



(51) International Patent Classification:
G06F 21/56 (2013.01)

(21) International Application Number:
PCT/US2017/067450

(22) International Filing Date:
20 December 2017 (20.12.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/449,367 23 January 2017 (23.01.2017) US
15/491,525 19 April 2017 (19.04.2017) US

(71) Applicant: **MICROSOFT TECHNOLOGY LICENSING, LLC** [US/US]; One Microsoft Way, Redmond, Washington 98052-6399 (US).

(72) Inventors: **TAMIR, Gal**; Microsoft Technology Licensing, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). **IWANIR, Elad**; Microsoft Technology

Licensing, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). **BEN-MENACHEM, Avi**; Microsoft Technology Licensing, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US).

(74) Agent: **MINHAS, Sandip, S.** et al.; Microsoft Technology Licensing, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(54) Title: RANSOMWARE RESILIENT DATABASES

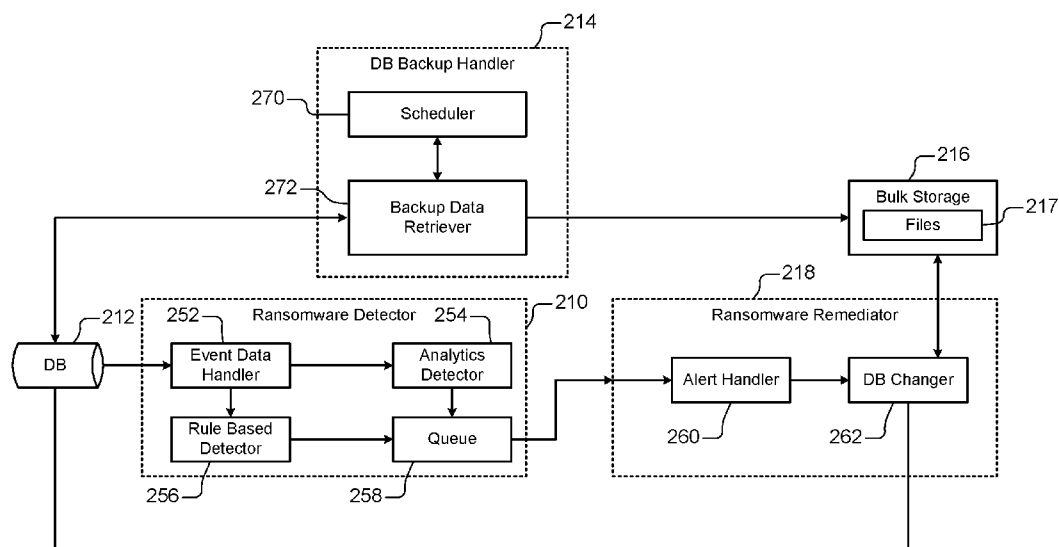


FIG. 2B

(57) Abstract: A system for protecting a database against a ransomware attack includes a database backup handler configured to selectively output database backup data associated with a database to a storage device. A ransomware detector is configured to monitor changes to the database and to detect data changes to the database resulting from a ransomware attack. A ransomware remediator communicates with the ransomware detector and the database backup handler and is configured to restore data in the database to a point prior to the ransomware attack based upon the backup data in the storage device.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

- *with international search report (Art. 21(3))*

RANSOMWARE RESILIENT DATABASES

FIELD

5 [0001] The present disclosure relates to computer systems and methods for detecting and remediating database data adversely affected by ransomware.

BACKGROUND

10 [0002] The background description provided herein is for the purpose of generally presenting the context of the disclosure. Work of the presently named inventors, to the extent the work is described in this background section, as well as aspects of the description that may not otherwise qualify as prior art at the time of filing, are neither expressly nor impliedly admitted as prior art against the present disclosure.

[0003] Ransomware is malware that is used to deny access to computer files or other data on a computer. A ransom payment is requested in return for allowing access to the computer files or data. For example, ransomware may be used to encrypt the computer files or data.
15 A key for decrypting the files or data is sent after the ransom payment is received. Ransomware may be installed on computers via Trojan horses, which are malware files that are disguised as legitimate files or programs. If the ransom payment is paid but the ransomware is not removed from the computer, the ransomware may repeat the process of encrypting files or data and demanding a ransom payment. For example, an email with an
20 attachment including a malicious macro may be sent to a potential ransomware victim. When the user opens the attachment, the macro installs the ransomware on the computer.

SUMMARY

[0004] A system for protecting a database against a ransomware attack includes a database backup handler configured to selectively output database backup data associated with a
25 database to a storage device. A ransomware detector is configured to monitor changes to the database and to detect data changes to the database resulting from a ransomware attack. A ransomware remediator communicates with the ransomware detector and the database backup handler and is configured to restore data in the database to a point prior to the ransomware attack based upon the backup data in the storage device.

30 [0005] In other features, the ransomware detector includes an event data handler in communication with the database that is configured to receive database events from the database. A rule-based detector is configured to receive an output of the event data handler and to use a plurality of rules to detect the ransomware attack and generate a ransomware alert.

