MQTT (Message Queuing Telemetry Transport) and CoAP (Constrained Application Protocol).

[0027] In an embodiment, these POS devices using IOT protocols are equipped with contactless communication technologies to interact with users' devices, enhancing the user experience and enabling secure payments. The technologies that these POS devices may use include Radio-Frequency Identification (RFID), Near Field Communication (NFC) etc. for contactless communication with users' devices.

[0028] A detailed functioning of the Interconnected IoT Devices is described herewith (POS devices with biometric scanners):

•**Input**: The primary input for these devices is the biometric data provided by the user at the point of payment. Additionally, these devices may receive signals from the central server that may be in the form of commands, updates, etc.

•**Processing**: The devices process the biometric data of the user using inbuilt hardware (for example-the image sensors in a facial recognition camera). This raw biometric data may then be converted into a digital format.

•**Output**: The digital biometric data may then be encrypted and transmitted securely to the central server for verification. In an embodiment, these devices may display or print out payment receipts after successful transactions.

[0029] In an embodiment, a robust Blockchain Transaction System may be employed to handle transactions securely and transparently. This system may utilize a private blockchain network, which can be built using well-established platforms including but not limited to Hyperledger Fabric, Ethereum etc.

[0030] The Blockchain Transaction Network works as follows:

Input:
The primary inputs for this system may encompass two key components:

Payment Requests: These requests may be initiated by the cloud server after successful biometric verification of the user. They may contain essential information, including the transaction amount, payment destination, user identification etc.

Digital Wallets: Each participant in the system, including users and retailers may possess a unique digital wallet within the blockchain network. These wallets may serve as the repositories for their respective cryptocurrency or digital payment tokens.

Processing:
Transaction Handling: Each payment request received by the system may be processed as a transaction. These transactions may then be submitted to the private blockchain network, where they undergo validation and consensus.

Smart Contracts: Smart contracts, which are self-executing agreements with predefined rules and conditions, automatically handle the transaction logic. Upon execution, these contracts facilitate the transfer of cryptocurrency or digital tokens, debiting the user's wallet for the transaction amount and crediting the retailer's wallet.

Node Validation: Transactions may then be subjected to validation by nodes (computers) within the blockchain network. Once consensus is reached, and the transaction is verified as legitimate, it is added to a new block in the blockchain.

Output:

The output of this system is a robust, immutable record of each transaction on the blockchain. This record may be accessed and viewed by all participants in the network, ensuring complete transparency and trust in the payment process. Furthermore, the system may promptly generate a transaction confirmation, providing users and retailers with tangible proof that the payment was successfully executed. In cases where a transaction encounters issues, an error message may be generated and sent back to the cloud server for appropriate handling.

[0031] In an embodiment, real-time biometric verification may play a pivotal role in enhancing security and user authentication. When a user initiates a transaction at a POS device, their biometric data may promptly be captured by the device itself. This biometric data may then securely be transmitted to the cloud server for real-time verification. The cloud server houses the necessary machine learning models and neural networks to compare the presented biometric data with the registered data, ensuring the user's identity. To expedite this verification process and reduce latency, edge computing techniques may be employed. Edge computing allows data processing to occur closer to the source, such as at the POS device or nearby edge servers, rather than relying solely on centralized cloud servers. This approach accelerates the verification process and ensures swift responses to users' payment requests.

[0032] In an embodiment, the payment authorization process in this system may be facilitated by smart contracts, which are programmed with specific logic to ensure secure and automated transactions. Once the cloud server successfully verifies the user's identity through their biometric data, it may trigger a smart contract on the blockchain. This smart contract may contain predefined transaction logic, including the instructions to debit the user's digital wallet for the transaction amount and credit the retailer's digital wallet with the same amount. The contract ensures that these actions are executed seamlessly and securely.

[0033] In an embodiment, following the execution of the smart contract and the completion of the transaction, the transaction details, including the amount, timestamp, user and retailer identifiers, and any other relevant information, may be recorded as a block on the blockchain. This recording ensures the immutability and transparency of the payment history. Subsequently, a transaction receipt may be generated, serving as a formal confirmation that the payment was successfully processed. This receipt may include essential transaction details and may be made available to both the user and the retailer. Users may receive the receipt electronically, while retailers may choose to receive it through various means, including email or integrated point-of-sale systems.

[0034] In an embodiment, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer-readable storage medium refers to any type of physical memory on which information or data readable by a processor may be stored. Thus, a computer-readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) to perform steps or stages consistent with the embodiments described herein. A non-transitory computer readable medium may include media such as magnetic storage medium, optical storage, volatile and non-volatile memory devices etc. Further, non-transitory computer-readable media may include all computer-readable media except for a transitory. The code implementing the described operations may further be implemented in hardware logic (e.g., an integrated circuit chip, Programmable Gate Array (PGA), Application Specific Integrated Circuit (ASIC), etc.).

[0035] The described operations may be implemented as a method, system or article of manufacture using standard programming and/or engineering techniques to produce software, firmware, hardware, or any combination thereof. The described operations may be implemented as code maintained in a “non-transitory computer readable medium”, where a processor may read and execute the code from the computer readable medium. The processor is at least one of a microprocessor and a processor capable of processing and executing the queries.

