US 20210004492A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2021/0004492 A1

Britt et al. (43) Pub. Date: Jan. 7, 2021

(54) **DATA BREACH PREVENTION AND REMEDIATION**

(71) Applicant: **Cyber Team Six**, Huntersville, NC (US)

(72) Inventors: **Jason Britt**, Birmingham, AL (US); **Patrick A. Westerhaus**, Huntersville, NC (US)

(73) Assignee: **Cyber Team Six**

(21) Appl. No.: **16/879,680**

(22) Filed: **May 20, 2020**

Related U.S. Application Data

(60) Provisional application No. 62/870,332, filed on Jul. 3, 2019, provisional application No. 62/897,197, filed on Sep. 6, 2019.

Publication Classification

(51) **Int. Cl.**

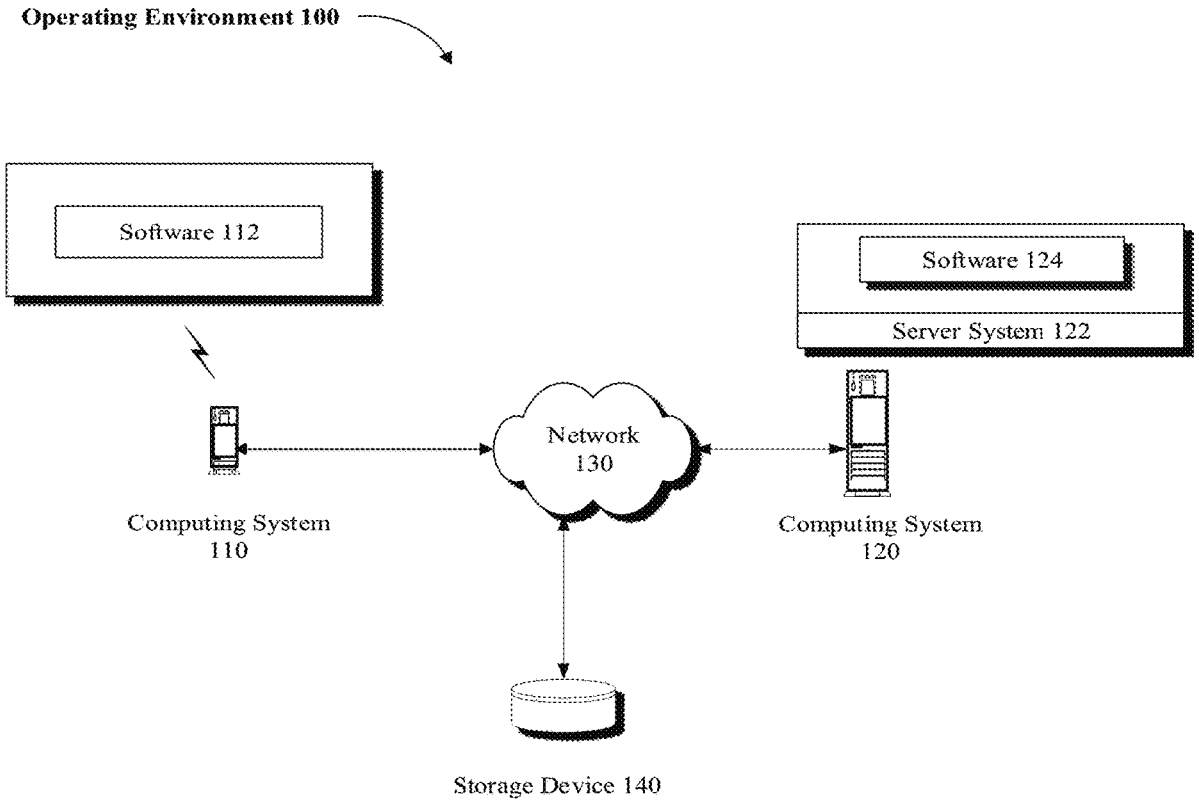
G06F 21/64	(2006.01)
G06F 21/62	(2006.01)
H04L 9/32	(2006.01)
G06F 21/60	(2006.01)

(52) **U.S. Cl.**

CPC ***G06F 21/64*** (2013.01); ***G06F 21/602*** (2013.01); ***H04L 9/3239*** (2013.01); ***G06F 21/6245*** (2013.01)

(57) **ABSTRACT**

Data validation systems and methods are provided. The method comprises generating a data set associated with a first credential information; submitting the data set to a data provider over a computing network to validate the first credential information, the data provider analyzing the data set to determine whether a match is found for the first credential information based on second credential information known to have been compromised; and in response to a match being found, determining that the first credential information has been potentially compromised.



