UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
62/460,217	02/17/2017		130	520619335		

CONFIRMATION NO. 4463

FILING RECEIPT

Sanjay Shrivastava
34 Southern Hills Drive
Skillman, NJ 08558

OC000000089545326

Date Mailed: 03/01/2017

Receipt is acknowledged of this provisional patent application. It will not be examined for patentability and will become abandoned not later than twelve months after its filing date. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Sanjay Shrivastava, Skillman, NJ;
Kawaljit Singh, Princeton, NJ;
Amit Poddar, Stamford, CT;

Applicant(s)

Sanjay Shrivastava, Skillman, NJ;
Kawaljit Singh, Princeton, NJ;
Amit Poddar, Stamford, CT;

Power of Attorney: None

Permission to Access Application via Priority Document Exchange: No

Permission to Access Search Results: No

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 02/28/2017

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 62/460,217**

Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

Software and method for enabling secure storage and authentication of user digital credential and assets

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
62/460,217	02/17/2017		130	520619335		

CONFIRMATION NO. 4463

PROVISIONAL APPLICATION FOR PATENT

INVENTION TITLE

Software and method for enabling secure storage and authentication of user digital credential and assets.

BACKGROUND OF THE INVENTION

Problem Solved: In current forms of identity management, customer's personal digital assets are stored with a single trusted entity, which acts as a centralized authority for safekeeping of this information.

The security concern with this approach is that if the trusted entity gets hacked, there is a risk of the customer's personal digital assets being compromised.

Further, such solutions have the limitation of single point of failure i.e. if the identity management server/domain goes down, user authentication cannot proceed and overall user experience is compromised.

Current identity management solutions store user's confidential identity digital assets in its entirety within one company/domain. There are two problems with this approach -

- User's personal data can be compromised if the company's backend servers are hacked and,

- Such solutions have the limitation of single point of failure i.e. if the identity management server/domain is down, user authentication cannot proceed and overall user experience is compromised.

With this invention

- User's confidential digital asset can never be compromised as it is never stored in it's entirely on a single company/domain. Encrypting the digital asset, splitting it into multiple parts and then decentralizing the storage of these individual parts across multiple trusted domains/companies, safeguards the asset from any possible hacks.

- We are immune to a single point of failure in the network or storage, since the user confidential digital asset is split into multiple parts and redundantly stored on multiple servers across multiple domains/companies.

DETAILED DESCRIPTION OF THE INVENTION

As stated above, in current forms of identity management, customer's personal digital assets are stored with a single trusted entity, which acts as a centralized authority for safekeeping of this information.

The security concern with this approach is that if the trusted entity gets hacked, there is a risk of the customer's personal digital assets being compromised.

Further, such solutions have the limitation of single point of failure i.e. if the identity management server/domain goes down, user authentication cannot proceed and overall user experience is compromised. The invention claimed here solves this problem.

This invention does not store the customer's identity digital assets in its entirety in a single domain/company and never does this information go on the wire/network to a single domain/company in its entirety. Also, information is never merged or reconstructed thereafter.

Our approach to digital identity is immune to a single point of failure in the network or storage, since the user confidential digital asset is split into multiple parts and redundantly stored on multiple servers across multiple domains/companies.

The claimed invention differs from what currently exists. Customer's confidential identity digital assets are never stored in its entirety within a single company/domain at any time. Splitting the digital asset

into multiple parts and then redundantly storing these individual parts across multiple trusted domains/companies, safeguards the asset from any possible hacks and single point of failure.

This invention is an improvement on what currently exists. Customer's confidential identity digital assets are never stored in its entirety within a single company/domain at any time. Splitting the digital asset into multiple parts and then redundantly storing these individual parts across multiple trusted domains/companies, safeguards the asset from any possible hacks and single point of failure.