[0006] In other features, the ransomware detector further includes an analytics detector configured to receive the output of the event handler, to detect the ransomware attack using at least one of deep learning analysis detection and machine learning and to generate a ransomware alert.

5 [0007] In other features, the ransomware remediator includes an alert handler configured to receive the ransomware alert from the ransomware detector. A database data changer is configured to change at least one of selected rows and selected tables in the database based upon the database backup data in response to the ransomware alert.

10 [0008] In other features, the database backup handler is configured to schedule snapshots of the database in response to at least one of an event or a predetermined backup period and to store the snapshots in the storage device. The database backup handler includes a backup data retriever configured to retrieve changed row data and to store the changed row data in the storage device. The database backup handler is configured to retrieve changes to a database log and to store the changes in the storage device.

15 [0009] A system for protecting a database against a ransomware attack includes a processor and memory. A ransomware detection and remediation application, stored in the memory and executed by the processor, is configured to: retrieve and store database backup data associated with a database to a storage device; monitor the database to detect data changes to the database resulting from a ransomware attack; and in response to the
20 ransomware attack, restore data in the database to a point prior to the ransomware attack based upon the backup data in the storage device.

[0010] In other features, the ransomware detection and remediation application is further configured to receive database events from the database, and apply a plurality of rules to the database events to detect the ransomware attack. The ransomware detection and
25 remediation application is further configured to detect the ransomware attack based on the database events using at least one of deep learning analysis detection and machine learning.

[0011] In other features, the ransomware detection and remediation application is further configured to receive ransomware alerts and change at least one of a row and a table in the database based upon the database backup data in response to the ransomware alerts.

30 [0012] In other features, the ransomware detection and remediation application is further configured to schedule snapshots of the database in response to at least one of an event or a predetermined backup period and to store the snapshots in the storage device. The ransomware detection and remediation application is further configured to retrieve changed row data and to store the changed row data in the storage device.

[0013] In other features, the ransomware detection and remediation application is further configured to retrieve changes to a database log and to store the changes in the storage device.

5 [0014] A method for protecting a database against a ransomware attack includes selectively outputting database backup data associated with a database to a storage device; monitoring changes to the database; detecting data changes to the database resulting from a ransomware attack; and in response to detecting the ransomware attack, restoring data in the database to a point prior to the ransomware attack based upon the backup data in the storage device.

10 [0015] In other features, the method includes receiving database events from the database and monitoring the database events using a plurality of rules to detect the ransomware attack and to generate a ransomware alert.

[0016] In other features, the method includes detecting the ransomware attack and generating the ransomware alert based on the database events using at least one of deep
15 learning analysis detection and machine learning. The database backup data includes row changes made to the database and the method further comprises, in response to the ransomware alert, changing data in the database based upon the database backup data.

[0017] In other features, the database backup data includes snapshots of the database and the method further comprises restoring the database using the snapshots in response to the
20 ransomware alerts. The database backup data includes a database log and the method further comprises restoring the database using the database log in response to the ransomware alerts.

[0018] Further areas of applicability of the present disclosure will become apparent from the detailed description, the claims and the drawings. The detailed description and specific
25 examples are intended for purposes of illustration only and are not intended to limit the scope of the disclosure.

BRIEF DESCRIPTION OF DRAWINGS

[0019] FIG. 1 is a functional block diagram of an example of a computer network according to the present disclosure;

30 [0020] FIG. 2A is a functional block diagram of an example of a ransomware detector and remediator according to the present disclosure;

[0021] FIG. 2B is a functional block diagram of another example of a ransomware detector and remediator according to the present disclosure;

[0022] FIG. 3 is a functional block diagram of another example of a ransomware detector

and remediator according to the present disclosure;

[0023] FIGs. 4A-4G are functional block diagrams illustrating additional examples of ransomware detectors according to the present disclosure;

5 [0024] FIG. 5 is a flowchart illustrating ransomware detection and remediation using database snapshots according to the present disclosure;

[0025] FIG. 6 is a flowchart illustrating ransomware detection and remediation using database log files according to the present disclosure; and

[0026] FIG. 7 is a flowchart illustrating ransomware detection and remediation using a database row changes according to the present disclosure.

10 [0027] In the drawings, reference numbers may be reused to identify similar and/or identical elements.

DESCRIPTION

[0028] A ransomware detection and remediation system and method according to the present disclosure includes a ransomware detector that detects database data (such as data
15 entries, rows or tables) that is altered by ransomware. Once the ransomware detector detects database that is affected by ransomware, a ransomware remediator returns the database to a state prior to a point when the ransomware affected the database data.

[0029] In some examples, a database backup handler periodically stores snapshots of database data such as data entries, rows and/or tables in the database. The ransomware
20 remediator uses a snapshot taken prior to a time when the ransomware altered the database data. The snapshot is used to restore the ransomware altered data with backup data in the snapshot.