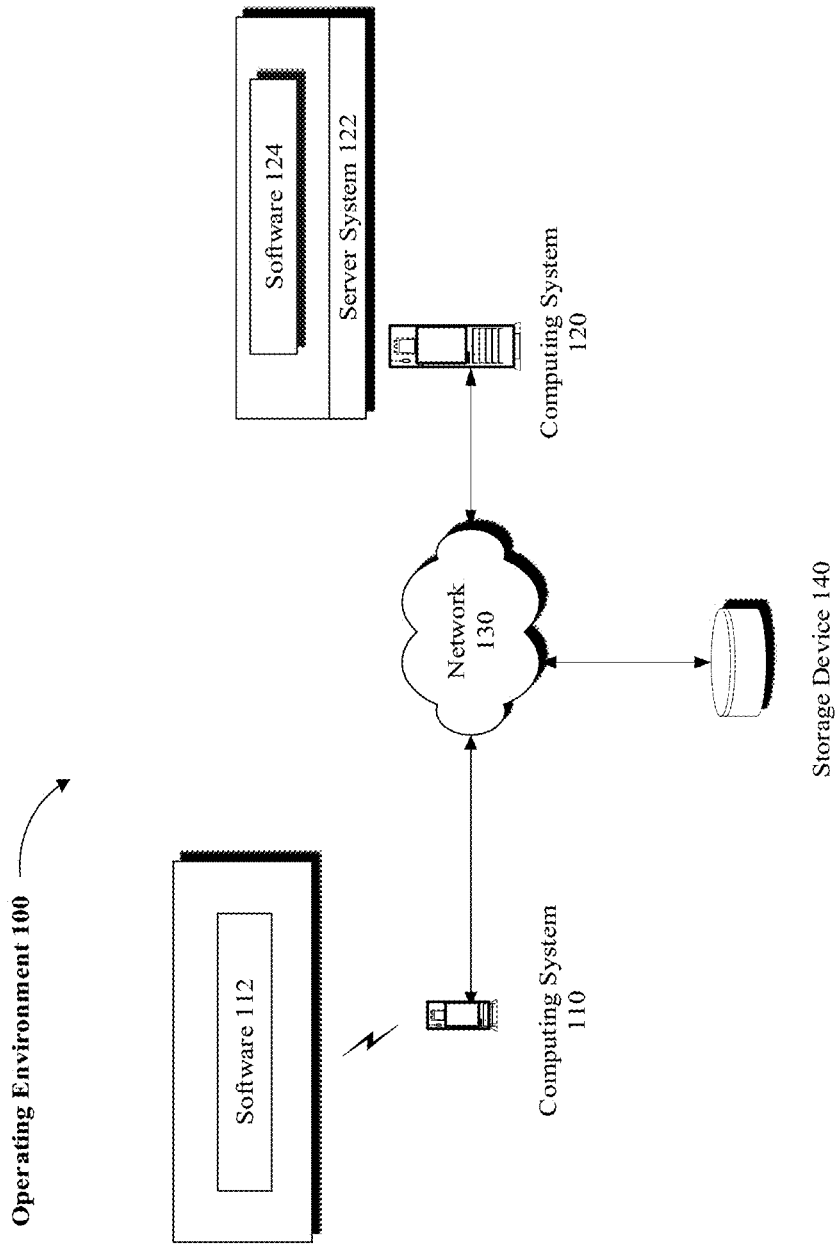

Operating Environment 100
Software 112
Computing System 110
Network 130
Storage Device 140
Computing System 120
Server System 122
Software 124

FIG. 1

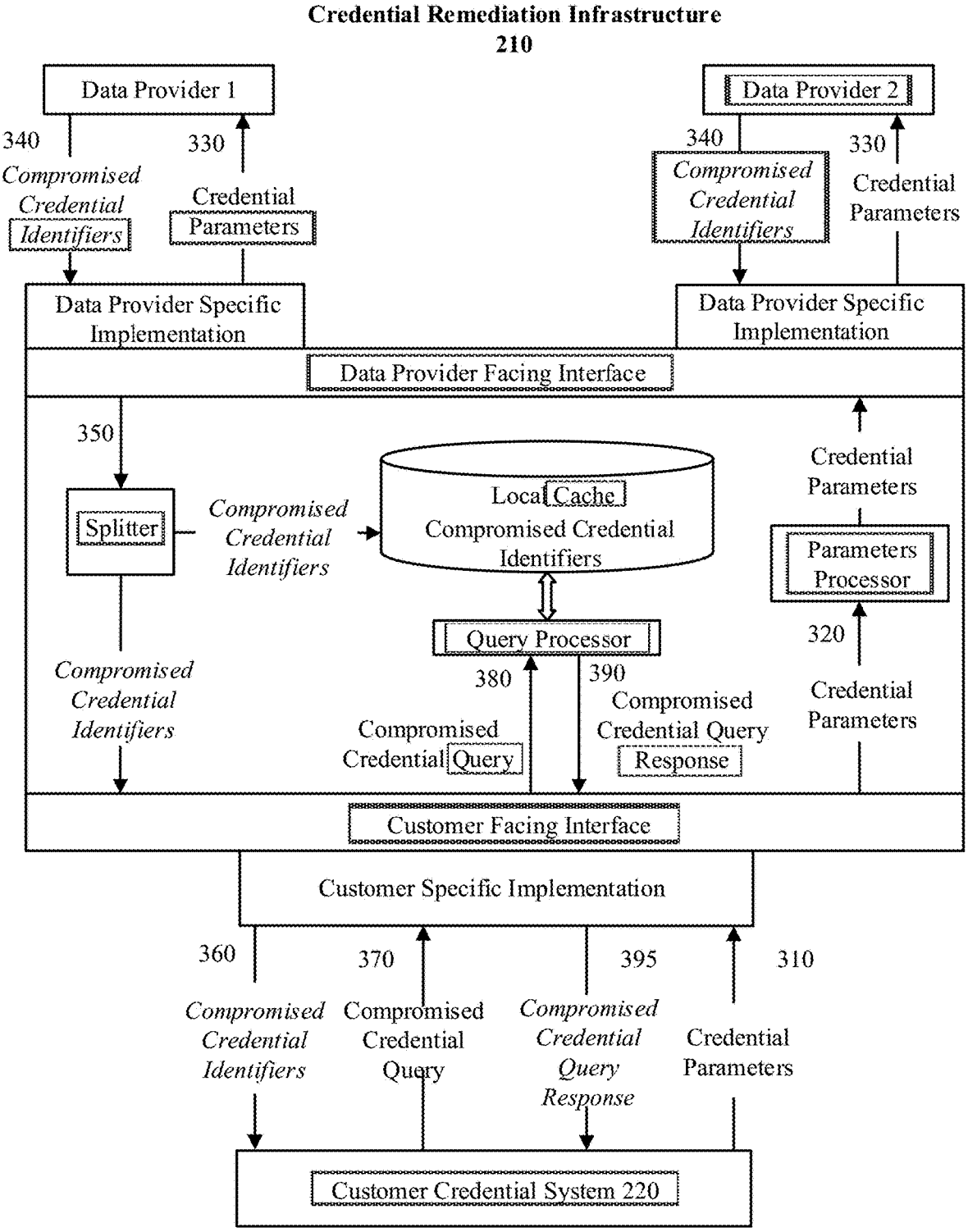

Credential Remediation Infrastructure
210
Data Provider 1
Data Provider 2
340
Compromised Credential Identifiers
330
Credential Parameters
340
Compromised Credential Identifiers
330
Credential Parameters
Data Provider Specific Implementation
Data Provider Specific Implementation
Data Provider Facing Interface
350
Splitter
Compromised Credential Identifiers
Local Cache
Compromised Credential Identifiers
Credential Parameters
Parameters Processor
320
Query Processor
380
390
Compromised Credential Query
Response
Compromised Credential Identifiers
Compromised Credential Query
Credential Parameters
Customer Facing Interface
Customer Specific Implementation
360
370
395
310
Compromised Credential Identifiers
Compromised Credential Query
Compromised Credential Query Response
Credential Parameters
Customer Credential System 220