As mentioned above, these current systems are inherently disadvantaged because of

- Possibility of user confidential digital asset being compromised and,

- Single point of failure

With this invention

- User's confidential digital asset can never be compromised as it is never stored in it's entirely on a single company/domain. Splitting the digital asset into multiple parts and then decentralizing the storage of these individual parts across multiple trusted domains/companies, safeguards the asset from any possible hacks.

- We are immune to a single point of failure in the network or storage, since the user confidential digital asset is split into multiple parts and redundantly stored on multiple servers across multiple domains/companies.

The Version of The Invention Discussed Here Includes:

1. Client devices such as customer/s desktop/laptop computers, mobile devices
2. Client Application such as a web-browser plug-in, native or HTML5 application running on customer's computing device
3. Customer's Digital Assets such as Passwords, Secret Questions/Answers, Biometrics, NLP, Fingerprints, Personal Records that help to uniquely identify the user
4. End-Point devices such as backend computer servers deployed by trusted domains/companies to store customer's identity data
5. Client Authentication Protocol (CAP) is a client application specific software component

Relationship Between The Components:

A customer uses a Client Application (2) on his Computer Device (1) to create a new account or, to access an existing account on a merchant's website. As part of the sign-in process, he enters his login credentials i.e. Digital Asset (3) which could be any combination of password, facial recognition, fingerprints, etc. The Client Authentication Preprocessor (5) generates a one-way hash of the digital asset, encrypts the hash and splits it into multiple parts. The split components are sent over an asymmetric encrypted channel (like https) to End-Point devices (4) on different domains/organizations/companies for storage in case of a new account creation or, for authentication in case of sign-in.

How The Invention Works:

The present invention enables to secure any user confidential authentication information (passwords, NLP, fingerprints, etc.) for applications connecting to a merchant domain/server. It prevents user confidential assets from being compromised because of various security bugs (like Heartbleed), man-in-the-middle attack and hackers gaining access to a merchant's data center.

This invention describes how a user can be securely authenticated into a master end-point (Company A) using a consensus-based model employing multiple end-points within a trusted Identity network on the cloud.

Creating A New Account

==========

User opens up the Client Application (could be a browser connecting to Merchant Website or a Merchant App) and enters his login credentials (username, password) to create an account.

Step 1: The iLogin Client Authentication Preprocessor (CAP) that is integrated into the Merchant's sign-up page, first validates the password format and then splits the password into "N+1" parts, where N is the # of Nodes in the iLogin Identity Cloud –

$$f(\text{Password, SPLIT}) = \text{Password}_{\text{merchant}} , \text{Password}_{\text{ilogin-p1}} , \text{Password}_{\text{ilogin-p2}} , \ldots , \text{Password}_{\text{ilogin-pn}}$$

Step 2: CAP sends a *Create New Account* request to the Merchant - the request includes the username and $\text{Password}_{\text{merchant}}$

Step 3: Once Merchant validates user data, it broadcasts a *Create New Account* request to the iLogin Identity cloud - this request includes the anonymized username and a unique one-time use session-Id (S_1). This session-Id is the identifier for the CAP -> iLogin Identity Cloud communication.

Step 4: Merchant sends the anonymized username and session-Id (S_1) to the CAP to be used for communication between CAP and iLogin Identity Cloud.

Step 5: CAP sends the *Create New Account* request to the "N" trusted Nodes within the iLogin Identity Cloud. The request to each Node includes the anonymized username, session-Id (S_1) and its password component, $\text{Password}_{\text{ilogin-pn}}$. Each Node within the iLogin Identity Cloud consists of one or more computer server(s) within one of more domains.

Step 6: Once each Node within the iLogin Identity Cloud has successfully stored the user credentials in its ledger, it sends a notification back to the Merchant.

Step 7: Merchant notifies the CAP that the account has been created.

Authenticating A User Account

==========

User opens up the Client Application (could be a browser connecting to Merchant Website or a Merchant App) and enters his login credentials (username, password) to sign in to his account on the merchant site.