[0030] In other examples, the database application stores a log of changes to the database. The ransomware remediator uses the database log file (by reversing the changes) to return
25 the database to a state prior to a time when the ransomware altered the database data.

[0031] In other examples, the database backup handler stores a file including chronological list of row changes that are made to the database. The ransomware remediator reverses the row changes to return the state of the database to a point that is prior to a time
30 when the ransomware altered the database data. As a result, the database owner will have the option to remediate the altered database data without the need to pay a ransom.

[0032] As can be appreciated, the ransomware detector and the ransomware remediator can be implemented in a network in a variety of ways. In some examples, the database, the ransomware detector and the ransomware remediator are stored and executed, respectively, by the same computing device. In other examples, the database, the ransomware detector

and the ransomware remediator are executed by two or more computing devices. In some examples, the database, the ransomware detector and the ransomware remediator are all implemented in a cloud network using one or more servers, virtual machines or containers. Alternately, the database, the ransomware detector and the ransomware remediator can be implemented in an enterprise network using one or more servers, virtual machines or containers.

[0033] Referring now to FIG. 1, one or more hacker computing devices 120-1, 120-2 ... , and 120-N (collectively hacker computing devices or hackers 120) (where N is an integer greater than zero) in a network 100 are connected by a distributed communication system (DCS) 110 such as the Internet to one or more other computers. The hackers 120 attempt to install ransomware that may adversely affect data stored on databases (DB) of computing devices such as stand-alone computing devices or computing devices such as servers, virtual machines or containers associated with an on premises enterprise network or a cloud services provider.

[0034] For example, the network 100 may further include a computing device 130, a cloud services provider 140, and/or an enterprise network 150. The computing device 130 may be connected to one or more local or remote databases 132. The cloud services provider 140 may manage or is connected to one or more databases 142. The enterprise network 150 may manage or is connected to one or more local or remote databases 152. All of the databases are potential targets for ransomware attacks by the hackers 120.

[0035] Referring now to FIG. 2A, a system 200 for detecting and remediating ransomware is shown to include a ransomware detector 210. The ransomware detector 210 detects data altered by ransomware in a database 212. In some examples, the ransomware detector 210 includes a software module or controller.

[0036] A database backup handler 214 selectively backs up portions of the database 212. In some examples, the database backup handler 214 includes a software module or controller. In some examples, the database backup handler 214 uses a snapshot feature of the database to store files 217 in bulk storage 216 such as a hard disk drive. When the ransomware detector 210 detects database data altered by the ransomware, the snapshots are used to return the database to a state prior to the ransomware attack. Alternately, the database backup handler 214 stores a chronological database log file of changes made to the database in the bulk storage 216.

[0037] In other examples, the database backup handler 214 stores row changes in chronological order in the bulk storage 216. In response to ransomware being detected by

the ransomware detector 210, a ransomware remediator 218 uses the files 217 to restore the database to a time prior to the point where the ransomware altered the database data (for example by reversing the database changes). In some examples, the ransomware remediator includes a software module or controller. As can be appreciated, the locations of the ransomware detector 210, the database 212, the database backup handler 214, the bulk storage 216 and the ransomware remediator 218 will vary depending upon the architecture of the network.

[0038] Referring now to FIG. 2B, the ransomware detector 210 may include an event data handler 252 that receives event data from the database 212 when events such as row updates or other database changes occur. In some examples, the event data handler 252 includes an event hub. The event data handler 252 outputs the event data to an analytics detector 254 and/or a rule-based detector 256. In some examples, the analytics detector 254 uses deep analysis detection, machine learning or other techniques described below to detect ransomware attacks on the data in the database 212. The rule-based detector 256 uses a set of rules to analyze the event data.

[0039] If a ransomware attack is detected, the analytics detector 254 and/or the rule-based detector 256 outputs a ransomware alert to a queue 258. The queue 258 outputs the ransomware alerts to an alert handler 260 associated with the ransomware remediator 218. The alert handler 260 coordinates with a database changer 262 to use the files 217 stored in the bulk storage 216 to restore the data by restoring the database back to a point before the ransomware attack occurred. The database backup handler 214 includes a backup scheduler 270 and a backup data retriever 272. The backup scheduler 270 may schedule backups on a periodic basis or an event basis. For example, the backup scheduler 270 may schedule backups in response to an event relating to unusual or atypical amount of changes being made to the database within a predetermined period. The backup data retriever 272 retrieves row changes, database log file changes or snapshots and stores them in the files 217.

[0040] In FIG. 3A, a computing device 290 such as a stand-alone computing device, or a server, virtual machine or container in an enterprise network or a cloud network is shown. The computing device 290 includes one or more processors 300 and memory 302. A host operating system 308 executes one or more user applications 312. In some examples, the computing device 290 may include an application 316 with a database interface to allow the application to send information to or retrieve information from a local or remote database or to set configuration parameters specifying backup intervals or notification preferences (or no notification and immediate remediation) in the event of a ransomware attack. In this

example, some of the data in the database (stored remotely in the cloud or on a remote server) may be altered by ransomware and may need to be detected and corrected by the ransomware detector and the ransomware remediator described below. The computing device 290 further includes a wired or wireless interface 334 and bulk storage 338 such as a hard disk drive.