FIG. 2

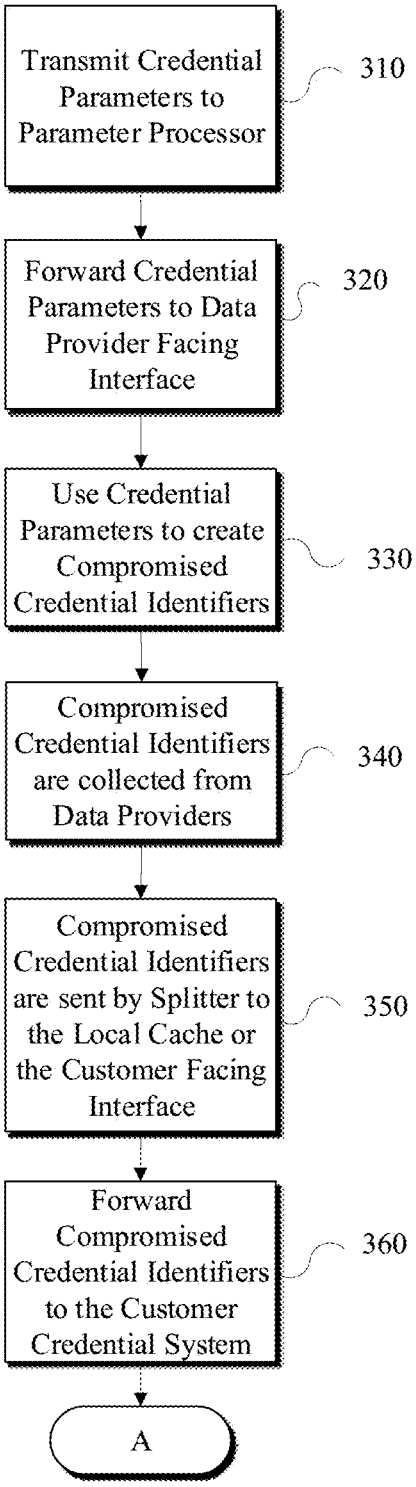

Transmit Credential Parameters to Parameter Processor
310
Forward Credential Parameters to Data Provider Facing Interface
320
Use Credential Parameters to create Compromised Credential Identifiers
330
Compromised Credential Identifiers are collected from Data Providers
340
Compromised Credential Identifiers are sent by Splitter to the Local Cache or the Customer Facing Interface
350
Forward Compromised Credential Identifiers to the Customer Credential System
360
A

FIG. 3A

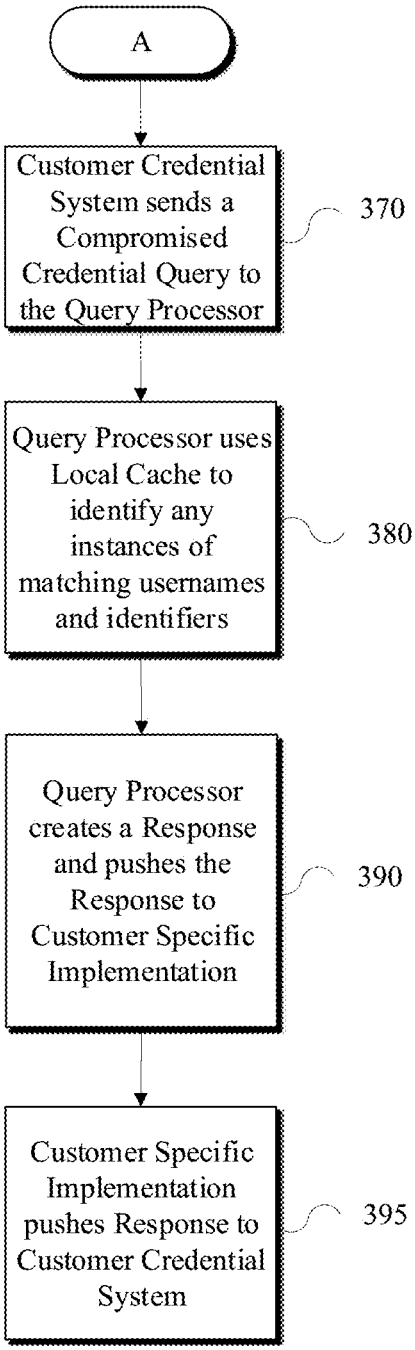

A
Customer Credential System sends a Compromised Credential Query to the Query Processor
370
Query Processor uses Local Cache to identify any instances of matching usernames and identifiers
380
Query Processor creates a Response and pushes the Response to Customer Specific Implementation
390
Customer Specific Implementation pushes Response to Customer Credential System
395

FIG. 3B

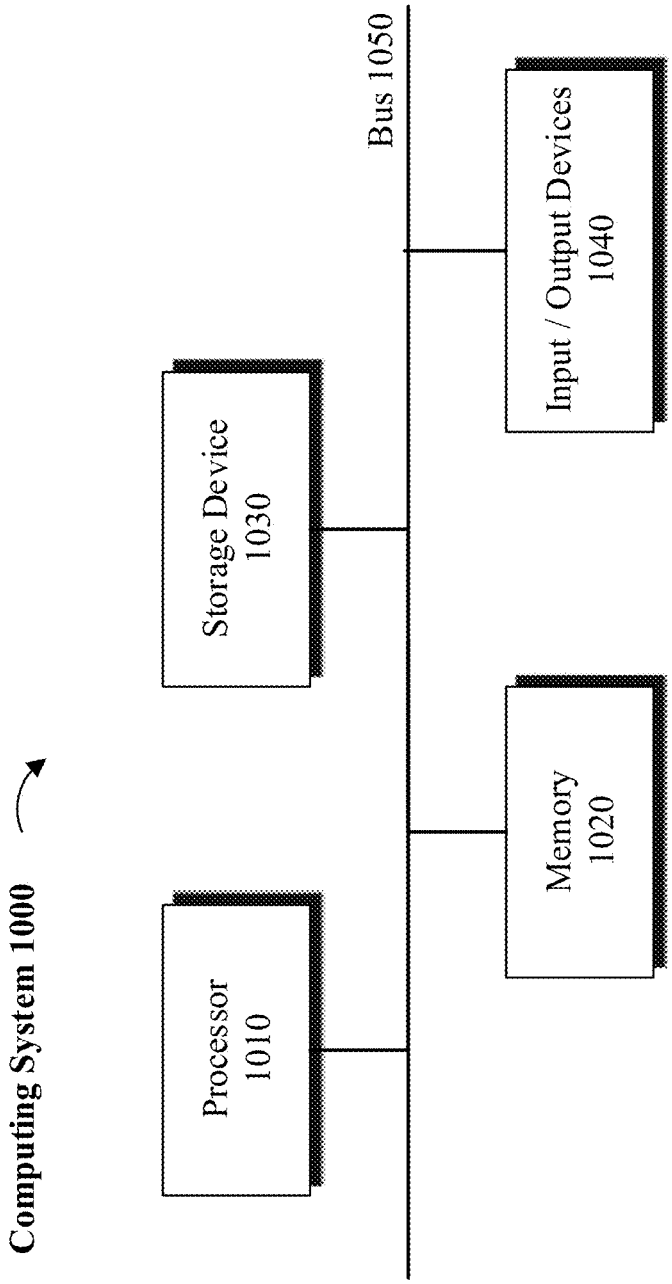

Computing System 1000
Processor 1010
Storage Device 1030
Memory 1020
Bus 1050
Input / Output Devices 1040

FIG. 4

DATA BREACH PREVENTION AND REMEDIATION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims priority to and the benefit of the earlier filing date of Provisional Application Ser. Nos. 62/870,332, and 62/897,197, filed on Jul. 3, 2019 and Sep. 6, 2019, respectively, the content of which is incorporated herein by reference in entirety.