Step 1: The iLogin Client Authentication Preprocessor (CAP) that is integrated into the Merchant's sign-up page, first validates the password format and then splits the password into "N+1" parts, where N is the # of Nodes in the iLogin Identity Cloud –

f(Password, SPLIT) = $Password_{merchant}$, $Password_{ilogin\text{-}p1}$,$Password_{ilogin\text{-}p2}$, … , $Password_{ilogin\text{-}pn}$

Step 2: CAP sends a *Validate New Account* request to the Merchant - the request includes the username and $Password_{merchant}$.

Step 3: Once Merchant validates user data, it broadcasts a *Validate New Account* request to the iLogin Identity Cloud - this request includes the anonymized username and a unique one-time use session-Id (S_1). This session-Id is the identifier for the CAP -> iLogin Identity Cloud communication.

Step 4: Merchant sends the anonymized username and session-Id (S_1) to the CAP to be used for communication between CAP and iLogin Identity Cloud.

Step 5: CAP sends the *Validate New Account* request to the "N" trusted Nodes within the iLogin Identity Cloud. The request to each Node includes the anonymized username, session-Id (S_1) and its password component, $Password_{ilogin\text{-}pn}$.

Step 6: Once each Node within the iLogin Identity Cloud has validated the user credentials, it sends a notification back to the Merchant. The servers within each of the trusted Node use a consensus voting mechanism to validate their part of the password and based on the result, a success or failure response is sent back from each Node to the Merchant.

Step 7: Merchant notifies the CAP that the account has been created. The Merchant analyzes the response it receives from the iLogin Identity Cloud Nodes and has the final authority to grant/deny login access - it conveys the outcome to the CAP.

Client Authentication Preprocessor (CAP)

==========

The Client Authentication Preprocessor (CAP) runs in the client application (web browser or native application) on the user's computing device. CAP generates a one-way hash of the digital asset, encrypts the hash and splits it into multiple parts. Each part is sent over an asymmetric encrypted channel (like https) to its endpoint. Each endpoint is a different trusted domain/company. Described below is the algorithm CAP uses to split the digital asset -

L = length of authentication token (one way hash of the user credential)

N = number of distinguished endpoints / companies / domains that will authenticate each part of the token

L_x = length of the authentication token at a given endpoint

$L = L_1 + L_2 + L_3 + L_4 + ... + L_N$

$seed_1$ = f(username, password, merchant-name)

salt = f(Random($seed_1$)); salt is used to generate each end-points index into the authentication token

Receiving endpoint index for each character in password = (next Random number using the salt) % N

How To Make The Invention:

To make this invention one must develop the software and web services that are able to complete the requisite tasks described above. This includes -

1. CAP plug-in - JavaScript component and native iOS and Android libraries for mobile apps.

2. For encryption, Public/Private Key Management software to use within iLogin Identity Cloud.

3. Software component to manage (add/update/validate/delete) the ledger that stores encrypted password components at each of the end-point servers.

4. Web services interface for the CAP to communicate with each of the Nodes in the iLogin Identity Cloud and for the Nodes to communicate with each other.

5. Configuration-driven Consensus software that will be used by the servers within a Node in the iLogin Identity Cloud to vote and validate their respective password component.

All components mentioned above are necessary; however, in the most basic implementation of the iLogin Identity Cloud end-nodes, each end node could have one server, which would preclude the use of consensus software.

This invention allows a merchant / company to authenticate a user not just by using a simple username/password field, but by including other forms of digital assets that are unique to a user - this could include facial recognition, NLP, image, etc. (any personal asset that can be digitized).

How To Use The Invention:

From a customer's perspective, there is no change in the way they authenticate and access their account on a merchant site. In this invention, the emphasis is on the uniqueness and enhanced security

associated with encrypting and splitting the customer's confidential identity digital asset into multiple parts and then storing the individual split components redundantly across multiple trusted servers in the iLogin Identity Cloud. Customer's data is always protected as it is never stored in its entirety in a single domain/company and never does this information go on the wire/network to a single domain/company in its entirety. Also, this information is never merged or reconstructed thereafter. Our solution will protect the consumer's sensitive information in the scenario where a hacker compromises the merchant's data center.