[0041] The computing device 290 communicates with a network 340 such as an enterprise network or cloud network (for example via the DCS, a firewall 342 and a router 344 shown in FIG. 3). A computing device 350 associated with the network 340 includes one or more processors 352 and memory 362. In some examples, the computing device 350 is a server, virtual machine or container in an enterprise network or a cloud network. The memory 362 includes a host operating system 368 and an anti-ransomware application 380. The anti-ransomware application includes a ransomware detector 384, a database backup handler 386 and a ransomware remediator 388, which can be implemented using software sub-modules. While the ransomware detector 384, the database backup handler 386 and the ransomware remediator 388 are shown on a single server, virtual machine or container, separate servers, virtual machines or containers can be used. The computing device 350 further includes a wired or wireless interface 394 and bulk storage 398. In some examples, the database backup data can be stored as files 400 in the bulk storage 398.

[0042] The computing device 350 communicates via the router 344 with a server 410 storing a database 412. The computing device 250 also communicates with one or more additional servers 420 and 430. In some examples, the servers 410 and/or 420 may be used to store the backup files.

[0043] Referring now to FIGs. 4A-4G, various other examples of the ransomware detector 210 are shown. In FIG. 4A, a hypersurface generator 524 receives training data including sample data and a label identifying whether the data is ransomware or not. As will be described further below, the hypersurface generator 524 generates a hypersurface model 528 that is used in a hypersurface detector 540 in FIG. 4B.

[0044] In other examples shown in FIG. 4C, the ransomware detector 210 includes a rules filter 550. The rules filter 550 includes one or more rules that are used to filter database data or database event data and to identify ransomware based upon changes in frequency, timing, file types, user profiles, packet data such as source, destination, etc., file extensions, and/or information, etc. For example, the rules filter 550 may look for changes to honeypot database data and/or changes to file extensions that are indicators of a ransomware attack, although other rules may be used.

[0045] In FIG. 4D, the ransomware detector 210 includes a neural network 560 that is trained using known data. Once trained, the neural network 560 is used to identify ransomware.

[0046] In FIG. 4E, the ransomware detector 210 includes an entropy detector 570. The entropy detector 570 measures the relative randomness of a data entry, row, column or table in the database and assigns a randomness level on a predetermined scale. For example, a table including unencrypted list of addresses and names would be relatively non-random whereas an encrypted table would be completely random. After a ransomware attack, the randomness of the table may increase as a result of encryption applied by the attacker.

[0047] In FIG. 4F, a honeypot change detector 570 detects changes to honeypot database data such as data entries, rows, or tables. As can be appreciated, while specific examples are shown, other types of ransomware detectors are contemplated. In addition, two or more of the ransomware detection techniques described above and below can be used in combination.

[0048] In FIG. 4G, the ransomware detector 210 includes a ransomware note detector 574 that detects a ransomware note in the changes to the data. In some examples, the ransom note may be sent by the hacker to the infected computing device. The note can be a, an e-mail, a text file, an image file, a short messaging service (SMS), or any other form of communication. In some examples, the note is not sent to the infected device but rather is sent to another computing device such as one associated with the owner of the infected computing device. In some examples, the ransomware note detector 574 looks in the data changes for keyword terms such as requests for ransom, requests for bitcoins or other currency, and/or other terms that are typically used in ransom notes. In some examples, the ransomware note detector 574 uses image recognition, optical character recognition or cognitive analysis to detect the ransom note.

[0049] In some examples, the ransomware detector 210 may use data analytics to help distinguish between legitimate changes and malicious changes. The ransomware detector 210 may use various machine-learning techniques, such as a support vector machine, a Bayesian network, learning regression, a neural network, big data analytics, an evolutionary algorithm, and so on to detect malicious changes. The ransomware detector 210 may collect various features such as the number and frequency of changes, the location of changes, the patterns of the changes (extensions, headers, entropy changes, types), user information (e.g., organization or location), and so on. After collecting the features, the ransomware detector 210 may learn a classifier on a per-user basis, a per-organization basis, or on the basis of

some other division of users. For example, the ransomware detector 210 may use various clustering techniques to generate clusters of users based on various attributes of the users (e.g., business user or personal user and frequency of computer usage).

[0050] In some examples, the ransomware detector 210 may employ a support vector machine to train classifiers for each user or each division of users. To train a classifier, the training data includes samples of malicious data changes and samples of legitimate data changes where each sample comprises a feature vector of features and a label indicating whether the sample represents a malicious or legitimate change. A support vector machine operates by finding a hypersurface in the space of possible inputs. The hypersurface attempts to split the positive examples (e.g., ransomware) from the negative samples (e.g., not ransomware) by maximizing the distance between the nearest of the positive and negative samples and the hypersurface.