TECHNICAL FIELD

[0002] The disclosed subject matter generally relates to data security and, more particularly, to managing credential data which may have been compromised.

BACKGROUND

[0003] Data security is of paramount importance especially when the data includes sensitive, personal or confidential information. A breach in data security often leads to theft of data where sensitive or critical information is copied, transmitted or viewed unlawfully or without authorization.

[0004] Theft of sensitive data that includes financial information (e.g., credit card or bank account numbers), personal information (e.g., medical data, social security number, driver license number, etc.), secrets (e.g., government data, intellectual property, trade secret, etc.) or a combination thereof can have sever ramifications for the owners of the data and institutions that are tasked with maintaining the data secure.

[0005] Unfortunately, data breaches can be detrimental to businesses, individuals, financial institutions and governmental entities. It is now well known that such incidents can lead to interference with business or political practices, financial loss, damage to reputation, identity theft and other serious threats. A variety of shortcomings can lead to a security breach, depending on the entities that have been compromised and their customers or constituents.

[0006] Such shortcomings include unknown design vulnerabilities, computing bugs, naïve user behavior, weak credential authentication settings and mechanisms and other factors that can render a data system susceptible to attack. Some of these factors may involve phishing sites that imitate a login page, malware that is non-active but has gathered usernames and passwords from infected machines, or usernames and passwords collected from data breaches.

SUMMARY

[0007] For purposes of summarizing, certain aspects, advantages, and novel features have been described herein. It is to be understood that not all such advantages may be achieved in accordance with any one particular embodiment. Thus, the disclosed subject matter may be embodied or carried out in a manner that achieves or optimizes one advantage or group of advantages without achieving all advantages as may be taught or suggested herein.

[0008] In accordance with one or more embodiments, a computer-implemented data validation method is provided. The method may comprise generating a data set associated with a first credential information and submitting the data set to a data provider over a computing network to validate the first credential information. The data provider may analyze the data set to determine whether a match is found for the first credential information based on second credential information known to have been compromised. In response to a match being found, it is determined that the first credential information has been potentially compromised.

[0009] A user associated with the first credential information may be requested to update the first credential information, in response to confirming that the first credential information has been compromised. The data set may include a cryptographic hash of at least a part of the first credential information. The data provider may search a series of hash values to find a match for the cryptographic hash. The series of hash values may include a hash of at least a part of the second credential information known to have been compromised.

[0010] In certain aspects, information associated with the match found may be stored in a cache locally available to a customer credential system of an institution responsible for safeguarding the first credential information. A splitter may be utilized to provide the information associated with the match found to one or more of the cache or the customer credential system of the institution responsible for safeguarding the first credential information. The match may be found by comparing a partial hash of the first credential information with a partial hash of the second credential information known to have been compromised.

[0011] In one or more implementations, in response to the match being found, a full hash value of the second credential information known to have been compromised is received. The full hash value of the second credential information may be compared with the full hash value of the first credential information to confirm the first credential information has been compromised. In accordance with some embodiments, a computer program product or system may be configured or programmed to perform the steps or processes disclosed in the above-noted computer-implemented methodology.

[0012] The details of one or more variations of the subject matter described herein are set forth in the accompanying drawings and the description below. Other features and advantages of the subject matter described herein will be apparent from the description and drawings, and from the claims. The disclosed subject matter is not, however, limited to any particular embodiment disclosed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] The accompanying drawings, which are incorporated in and constitute a part of this specification, show certain aspects of the subject matter disclosed herein and, together with the description, help explain some of the principles associated with the disclosed implementations as provided below.

[0014] FIG. **1** illustrates an example operating environment for credential validation, in accordance with one or more embodiments, in which the operations and functionalities disclosed herein may be implemented.

[0015] FIG. **2** is a block diagram of an exemplary system for identifying compromised credentials in accordance with one or more embodiments.

[0016] FIGS. **3**A and **3**B are flow diagrams of a method of determining whether certain credentials have been compromised, in accordance with an example implementation.

[0017] FIG. **4** is a block diagram of an example computing system that may be utilized to perform one or more computing operations or processes as consistent with one or more disclosed features.

[0018] The figures may not be to scale in absolute or comparative terms and are intended to be exemplary. The relative placement of features and elements may have been modified for the purpose of illustrative clarity. Where practical, the same or similar reference numbers denote the same or similar or equivalent structures, features, aspects, or elements, in accordance with one or more embodiments.

DETAILED DESCRIPTION OF EXAMPLE IMPLEMENTATIONS

[0019] In the following, numerous specific details are set forth to provide a thorough description of various embodiments. Certain embodiments may be practiced without these specific details or with some variations in detail. In some instances, certain features are described in less detail so as not to obscure other aspects. The level of detail associated with each of the elements or features should not be construed to qualify the novelty or importance of one feature over the others.

[0020] When a security breach compromises credential data (e.g., username, password) or any type of sensitive or secret data, it is important to efficiently and quickly identify the compromised data and take proactive steps to mitigate the breach. For example, if it is determined that a bank customer's username or password has been compromised, the customer can be notified. The customer may be also asked to change the compromised data. The present disclosure is directed to systems and methods that can efficiently identify compromised data and effectively remediate an existing security threat.

[0021] Referring to FIG. **1**, an example operating environment **100** is illustrated in which a computing system **110** may be used to interact with software **112** being executed on computing system **110**. The computing system **110** may be a general-purpose computer, a handheld mobile device (e.g., a smart phone), a tablet (e.g., an Apple iPad®), or other communication capable computing device. Software **112** may be a web browser, a dedicated app or other type of software application running either fully or partially on computing system **110** for the purpose of managing customer credential data and detecting potentials for security breach.

[0022] Computing system **110** may communicate over a network **130** to access data stored on storage device **140** or to access services provided by a computing system **120**. Depending on implementation, storage device **140** may be local to, remote to, or embedded in one or more of computing systems **110** or **120**. A server system **122** may be configured on computing system **120** to service one or more requests submitted by computing system **110** or software **112** (e.g., client systems) via network **130**. Network **130** may be implemented over a local or wide area network (e.g., the Internet).

[0023] Computing system **120** and server system **122** may be implemented over a centralized or distributed (e.g., cloud-based) computing environment as dedicated resources or may be configured as virtual machines that define shared processing or storage resources. Execution, implementation or instantiation of software **124**, or the related features and components (e.g., software objects), over server system **122** may also define a special purpose machine that provides remotely situated client systems, such as computing system **110** or software **112**, with access to a variety of data providers and services, as provided in further detail below.