Additionally: The emphasis is on the uniqueness and enhanced security associated with "split" storage of digital assets. The Identity management implementation described in this document for "split and validate" solution can be modified to suit different applications/scenarios.

Also, it can create: This invention can be productized as a cloud-based secure Identity Management Product.

ABSTRACT

Software and method for enabling secure storage and authentication of user digital credential and assets is disclosed. With this invention

- User's confidential digital asset can never be compromised as it is never stored in it's entirely on a single company/domain. Splitting the digital asset into multiple parts and then decentralizing the storage of these individual parts across multiple trusted domains/companies, safeguards the asset from any possible hacks.

- We are immune to a single point of failure in the network or storage, since the user confidential digital asset is split into multiple parts and redundantly stored on multiple servers across multiple domains/companies.

APPENDIX:

Mobile devices such as smart phones (IPhone, Android phones) , tables(IPad etc), net-books– *will be referred as* ***mobile device*** *in the rest of this document.*

Computing device – Includes customer's personal computers such as desktop PCs. Also include any mobile devices.

Client application - includes any web-browser plug-in, native or HTML5 application running on customer's computing device.

Mobile devices, Computing device and Client Application are used interchangeably.

Title: Software solution called "Split and Merge" comprising of client application and web services to enable secure credit card storage and retrieval for payment transactions.

Problem that invention solves: There are various client solutions (apps) available in the market today which enable customers to use their computing devices to pay for online and in-store purchases. Customers have to enter their credit card information only once in the client application. The application stores the information for later use. This makes it unnecessary for customer to refer to their credit cards every time they make a transaction requiring credit card. All the client application providers in the market today adopt one of the two secure methods (listed below) to store customer's credit card number.

Securely store the customer's credit card number on the customer's computing device.
Securely store the customer's credit card number remotely on the cloud/ servers.

Merchant's biggest concern is always the financial liability and bad press resulting from a hacker getting access to the customer's credit card data from any of the payment systems/applications they are integrated with.

Both the above mentioned solutions are insecure in certain scenarios. (Table 1 and 2)

	Server hacked by external users	Information leaked by internal rouge employee	Lost phone	Malicious software on phone	Secure/Not Secure
	False	False	False	False	Secure
Card Information Stored on Server	False	False	False	True	Secure
	False	False	True	False	Secure
	False	False	True	True	Secure
	False	True	False	False	Not Secure
	False	True	True	False	Not Secure
	False	True	False	True	Not Secure
	False	True	True	True	Not Secure
	True	False	False	False	Not Secure
	True	False	False	True	Not Secure
	True	False	True	False	Not Secure
	True	False	True	True	Not Secure
	True	True	False	False	Not Secure
	True	True	True	False	Not Secure
	True	True	False	True	Not Secure
	True	True	True	True	Not Secure

	Server hacked by external users	Information leaked by internal rouge employee	Lost phone	Malicious software on phone	Secure/Not Secure
	False	False	False	False	Secure
Card Information Stored on Phone	False	False	False	True	Not Secure
	False	False	True	False	Not Secure
	False	False	True	True	Not Secure
	False	True	False	False	Secure
	False	True	True	False	Not Secure
	False	True	False	True	Not Secure
	False	True	True	True	Not Secure
	True	False	False	False	Secure
	True	False	False	True	Not Secure
	True	False	True	False	Not Secure

	True	False	True	True	Not Secure
	True	True	False	False	Secure
	True	True	True	False	Not Secure
	True	True	False	True	Not Secure
	True	True	True	True	Not Secure