[0036] The illustrated steps are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purposes of illustration, and not limitation. Further, the boundaries of the functional building steps have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments. Also, the words "comprising," "having," "containing," and "including," and other similar forms are intended to be equivalent in meaning and be open ended in that an item or items following any one of these words is not meant to be an exhaustive listing of such item or items or meant to be limited to only the listed item or items. It must also be noted that as used herein, the singular forms “a,” “an,” and “the” include plural references unless the context clearly dictates otherwise.

[0037] Finally, the language used in the specification has been principally selected for readability and instructional purposes, and it may not have been selected to delineate or circumscribe the inventive subject matter. Accordingly, the disclosure of the embodiments of the disclosure is intended to be illustrative, but not limiting, of the scope of the disclosure.

[0038] With respect to the use of substantially any plural and/or singular terms herein, those having skill in the art can translate from the plural to the singular and/or from the singular to the plural as is appropriate to the context and/or application. The various singular/plural permutations may be expressly set forth herein for sake of clarity.

INFINITY PAY

ABSTRACT

The present disclosure relates to the field of contactless payment systems and biometric authentication. More specifically, it relates to a novel system and method for enabling secure contactless payments using biometric identification, even in situations where the user's primary device is unavailable. This innovative solution incorporates a combination of machine learning, neural networks, blockchain technology, and interconnected IoT devices to facilitate seamless and secure transactions.

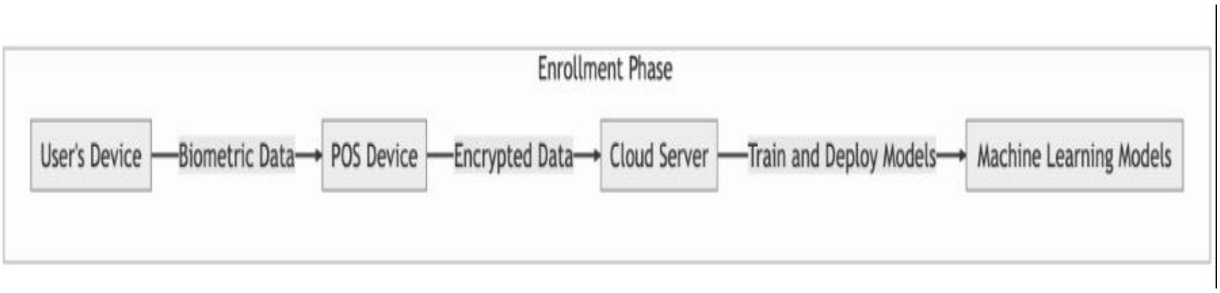
Enrollment Phase
User's Device
Biometric Data
POS Device
Encrypted Data
Cloud Server
Train and Deploy Models
Machine Learning Models

Fig. 1

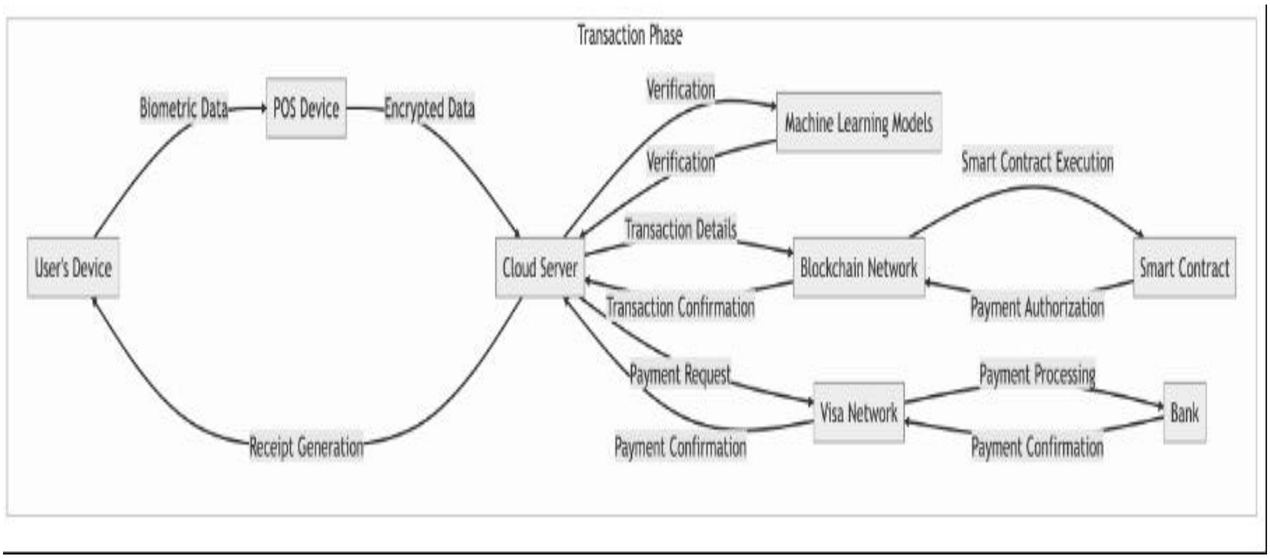
Transaction Phase
Biometric Data
POS Device
Encrypted Data
Verification
Machine Learning Models
Verification
Smart Contract Execution
User's Device
Cloud Server
Transaction Details
Blockchain Network
Smart Contract
Transaction Confirmation
Payment Authorization
Payment Request
Payment Processing
Visa Network
Bank
Receipt Generation
Payment Confirmation
Payment Confirmation

Fig. 2