[0024] In accordance with one or more implementations, the provided services by the special purpose machine (e.g., server system **122** or software **124**) may include providing an operating environment **100** which supports an interface between a customer system, implemented on computing system **110**, and one or more data providers implemented on one or more computing systems **120**, for example. Software **112** running on computing system **110** may be configured to provide validation information over network **130** to computing system **110** in a secure manner. Software **124** running on server system **122**, in relationship with software **112**, may be configured to determine if the provided sensitive data or credential information (e.g., username and/or password) are potentially compromised.

[0025] Referring to FIG. **2**, a credential remediation infrastructure **210** may be implemented as supported by operating environment **100** to help one or more institutions that store confidential, private or secret information maintain the integrity of such information by continually checking whether the credential information for any of their customers has been compromised. As shown, the credential remediation system **210** may include a customer credential system **220** that communicates with one or more data providers (e.g., data providers **1** and **2**). An interface platform, for example including an application programming interface (API), may be provided that has a customer facing interface or a data provider facing interface, or both, depending on implementation.

[0026] In certain embodiments, a processing and storage platform may be provided that includes at least one data splitter, a data caching mechanism, and one or more data processors (e.g., query processors, parameters processors, etc.). The computer interface may be configured to support a data provider implementation and a customer specific implementation. The customer specific implementation may be configured as a portion of the customer facing interface to communicate data according to a transmission protocol or specific transmission attributes of the customer credential system **220**. The data provider specific implementation, on the other hand, may be configured as a portion of the data provider facing interface to communicate with the one or more data providers.

[0027] In some implementations, the data provider **1** and the data provider **2** may have a proprietary or customized implementation as configurable to communicate with the data provider facing interface. Relying on the interface components noted above, the customer credential system **220** may communicate with the data providers to determine which customer or user credentials are possibly compromised. If compromised user credentials are identified, the credentials can be replaced by new credentials by requesting a user to change his username and password. To ensure secured transmission, in one example embodiment, customer credential system **220** may use a hash algorithm to provide hashes of credential information to one or more data providers.

[0028] In one example scenario, instead of a full hash, a partial hash of the credential information may be calculated. To further secure (e.g., encrypt) the transmission of credential information, a random text (e.g., "salt") may be also added to the partial hash. An encrypted credential information may be transmitted to the one or more data providers by way of a series of intermediary components in the implemented interface, as provided in further detail herein. A data

provider, upon receiving the encrypted credential information may apply the same hash algorithm to a series of credentials that are known to have been compromised.

[0029] Information about the hash algorithm and salt used to encrypt the credentials may be forwarded to the data provider, either along with the encrypted credentials or independently during a separate transmission. Without limitation, various procedures may be implemented or utilized by a provider to determine whether or not customer credentials have been compromised. The provider may have obtained the compromised credentials by performing a search on the dark web, for example.

[0030] Accordingly, a data provider may generate full or partial hashes of the compromised credentials and compare the generated hash values with the hash values transmitted from the customer credential system **220** to the data provider. A Bloom filter, for example, which can indicate that a match is possibly found (or definitely not found) may be utilized by the data provider to determine whether a credential submitted by the customer credential system **220** matches a known compromised credential. If a match is found (or is likely to be found), the data provider may notify the customer credential system that certain credentials associated with the hash have been compromised.

[0031] In embodiments where a partial hash is provided to the data provider, the data provider may return to the customer credential system **220** the full hash of the matched credential and additional information about the matched credential (e.g., the nature of the threat). Customer credential system **220**, upon receiving the information about the potential match, may compare the full hash of the credential information (e.g., the full hash of the username assigned to a customer) with the full hash of matched credentials provided by the provider. If there is a match, then customer credential system **220** may notify a customer or the corresponding institution (e.g., a bank) that the credential has been compromised.

[0032] In some embodiments, once it is determined that a certain credential (e.g., a username) is compromised, additional credential information (e.g., password data, pin, etc.) associated with the matched credential may be also analyzed to determine the extent of the breach or security threat. This analysis may be performed by the customer credential system **220**, the data provider or an independent entity. Furthermore, as noted earlier, additional information about the breach may be also provided by the data provider. Such information may include, for example, the source of the breach or any other attributes or characteristics related to the breach that may be useful for the purpose of mitigating or remediating the breach or associated security concern.

[0033] In accordance with one implementation, if it is determined that a customer's credentials are compromised, the customer may be contacted and asked to update or change his or her credentials (e.g., username, password, etc.). When the customer updates the credentials, the updated credential values may be submitted to the provider to ensure the updated credentials are not on the list of known compromised credentials. If so, the customer may be prompted not to use the new credential.

[0034] In accordance with another implementation, a cache mechanism may be implemented to store information about compromised credentials as the corresponding information is received from the one or more data providers. In certain scenarios, instead of forwarding credential-related data to the data providers for monitoring, the credentials (e.g., new or updated credential data) may be compared with the information in the cache. This implementation can improve credential validation efficiency and speed by avoiding the latency associated with having to transmit the credential information to data providers that are remotely situated. In an embodiment where the cache mechanism is implemented locally in relation to the customer credential system **220**, credential validation can advantageously take place in real-time or near real-time in an expedited manner, due to time savings and resource efficiencies associated with accessing a local cache.

[0035] Referring to FIGS. **2**, **3**A and **3**B, a more detailed example of credential validation and data breach remediation is provided, in accordance with one or more embodiments. It is noteworthy that the details provided are by way of example and certain steps, processes and features may be implemented or performed in different configurations or orders or using similar or completely different types of computing resources, which may be capable of performing the same functionalities or operations.

[0036] As provided in further detail herein, the customer credential system **220** may invoke a process to validate one or more credentials for one or more users or customers. The validation process may be invoked for a single customer, for example, when the customer initially sets up a username and password, or at a time when the customer updates the credentials. In alternative embodiments, a batch process may be executed at predetermined time intervals (e.g., daily or weekly) to invoke a validation process to validate the credential data periodically.

[0037] As shown in FIG. **3**A, the customer credential system **220** may thus collect and transmit credential-related parameters (e.g., hashed usernames or passwords, prefixed or postfixed salt, the hashing algorithm used to hash the username or password) to a parameter processor via the customer specific implementation of a customer facing interface (**310**). The parameter processor may forward the credential parameters to the data providers via the data provider facing interface (**320**). The data providers may use the credential parameters to identify possibly compromised credentials and create compromised credential identifiers to send back to the customer credential system **220** (**330**).