How does invention solve problem

Our solution uses a unique Random Split and Merge technique to ensure that the credit card number is never compromised in any of the four scenarios described in the problem above. Our solution NEVER stores the complete credit card number in one place. It splits the credit card number, into two or more pieces. Based on a random key/seed, each part is randomized and encrypted. Some of the randomized and encrypted pieces are stored on consumer's computing device and the other on the server cloud. Only at the time of the transaction, we merge the pieces together. For instance a customer's credit card number is only merged during the time of payment and handed over to merchant. The transaction has to be authorized by the customer by providing a six-digit pin. This six-digit pin uses a flavor of the split and merge algorithm. The entire pin is never stored on the mobile device or server. This solution ensures that the credit card number is not compromised in any of these situations

the servers are hacked,

a rouge employee leaks the information

customer loses his/her mobile device

Malicious software hacks their desktop/browser.

	Server hacked by external users	Information leaked by internal rouge employee	Lost phone	Malicious software on phone	Secure/Not Secure
	False	False	False	False	Secure
Card Information Stored Using ILogin Split and Merge	False	False	False	True	Secure
	False	False	True	False	Secure
	False	False	True	True	Secure
	False	True	False	False	Secure
	False	True	True	False	Secure
	False	True	False	True	Secure
	False	True	True	True	Secure
	True	False	False	False	Secure
	True	False	False	True	Secure
	True	False	True	False	Secure
	True	False	True	True	Secure
	True	True	False	False	Secure
	True	True	True	False	Secure

	True	True	False	True	Secure
	True	True	True	True	Secure

How our invention is different and better than anything that exists in its field

In current available solutions, credit card number is stored as plain text or, in most cases, encrypted and stored in its entirety on either the customer's computing device or remotely on the servers. The vulnerability when the information is stored on the server side is that data can still be compromised if the encryption keys are compromised by a rouge employee. There is also a possibility that malicious software can hack the credit card number from the server's memory.

When data is stored on the customer's computing device and if the user loses their device, data from the device can be hacked.

As our solution does not store the complete credit card number in one place, there is no possibility of the data being compromised if either the customer's computing device or back-end server is hacked.

Components required for Split and Merge solution

Components described below are for a sample implementation of random split and merge technique to protect credit card number. The sample application is called ***ILogin payment solution*** and is used to secure customer credit cards using split and merge technique. Here are the main components.

Any computing device used by the customer - includes any mobile device such as mobile phone, tablet etc.. and home computers such as desktop PCs. (C-1)

Credit card number and other credit card details. (C-2)

ILogin web services.(C-3)

ILogin servers on the cloud.(C-4)

ILogin application with Random Split and Merge software library.(C-5)

ILogin powered ecommerce applications OR ILogin powered point of sale terminals at retail stores.(C-6)

The relationship between components is described below

Customers install the ILogin application (C-5) on their computing device (C-1).

Customer creates an account with ILogin using ILogin application (C-5) which internally uses ILogin web services (C-3) and ILogin servers (C-4).

Customer creates a six digit security PIN using ILogin application (C-5) which internally uses ILogin web services (C-3) and ILogin servers (C-4).

Customer registers sensitive data like a credit card number(C-2) with ILogin using ILogin application (C-5) and ILogin web services (C-3). During the registration the ILogin application (C-5) does the following

Splits the credit card number (C-2) into two or more parts – CC_SplitPart_ 1, CC_SplitPart_2, CC_SplitPart_N

Encrypts CC_SplitPart_ 1, CC_SplitPart_ 2…..CC_SplitPart N

Stores CC_SplitPart_ 1 on the computing device (C-1) .

Store CC_SplitPart_ 2, CC_SplitPart N on the ILogin servers on the cloud (C-4).

During the transaction with an e-commerce application or a retail merchant (C-6), the customer authorizes ILogin application (C-5) to provide the credit card information (C-2) to the e-commerce application or retail merchant POS (C-6). The ILogin application (C-5) does the following during the transaction

Verifies that the customer PIN is correct by communicating with ILogin servers in the cloud (C-4) using ILogin web services (C-3).