[0051] A support vector machine simultaneously minimizes an empirical classification error and maximizes a geometric margin. This allows for correct classification of data that is similar to but not identical to the training data. Various techniques can be used to train a support vector machine. One technique uses a sequential minimal optimization algorithm that breaks the large quadratic programming problem down into a series of small quadratic programming problems that can be solved analytically. (See Platt, J., "Sequential Minimal Optimization: A Fast Algorithm for Training Support Vector Mechanisms," 1998, <http://research.microsoft.com/pubs/69644/tr-98-14.pdf>, which is Incorporated herein by reference in its entirety.)

[0052] A support vector machine is provided training data represented by (x_i, y_i) where x_i represents a feature vector and y_i represents a label for sample i . A support vector machine may be used to optimize the following:

$$\min_{w, b, T} \frac{1}{2} w^T w + C \sum_{i=1}^l \xi_i$$

$$\text{such that } y_i (w^T \phi(x_i) + b) \geq 1 - \xi_i, \xi_i \geq 0$$

where vector w is perpendicular to the separating hypersurface, the offset variable b is used to increase the margin, the slack variable ξ_i represents the degree of misclassification of x_i , the function ϕ maps the vector x_i into a higher dimensional space, and C represents a penalty parameter of the error term. A support vector machine supports linear classification but can be adapted to perform nonlinear classification by modifying the kernel function, as represented by the following:

$$(K(x_i, x_j) = \phi(x_i)^T(x_j))$$

[0053] In some examples, the ransomware detector uses a radial basis function (“RBF”) kernel, as represented by the following:

$$K(x_i, x_j) = \exp(-\gamma \|x_i - x_j\|^2), \gamma > 0$$

5 [0054] The ransomware detector may also use a polynomial Gaussian RBF or a sigmoid kernel. The ransomware detector may use cross-validation and grid search to find optimal values for parameters γ and C . (See Hsu, C. W., Chang, C. C., and Lin, C. J., “A Practical Guide to Support Vector Classification,” Technical Report, Dept. of Computer Science and Information Engineering, National Taiwan University, Taipei, 2003, which is hereby
10 Incorporated by reference in its entirety.)

[0055] In some examples, the ransomware detector inserts honeypot database data such as data entries, row entries or tables into the database being monitored. The honeypot database data is stored in the database solely for the purpose of detecting a malicious change to the honeypot database data. The user of the device may be unaware of the presence of the
15 honeypot database data and would have no reason to change the content of the honeypot database data. For example, if the ransomware detector detects any change to the honeypot database data (or even a deletion of the honeypot database data), the ransomware detector may assume that the change was caused by ransomware and take remedial actions such as those described above. In some examples, the honeypot database data includes content that
20 is similar to customer database data to help obscure detection by ransomware.

[0056] In some examples, the ransomware detector monitors changes to the honeypot database data, rather than behavior of an executing process (e.g., ransomware). The ransomware detector may factor in the entropy (e.g., Shannon entropy) of the honeypot database data because data affected by ransomware may have a high entropy output (e.g.,
25 as a result of encryption). The ransomware detector may also factor in variance in the honeypot database data because data affected by ransomware may have content that is completely dissimilar from its prior version. For example, the ransomware detector may employ a similarity-preserving hash function (e.g., Nilsimsa hash, TLSH, and Ssdeep) to detect changes. The ransomware detector may factor in the number of modifications to a
30 honeypot database data because data affected by ransomware may be heavily modified. For example, the ransomware detector may monitor “magic marker” type modifications, extension changes, and/or content deletions.

[0057] Referring now to FIG. 5, a method 800 for detecting ransomware in a database and

remediating the database to remove the effects of the ransomware is shown. At 804, the method determines whether a database backup period is up or an event occurs. For example, the backup period may be performed at a regular interval that can be shortened when unusual activity occurs in the database. When 804 is true, the database stores a snapshot of the database at 808. At 812, the method determines whether ransomware is detected. If not, the method returns to 804. When 812 is true, the method sends a message to a DB administrator to notify and request approval for remediation of the database at 816. If remediation is approved at 820, the method initiates the database remediation using snapshots that are earlier than the ransomware changes and overrides, deletes or renders obsolete later snapshots.

[0058] In some examples, the method proceeds from 812 when ransomware is detected to 828 without notifying and requesting approval for remediation as indicated at alternate path 829. If 820 is false, the method optionally returns at 831. Alternately, the method can continue from 820 to 824 where the method determines whether the database administrator or other user wants to further investigate the ransomware alert using a database management tool prior to initiating remediation. If 824 is true, the method continues at 828 and the database management tool is launched. After the investigation, the database administrator is allowed another opportunity to approve or disapprove of the database remediation at 830. If 830 is true, the method continues at 828. If 830 is false, the method returns.

[0059] Referring now to FIG. 6, a method 850 stores a log of database transactions at 854. When ransomware is detected, similar steps are performed. However, remediation is performed by reversing entries in the database log until the ransomware is removed at 858.