[0038] The credential identifiers are collected from data providers using a data provider specific fetching implementation to get converted and tagged (**340**). A data splitter may be configured to pull compromised credential identifiers via the data provider facing interface and store the compromised credential identifiers to a local cache and/or send the compromised credentials to the customer credential system **220** via the customer facing interface, for example (**350**). A customer specific implementation may capture, pull or receive new compromised credential identifiers from the splitter via the customer facing interface and pushes the information to the customer credential system **220** (**360**). Accordingly, the customer credential system **220** may be provided with an identification of one or more credentials that may have been compromised.

[0039] In some embodiments, to confirm that the partial hash values associated with the potentially compromised credentials are the same as that of a customer of the querying institution, the customer credential system **220** may request for additional information to be provided by the one or more data providers. For example, a complete hash value of the

comprised credential (e.g., username) and other associated credentials (e.g., password) may be calculated or requested. The additional information provided, in comparison to the information available to customer credential system **220**, may indicate or confirm that the potentially compromised credentials match. If so, then it is confirmed that the potentially compromised credentials are in fact compromised. Accordingly, the customer with compromised credentials may be requested to update the affected credential (e.g., update the old username and password) with new credentials.

[0040] Referring to FIG. **3**B, in certain embodiments, the newly updated credentials (e.g., username and password) may be validated by way of the same or similar processes provided in FIG. **3**A. In one implementation, for the purpose of efficiency, instead of forwarding the new credentials hashes all the way to the data providers, which may be remotely connected to the customer credential system **220**, the credentials are instead submitted by way of a compromised credential query to a query processor to determine if the new credentials can be matched against already compromised credentials stored in a cache (**370**). The customer credential system **220** may thus create a compromised credential query that is forwarded to the query processor via the customer specific implementation and the customer facing interface.

[0041] The query processor may search the local cache to identify any instances that match the queried credential (e.g., match the customer's username and password identifiers) (**380**). The query processor creates a compromised credential query response and sets a flag (e.g., a binary value) depending on whether a match is found or not (e.g., flag=1 indicating a match, flag=0 indicating no match), and forwards a compromised credential query response to the customer specific implementation via the customer facing interface system (**390**). The customer specific implementation then provides or pushes the result back to the customer credential system **220** (**395**). In this manner, the customer may be notified that his credentials have been compromised.

[0042] Referring to FIG. **4**, a block diagram illustrating a computing system **1000** consistent with one or more embodiments is provided. The computing system **1000** may be used to implement or support one or more platforms, infrastructures or computing devices or computing components that may be utilized, in example embodiments, to instantiate, implement, execute or embody the methodologies disclosed herein in a computing environment using, for example, one or more processors or controllers, as provided below.

[0043] As shown in FIG. **4**, the computing system **1000** can include a processor **1010**, a memory **1020**, a storage device **1030**, and input/output devices **1040**. The processor **1010**, the memory **1020**, the storage device **1030**, and the input/output devices **1040** can be interconnected via a system bus **1050**. The processor **1010** is capable of processing instructions for execution within the computing system **1000**. Such executed instructions can implement one or more components of, for example, a cloud platform. In some implementations of the current subject matter, the processor **1010** can be a single-threaded processor. Alternately, the processor **1010** can be a multi-threaded processor. The processor **1010** is capable of processing instructions stored in the memory **1020** and/or on the storage device **1030** to display graphical information for a user interface provided via the input/output device **1040**.

[0044] The memory **1020** is a computer readable medium such as volatile or non-volatile that stores information within the computing system **1000**. The memory **1020** can store data structures representing configuration object databases, for example. The storage device **1030** is capable of providing persistent storage for the computing system **1000**. The storage device **1030** can be a floppy disk device, a hard disk device, an optical disk device, or a tape device, or other suitable persistent storage means. The input/output device **1040** provides input/output operations for the computing system **1000**. In some implementations of the current subject matter, the input/output device **1040** includes a keyboard and/or pointing device. In various implementations, the input/output device **1040** includes a display unit for displaying graphical user interfaces.

[0045] According to some implementations of the current subject matter, the input/output device **1040** can provide input/output operations for a network device. For example, the input/output device **1040** can include Ethernet ports or other networking ports to communicate with one or more wired and/or wireless networks (e.g., a local area network (LAN), a wide area network (WAN), the Internet).

[0046] In some implementations of the current subject matter, the computing system **1000** can be used to execute various interactive computer software applications that can be used for organization, analysis and/or storage of data in various (e.g., tabular) format (e.g., Microsoft Excel®, and/or any other type of software). Alternatively, the computing system **1000** can be used to execute any type of software applications. These applications can be used to perform various functionalities, e.g., planning functionalities (e.g., generating, managing, editing of spreadsheet documents, word processing documents, and/or any other objects, etc.), computing functionalities, communications functionalities, etc. The applications can include various add-in functionalities or can be standalone computing products and/or functionalities. Upon activation within the applications, the functionalities can be used to generate the user interface provided via the input/output device **1040**. The user interface can be generated and presented to a user by the computing system **1000** (e.g., on a computer screen monitor, etc.).

[0047] One or more aspects or features of the subject matter disclosed or claimed herein may be realized in digital electronic circuitry, integrated circuitry, specially designed application specific integrated circuits (ASICs), field programmable gate arrays (FPGAs) computer hardware, firmware, software, and/or combinations thereof. These various aspects or features may include implementation in one or more computer programs that may be executable and/or interpretable on a programmable system including at least one programmable processor, which may be special or general purpose, coupled to receive data and instructions from, and to transmit data and instructions to, a storage system, at least one input device, and at least one output device. The programmable system or computing system may include clients and servers. A client and server may be remote from each other and may interact through a communication network. The relationship of client and server arises by virtue of computer programs running on the respective computers and having a client-server relationship to each other.

[0048] These computer programs, which may also be referred to as programs, software, software applications, applications, components, or code, may include machine instructions for a programmable controller, processor, microprocessor or other computing or computerized architecture, and may be implemented in a high-level procedural language, an object-oriented programming language, a functional programming language, a logical programming language, and/or in assembly/machine language. As used herein, the term "machine-readable medium" refers to any computer program product, apparatus and/or device, such as for example magnetic discs, optical disks, memory, and Programmable Logic Devices (PLDs), used to provide machine instructions and/or data to a programmable processor, including a machine-readable medium that receives machine instructions as a machine-readable signal. The term "machine-readable signal" refers to any signal used to provide machine instructions and/or data to a programmable processor. The machine-readable medium may store such machine instructions non-transitorily, such as for example as would a non-transient solid-state memory or a magnetic hard drive or any equivalent storage medium. The machine-readable medium may alternatively or additionally store such machine instructions in a transient manner, such as for example as would a processor cache or other random access memory associated with one or more physical processor cores.