Brings the encrypted part (CC_SplitPart_ 2, …CC_SplitPart N) stored on the ILogin servers (C-4) using the ILogin web services (C-3) to the ILogin application (C-5) running on the customer's computing device (C-1).

ILogin application (C-5) decrypts CC_SplitPart_ 1, CC_SplitPart_ 2 …. CC_SplitPart N and merges the encrypted parts on the customer's device (C-1) to derive the complete credit card number (C-2).

Passes the information to the e-commerce application or to the retail merchant POS (C-6).

Solution Details (Described for sample payment solution called ILogin)

Customer registration and credit card storage using Split Storage Technique - Figure 1

Step1: Customers install the ILogin application (C-5) on their computing devices (C-1).

Step2: Customer creates an account with ILogin using ILogin application (C-5) which internally uses ILogin web services (C-3) and ILogin servers (C-4).

Step3:

User enters Pin ($Pin_{userorg}$) on their client (C-1) a 6 digit number.
ILogin app (C-5) generates a random bit string Pin_{random}.
ILogin app(C-5) generates $Pin_{server} = f(Pin_{random}, Pin_{userorg})$.
Pin_{server} is stored on iLogin server (C-4) using ILogin web services (C-3).
Pin_{random} is stored on the device(C-1).

Step4:

User enters credit card (C-2) information ($CC_{entered}$, type, name, expiration, CVV2) on ILogin app(C-5).Manual entry can be replaced with camera and OCR techniques.

$CC_{entered}$, type, name, expiration and CVV2# is sent over HTTPs connection from the device (C-1) to a payment gateway (this request never touches ILogin servers(C-4)) such as authorize.net to check card validity. **This is only done once during credit card registration**. CVV2 is discarded. **(ILogin app(C-5) and server (C-4) never store CVV2 value).**

ILogin app (C-5) generates a random bit string $CC_{random.}$

ILogin app (C-5) splits the card into two or more parts - $CC_{entered\text{-}part1}$, $CC_{entered\text{-}part2.\ ...CCentered\text{-}part\ N}$ Part to be stored on device (C-1) called CC_{phone} = < $CC_{random,}$ F($CC_{random,}$ $CC_{entered\text{-}part1}$)>. Part to be stored on the Ilogin server (C-4) called CC_{server} = f($CC_{random,}$ $CC_{entered\text{-}part2,\ ...CCentered\text{-}part3}$) .

CC_{phone} is stored on device (C-1), tagged with type of card, last 4 digits/card alias - all encrypted with ($Pin_{userorg}$). Cc_{server}, type and other info from step 1 (excluding CVV2) is sent to ILogin server (C-4) using ILogin web services (C-3). On ILogin server (C-4), a unique CC Entity Id is assigned to this credit card. (The complete credit card information is never present on the ILogin server (C-4), only a encrypted part of it is there). This CC Entity Id is sent back to the device (C-1) where it is stored (along with the Cc_{phone}), encrypted with the ($Pin_{userorg}$).

<Since we refer to qrcodes below, lets add a line here about the qrcode being dynamically created on the phone - and, lets add in the credit card specific data that we encode in there.>

Payment at Brick and Mortar sore (Merge technique) - Figure 2.

The merchant uses an ILogin enabled Point Of Sale software (C-6) to accept payment through customer's mobile phone (ILogin app installed).

: Point of Sale software (C-6) displays ILogin window for scanning QR-Code from customer's mobile device (C-1).

: Merchant scans the ILogin QR-Code on customer's mobile device(C-1). This transfers CC_{phone}, Pin_{random}, ILogin customer Id and other information to the ILogin merchant module integrated with Point Of Sale software (C-6).