[0060] Referring now to FIG. 7, a method 880 stores a row changes at 854. When ransomware is detected, similar steps are performed. However, remediation is performed by reversing row changes until the ransomware is removed at 888.

[0061] The foregoing description is merely illustrative in nature and is in no way intended to limit the disclosure, its application, or uses. The broad teachings of the disclosure can be implemented in a variety of forms. Therefore, while this disclosure includes particular examples, the true scope of the disclosure should not be so limited since other modifications will become apparent upon a study of the drawings, the specification, and the following claims. It should be understood that one or more steps within a method may be executed in different order (or concurrently) without altering the principles of the present disclosure. Further, although each of the examples is described above as having certain features, any one or more of those features described with respect to any example of the disclosure can

be implemented in and/or combined with features of any of the other examples, even if that combination is not explicitly described. In other words, the described examples are not mutually exclusive, and permutations of one or more examples with one another remain within the scope of this disclosure.

5 **[0062]** Spatial and functional relationships between elements (for example, between modules, circuit elements, semiconductor layers, etc.) are described using various terms, including “connected,” “engaged,” “coupled,” “adjacent,” “next to,” “on top of,” “above,” “below,” and “disposed.” Unless explicitly described as being “direct,” when a relationship between first and second elements is described in the above disclosure, that relationship can
10 be a direct relationship where no other intervening elements are present between the first and second elements, but can also be an indirect relationship where one or more intervening elements are present (either spatially or functionally) between the first and second elements. As used herein, the phrase at least one of A, B, and C should be construed to mean a logical (A OR B OR C), using a non-exclusive logical OR, and should not be construed to mean
15 “at least one of A, at least one of B, and at least one of C.”

[0063] In the figures, the direction of an arrow, as indicated by the arrowhead, generally demonstrates the flow of information (such as data or instructions) that is of interest to the illustration. For example, when element A and element B exchange a variety of information but information transmitted from element A to element B is relevant to the illustration, the
20 arrow may point from element A to element B. This unidirectional arrow does not imply that no other information is transmitted from element B to element A. Further, for information sent from element A to element B, element B may send requests for, or receipt acknowledgements of, the information to element A.

[0064] In this application, including the definitions below, the term “module” or the term
25 “controller” may be replaced with the term “circuit.” The term “module” may refer to, be part of, or include: an Application Specific Integrated Circuit (ASIC); a digital, analog, or mixed analog/digital discrete circuit; a digital, analog, or mixed analog/digital integrated circuit; a combinational logic circuit; a field programmable gate array (FPGA); a processor circuit (shared, dedicated, or group) that executes code; a memory circuit (shared, dedicated,
30 or group) that stores code executed by the processor circuit; other suitable hardware components that provide the described functionality; or a combination of some or all of the above, such as in a system-on-chip.

[0065] The module may include one or more interface circuits. In some examples, the interface circuits may include wired or wireless interfaces that are connected to a local area

network (LAN), the Internet, a wide area network (WAN), or combinations thereof. The functionality of any given module of the present disclosure may be distributed among multiple modules that are connected via interface circuits. For example, multiple modules may allow load balancing. In a further example, a server (also known as remote, or cloud) module may accomplish some functionality on behalf of a client module.

[0066] The term code, as used above, may include software, firmware, and/or microcode, and may refer to programs, routines, functions, classes, data structures, and/or objects. The term shared processor circuit encompasses a single processor circuit that executes some or all code from multiple modules. The term group processor circuit encompasses a processor circuit that, in combination with additional processor circuits, executes some or all code from one or more modules. References to multiple processor circuits encompass multiple processor circuits on discrete dies, multiple processor circuits on a single die, multiple cores of a single processor circuit, multiple threads of a single processor circuit, or a combination of the above. The term shared memory circuit encompasses a single memory circuit that stores some or all code from multiple modules. The term group memory circuit encompasses a memory circuit that, in combination with additional memories, stores some or all code from one or more modules.

[0067] The term memory circuit is a subset of the term computer-readable medium. The term computer-readable medium, as used herein, does not encompass transitory electrical or electromagnetic signals propagating through a medium (such as on a carrier wave); the term computer-readable medium may therefore be considered tangible and non-transitory. Non-limiting examples of a non-transitory, tangible computer-readable medium are nonvolatile memory circuits (such as a flash memory circuit, an erasable programmable read-only memory circuit, or a mask read-only memory circuit), volatile memory circuits (such as a static random access memory circuit or a dynamic random access memory circuit), magnetic storage media (such as an analog or digital magnetic tape or a hard disk drive), and optical storage media (such as a CD, a DVD, or a Blu-ray Disc).

[0068] In this application, apparatus elements described as having particular attributes or performing particular operations are specifically configured to have those particular attributes and perform those particular operations. Specifically, a description of an element to perform an action means that the element is configured to perform the action. The configuration of an element may include programming of the element, such as by encoding instructions on a non-transitory, tangible computer-readable medium associated with the element.