[0049] To provide for interaction with a user, one or more aspects or features of the subject matter described herein may be implemented on a computer having a display device, such as for example a cathode ray tube (CRT) or a liquid crystal display (LCD) or a light emitting diode (LED) monitor for displaying information to the user and a keyboard and a pointing device, such as for example a mouse or a trackball, by which the user may provide input to the computer. Other kinds of devices may be used to provide for interaction with a user as well. For example, feedback provided to the user may be any form of sensory feedback, such as for example visual feedback, auditory feedback, or tactile feedback; and input from the user may be received in any form, including acoustic, speech, or tactile input. Other possible input devices include touch screens or other touch-sensitive devices such as single or multi-point resistive or capacitive trackpads, voice recognition hardware and software, optical scanners, optical pointers, digital image capture devices and associated interpretation software, and the like.

Terminology

[0050] When a feature or element is herein referred to as being "on" another feature or element, it may be directly on the other feature or element or intervening features and/or elements may also be present. In contrast, when a feature or element is referred to as being "directly on" another feature or element, there may be no intervening features or elements present. It will also be understood that, when a feature or element is referred to as being "connected", "attached" or "coupled" to another feature or element, it may be directly connected, attached or coupled to the other feature or element or intervening features or elements may be present. In contrast, when a feature or element is referred to as being "directly connected", "directly attached" or "directly coupled" to another feature or element, there may be no intervening features or elements present.

[0051] Although described or shown with respect to one embodiment, the features and elements so described or shown may apply to other embodiments. It will also be appreciated by those of skill in the art that references to a structure or feature that is disposed "adjacent" another feature may have portions that overlap or underlie the adjacent feature.

[0052] Terminology used herein is for the purpose of describing particular embodiments and implementations only and is not intended to be limiting. For example, as used herein, the singular forms "a", "an" and "the" may be intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms "comprises" and/or "comprising," when used in this specification, specify the presence of stated features, steps, operations, processes, functions, elements, and/or components, but do not preclude the presence or addition of one or more other features, steps, operations, processes, functions, elements, components, and/or groups thereof. As used herein, the term "and/or" includes any and all combinations of one or more of the associated listed items and may be abbreviated as "/".

[0053] In the descriptions above and in the claims, phrases such as "at least one of" or "one or more of" may occur followed by a conjunctive list of elements or features. The term "and/or" may also occur in a list of two or more elements or features. Unless otherwise implicitly or explicitly contradicted by the context in which it used, such a phrase is intended to mean any of the listed elements or features individually or any of the recited elements or features in combination with any of the other recited elements or features. For example, the phrases "at least one of A and B;" "one or more of A and B;" and "A and/or B" are each intended to mean "A alone, B alone, or A and B together." A similar interpretation is also intended for lists including three or more items. For example, the phrases "at least one of A, B, and C;" "one or more of A, B, and C;" and "A, B, and/or C" are each intended to mean "A alone, B alone, C alone, A and B together, A and C together, B and C together, or A and B and C together." Use of the term "based on," above and in the claims is intended to mean, "based at least in part on," such that an unrecited feature or element is also permissible.

[0054] Spatially relative terms, such as "forward", "rearward", "under", "below", "lower", "over", "upper" and the like, may be used herein for ease of description to describe one element or feature's relationship to another element(s) or feature(s) as illustrated in the figures. It will be understood that the spatially relative terms are intended to encompass different orientations of the device in use or operation in addition to the orientation depicted in the figures. For example, if a device in the figures is inverted, elements described as "under" or "beneath" other elements or features would then be oriented "over" the other elements or features due to the inverted state. Thus, the term "under" may encompass both an orientation of over and under, depending on the point of reference or orientation. The device may be otherwise oriented (rotated 90 degrees or at other orientations) and the spatially relative descriptors used herein interpreted accordingly. Similarly, the terms "upwardly", "downwardly", "vertical", "horizontal" and the like may be used herein for the purpose of explanation only unless specifically indicated otherwise.

[0055] Although the terms "first" and "second" may be used herein to describe various features/elements (including steps or processes), these features/elements should not be limited by these terms as an indication of the order of the features/elements or whether one is primary or more important than the other, unless the context indicates otherwise. These terms may be used to distinguish one feature/element from another feature/element. Thus, a first feature/element discussed could be termed a second feature/element, and similarly, a second feature/element discussed below could be termed a first feature/element without departing from the teachings provided herein.

[0056] As used herein in the specification and claims, including as used in the examples and unless otherwise expressly specified, all numbers may be read as if prefaced by the word "about" or "approximately," even if the term does not expressly appear. The phrase "about" or "approximately" may be used when describing magnitude and/or position to indicate that the value and/or position described is within a reasonable expected range of values and/or positions. For example, a numeric value may have a value that is +/−0.1% of the stated value (or range of values), +/−1% of the stated value (or range of values), +/−2% of the stated value (or range of values), +/−5% of the stated value (or range of values), +/−10% of the stated value (or range of values), etc. Any numerical values given herein should also be understood to include about or approximately that value, unless the context indicates otherwise.

[0057] For example, if the value "10" is disclosed, then "about 10" is also disclosed. Any numerical range recited herein is intended to include all sub-ranges subsumed therein. It is also understood that when a value is disclosed that "less than or equal to" the value, "greater than or equal to the value" and possible ranges between values are also disclosed, as appropriately understood by the skilled artisan. For example, if the value "X" is disclosed the "less than or equal to X" as well as "greater than or equal to X" (e.g., where X is a numerical value) is also disclosed. It is also understood that the throughout the application, data is provided in a number of different formats, and that this data, may represent endpoints or starting points, and ranges for any combination of the data points. For example, if a particular data point "10" and a particular data point "15" may be disclosed, it is understood that greater than, greater than or equal to, less than, less than or equal to, and equal to 10 and 15 may be considered disclosed as well as between 10 and 15. It is also understood that each unit between two particular units may be also disclosed. For example, if **10** and **15** may be disclosed, then 11, 12, 13, and 14 may be also disclosed.

[0058] Although various illustrative embodiments have been disclosed, any of a number of changes may be made to various embodiments without departing from the teachings herein. For example, the order in which various described method steps are performed may be changed or reconfigured in different or alternative embodiments, and in other embodiments, one or more method steps may be skipped altogether. Optional or desirable features of various device and system embodiments may be included in some embodiments and not in others. Therefore, the foregoing description is provided primarily for the purpose of example and should not be interpreted to limit the scope of the claims and specific embodiments or particular details or features disclosed.