: Customer is promoted to enter six digit ILogin PIN ($Pin_{userorg}$) on the POS console (C-6).*Note: Three unsuccessful PIN attempts locks the customer's ILogin account.*

Step 4: ILogin merchant module(C-5) calculates the Pin_{server} using f(Pin_{random}, $Pin_{userorg}$) and sends Pin_{server} to ILogin server (C-4) for validation using Ilogin web services (C-3). ILogin merchant module(C-5) uses Ilogin web services (C-3) to download CC_{server} and other necessary info from the ILogin server (C-4) once $Pin_{userorg}$ is validated. ILogin merchant module(C-5) decrypts CC_{server} and CC_{phone} and uses f($CC_{server,}$ $Cc_{phone)}$ to get the original credit card $CC_{entered.}$ (C-2). $CC_{entered,}$ expiration date and other necessary information needed for merchant to process the credit card transaction is passed to the POS software (C-6) from ILogin application (C-5).

Mobile e-commerce using ILogin (Merge technique) - Figure 3.

The customer uses an ILogin powered e-Commerce mobile app (C-6) to make payments.

: On the payment screen, the ILogin powered e-commerce app (C-6) gives option for customer to enter credit card information, one of which is "**Get CC Info from ILogin".**

: If customer selects "**Get CC Info from ILogin"** option, he or she is prompted to enter six-digit ILogin PIN ($Pin_{userorg}$).*Note: Three unsuccessful PIN attempts locks the customer's ILogin account*

Step 3**:**

ILogin merchant module(C-5) calculates the Pin_{server} using f(Pin_{random}, $Pin_{userorg}$) and sends Pin_{server} to ILogin server (C-4) for validation using Ilogin web services (C-3). ILogin merchant module(C-5) uses Ilogin web services (C-3) to download CC_{server} and other necessary info from the ILogin server (C-4) once $Pin_{userorg}$ is validated. ILogin merchant module(C-5) decrypts CC_{server} and CC_{phone} and uses f($CC_{server,}$ $Cc_{phone)}$ to get the original credit card $CC_{entered.}$ (C-2). $CC_{entered,}$ expiration date and other necessary information needed for merchant to process the credit card transaction is passed to the e-commerce application (C-6) from ILogin application (C-5).

How would a person make the invention? To make this invention one must develop the software (application and library) and web services that are able to complete the requisite tasks described here above.

Which elements are necessary? Which are optional? What elements could be added to make your invention work better? Please use complete sentences.

Essential elements -> ILogin web services.(C-3) , ILogin servers on the cloud.(C-4) and ILogin application with Random Split and Merge software library(C-5) are must to secure the sensitive information (C-2) using random split and merge technique.

Optional elements -> ILogin powered ecommerce applications OR ILogin powered point of sale terminals at retail stores.(C-6) is not required in case where consumer wants to use split and merge technique to digitize their sensitive information for easy access .

How can the components or elements be shuffled, interchanged, or reconfigured to cause the invention to perform an identical or similar function? (This is optional, but answering can potentially give you more protection in the future.) Please use complete sentences.

How would a person use the invention to solve the problem that your invention solves? This is another very important section: Please be specific about the steps involved

The consumers who don't want to carry the sensitive information in physical form such as credit cards , passwords, pins, health records, etc. would use the ILogin application to securely store their sensitive information using the random split storage technique. When they need the information at later point for personal viewing or to provide to someone else such as passing credit card, passowrds, pins, health records etc. information to e-commerce application, they can easily fetch it using the secure merge technique. Our solution will protect the consumer's sensitive information in the following four scenarios which can happen with solutions which store this information either on their servers or on customer's devices such as mobile phone or web browsers.

- the servers are hacked,
- a rouge employee leaks the information
- customer loses his/her mobile device
- malicious software hacks their desktop/browser.

Please list and describe all products and devices, compositions and other useful items that your invention can produce.

The emphasis is on the uniqueness and enhanced security associated with split storage and merge during transaction solution and not on the specific implementation of “split and Merge” solution described in this document. The exact implementation described in this document for “split and merge” solution can be modified to suit different applications/scenarios.

The split and merge technology can be used in embedded device or be built in the firmware of mobile phones, tablets, desktops, web browsers, client apps, POS terminals, card readers and other computing device which will eliminate the need for installation of application.