[0069] The apparatuses and methods described in this application may be partially or fully implemented by a special purpose computer created by configuring a general purpose computer to execute one or more particular functions embodied in computer programs. The functional blocks, flowchart components, and other elements described above serve as software specifications, which can be translated into the computer programs by the routine work of a skilled technician or programmer.

[0070] The computer programs include processor-executable instructions that are stored on at least one non-transitory, tangible computer-readable medium. The computer programs may also include or rely on stored data. The computer programs may encompass a basic input/output system (BIOS) that interacts with hardware of the special purpose computer, device drivers that interact with particular devices of the special purpose computer, one or more operating systems, user applications, background services, background applications, etc.

[0071] The computer programs may include: (i) descriptive text to be parsed, such as JavaScript Object Notation (JSON), hypertext markup language (HTML) or extensible markup language (XML), (ii) assembly code, (iii) object code generated from source code by a compiler, (iv) source code for execution by an interpreter, (v) source code for compilation and execution by a just-in-time compiler, etc. As examples only, source code may be written using syntax from languages including C, C++, C#, Objective C, Haskell, Go, SQL, R, Lisp, Java®, Fortran, Perl, Pascal, Curl, OCaml, Javascript®, HTML5, Ada, ASP (active server pages), PHP, Scala, Eiffel, Smalltalk, Erlang, Ruby, Flash®, Visual Basic®, Lua, and Python®.

[0072] None of the elements recited in the claims are intended to be a means-plus-function element within the meaning of 35 U.S.C. §112(f) unless an element is expressly recited using the phrase “means for,” or in the case of a method claim using the phrases “operation for” or “step for.”

CLAIMS

1. A system for protecting a database against a ransomware attack, comprising:
 - a database backup handler configured to selectively output database backup data associated with a database to a storage device;
 - a ransomware detector configured to monitor changes to the database and to detect data changes to the database resulting from a ransomware attack; and
 - a ransomware remediator that communicates with the ransomware detector and the database backup handler and that is configured to restore data in the database to a point prior to the ransomware attack based upon the backup data in the storage device.
2. The system of claim 1, wherein the ransomware detector includes:
 - an event data handler in communication with the database that is configured to receive database events from the database; and
 - a rule-based detector configured to receive an output of the event data handler and to use a plurality of rules to detect the ransomware attack and generate a ransomware alert.
3. The system of claim 2, wherein the ransomware detector further includes an analytics detector configured to receive the output of the event data handler, to detect the ransomware attack using at least one of deep learning analysis detection and machine learning and to generate a ransomware alert.
4. The system of claim 1, wherein the ransomware remediator includes:
 - an alert handler configured to receive the ransomware alert from the ransomware detector; and
 - a database data changer configured to change at least one of selected rows and selected tables in the database based upon the database backup data in response to the ransomware alert.
5. The system of claim 1, wherein the database backup handler is configured to schedule snapshots of the database in response to at least one of an event or a predetermined backup period and to store the snapshots in the storage device.
6. The system of claim 1, wherein the database backup handler includes a backup data retriever configured to retrieve changed row data and to store the changed row data in the storage device.
7. The system of claim 1, wherein the database backup handler is configured to retrieve changes to a database log and to store the changes in the storage device.
8. A system for protecting a database against a ransomware attack, comprising:
 - a processor;

memory;

a ransomware detection and remediation application that is stored in the memory and executed by the processor and that is configured to:

retrieve and store database backup data associated with a database to a storage device;

monitor the database to detect data changes to the database resulting from a ransomware attack; and

in response to the ransomware attack, restore data in the database to a point prior to the ransomware attack based upon the backup data in the storage device.

9. The system of claim 8, wherein the ransomware detection and remediation application is further configured to:

receive database events from the database; and

apply a plurality of rules to the database events to detect the ransomware attack.

10. The system of claim 9, wherein the ransomware detection and remediation application is further configured to detect the ransomware attack based on the database events using at least one of deep learning analysis detection and machine learning.

11. The system of claim 8, wherein the ransomware detection and remediation application is further configured to:

receive ransomware alerts; and

change at least one of a row and a table in the database based upon the database backup data in response to the ransomware alerts.

12. The system of claim 8, wherein the ransomware detection and remediation application is further configured to schedule snapshots of the database in response to at least one of an event or a predetermined backup period and to store the snapshots in the storage device.

13. The system of claim 8, wherein the ransomware detection and remediation application is further configured to retrieve changed row data and to store the changed row data in the storage device.