[0059] One or more aspects or features of the subject matter described herein can be realized in digital electronic circuitry, integrated circuitry, specially designed application specific integrated circuits (ASICs), field programmable gate arrays (FPGAs) computer hardware, firmware, software, and/or combinations thereof. These various aspects or features can include implementation in one or more computer programs that are executable and/or interpretable on a programmable system including at least one programmable processor, which can be special or general purpose, coupled to receive data and instructions from, and to transmit data and instructions to, a storage system, at least one input device, and at least one output device. The programmable system or computing system may include clients and servers. A client and server are generally remote from each other and typically interact through a communication network. The relationship of client and server arises by virtue of computer programs running on the respective computers and having a client-server relationship to each other.

[0060] These computer programs, which can also be referred to programs, software, software applications, applications, components, or code, include machine instructions for a programmable processor, and can be implemented in a high-level procedural language, an object-oriented programming language, a functional programming language, a logical programming language, and/or in assembly/machine language. As used herein, the term "machine-readable medium" refers to any computer program product, apparatus and/or device, such as for example magnetic discs, optical disks, memory, and Programmable Logic Devices (PLDs), used to provide machine instructions and/or data to a programmable processor, including a machine-readable medium that receives machine instructions as a machine-readable signal.

[0061] The term "machine-readable signal" refers to any signal used to provide machine instructions and/or data to a programmable processor. The machine-readable medium can store such machine instructions non-transitorily, such as for example as would a non-transient solid-state memory or a magnetic hard drive or any equivalent storage medium. The machine-readable medium can alternatively or additionally store such machine instructions in a transient manner, such as for example, as would a processor cache or other random access memory associated with one or more physical processor cores.

[0062] The examples and illustrations included herein show, by way of illustration and not of limitation, specific embodiments in which the disclosed subject matter may be practiced. As mentioned, other embodiments may be utilized and derived therefrom, such that structural and logical substitutions and changes may be made without departing from the scope of this disclosure. Such embodiments of the disclosed subject matter may be referred to herein individually or collectively by the term "invention" merely for convenience and without intending to voluntarily limit the scope of this application to any single invention or inventive concept, if more than one is, in fact, disclosed. Thus, although specific embodiments have been illustrated and described herein, any arrangement calculated to achieve an intended, practical or disclosed purpose, whether explicitly stated or implied, may be substituted for the specific embodiments shown. This disclosure is intended to cover any and all adaptations or variations of various embodiments. Combinations of the above embodiments, and other

embodiments not specifically described herein, will be apparent to those of skill in the art upon reviewing the above description.

[0063] The disclosed subject matter has been provided here with reference to one or more features or embodiments. Those skilled in the art will recognize and appreciate that, despite of the detailed nature of the example embodiments provided here, changes and modifications may be applied to said embodiments without limiting or departing from the generally intended scope. These and various other adaptations and combinations of the embodiments provided here are within the scope of the disclosed subject matter as defined by the disclosed elements and features and their full set of equivalents.

[0064] A portion of the disclosure of this patent document may contain material, which is subject to copyright protection. The owner has no objection to facsimile reproduction by any one of the patent documents or the patent disclosure, as it appears in the Patent and Trademark Office patent files or records, but reserves all copyrights whatsoever. Certain marks referenced herein may be common law or registered trademarks of the applicant, the assignee or third parties affiliated or unaffiliated with the applicant or the assignee. Use of these marks is for providing an enabling disclosure by way of example and shall not be construed to exclusively limit the scope of the disclosed subject matter to material associated with such marks.

What is claimed is:

1. A data validation method comprising:

generating a data set associated with a first credential information;

submitting the data set to a data provider over a computing network to validate the first credential information, the data provider analyzing the data set to determine whether a match is found for the first credential information based on second credential information known to have been compromised; and

in response to a match being found, determining that the first credential information has been potentially compromised.

2. The method of claim **1** further comprising requesting a user associated with the first credential information to update the first credential information, in response to confirming that the first credential information has been compromised.

3. The method of claim **1**, wherein the data set comprises a cryptographic hash of at least a part of the first credential information.

4. The method of claim **3**, wherein the data provider searches a series of hash values to find a match for the cryptographic hash.

5. The method of claim **4**, wherein the series of hash values comprise a hash of at least a part of the second credential information known to have been compromised.

6. The method of claim **1** further comprising storing information associated with the match found in a cache locally available to a customer credential system of an institution responsible for safeguarding the first credential information.

7. The method of claim **6**, wherein a splitter is utilized to provide the information associated with the match found to one or more of the cache or the customer credential system of the institution responsible for safeguarding the first credential information.

8. The method of claim **2**, wherein the match is found by comparing a partial hash of the first credential information with a partial hash of the second credential information known to have been compromised.

9. The method of claim **8**, wherein in response to the match being found, a full hash value of the second credential information known to have been compromised is received.

10. The method of claim **9** further comprising:

comparing the full hash value of the second credential information with the full hash value of the first credential information to confirm the first credential information has been compromised.

11. A system comprising:

at least one programmable processor; and

a non-transitory machine-readable medium storing instructions that, when executed by the at least one programmable processor, cause the at least one programmable processor to perform operations comprising:

generating a data set associated with a first credential information;

submitting the data set to a data provider over a computing network to validate the first credential information, the data provider analyzing the data set to determine whether a match is found for the first credential information based on second credential information known to have been compromised; and

in response to a match being found, determining that the first credential information has been potentially compromised.

12. The system of claim **11** further comprising requesting a user associated with the first credential information to update the first credential information, in response to confirming that the first credential information has been compromised.

13. The system of claim **11**, wherein the data set comprises a cryptographic hash of at least a part of the first credential information.

14. The system of claim **13**, wherein the data provider searches a series of hash values to find a match for the cryptographic hash.

15. The system of claim **14**, wherein the series of hash values comprise a hash of at least a part of the second credential information known to have been compromised.

16. The system of claim **11** further comprising storing information associated with the match found in a cache locally available to a customer credential system of an institution responsible for safeguarding the first credential information.

17. The system of claim **16**, wherein a splitter is utilized to provide the information associated with the match found to one or more of the cache or the customer credential system of the institution responsible for safeguarding the first credential information.

18. A computer program product comprising a non-transitory machine-readable medium storing instructions that, when executed by at least one programmable processor, cause the at least one programmable processor to perform operations comprising:

generating a data set associated with a first credential information;

submitting the data set to a data provider over a computing network to validate the first credential information, the data provider analyzing the data set to determine

whether a match is found for the first credential information based on second credential information known to have been compromised; and

in response to a match being found, determining that the first credential information has been potentially compromised.

19. The computer program product of claim **18**, wherein the match is found by comparing a partial hash of the first credential information with a partial hash of the second credential information known to have been compromised.

20. The computer program product of claim **19**, further comprising:

in response to the match being found, receiving a full hash value of the second credential information known to have been compromised; and

comparing the full hash value of the second credential information with the full hash value of the first credential information to confirm the first credential information has been compromised.

* * * * *