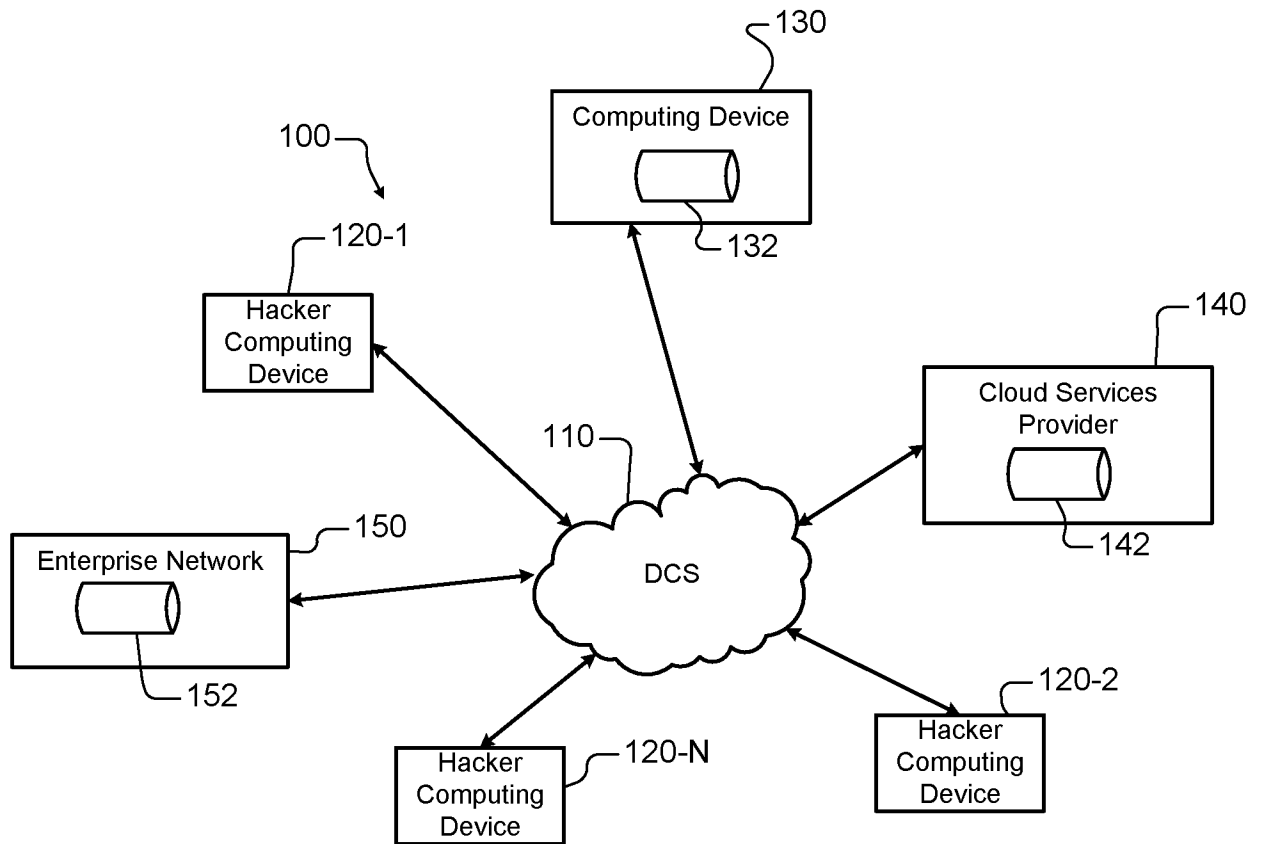
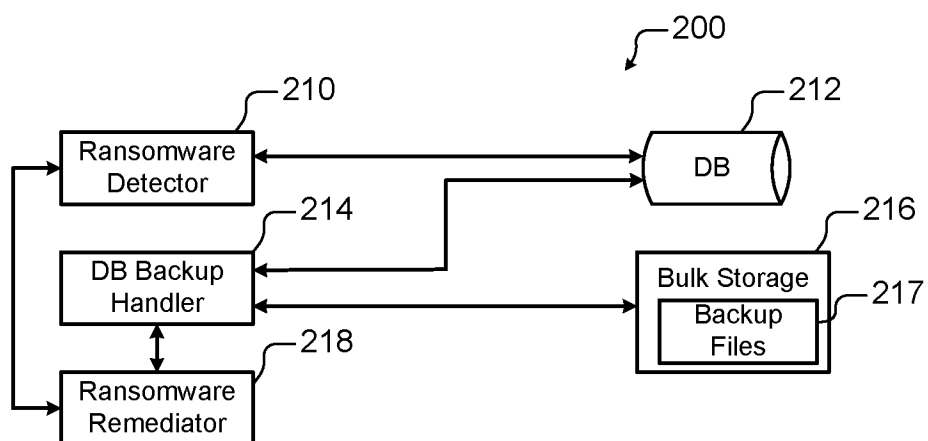
14. The system of claim 8, wherein the ransomware detection and remediation application is further configured to retrieve changes to a database log and to store the changes in the storage device.

15. A method for protecting a database against a ransomware attack, comprising:

selectively outputting database backup data associated with a database to a storage device;

monitoring changes to the database;
detecting data changes to the database resulting from a ransomware attack; and
in response to detecting the ransomware attack, restoring data in the database to a
point prior to the ransomware attack based upon the backup data in the storage device.

1/8

**FIG. 1****FIG. 2A**

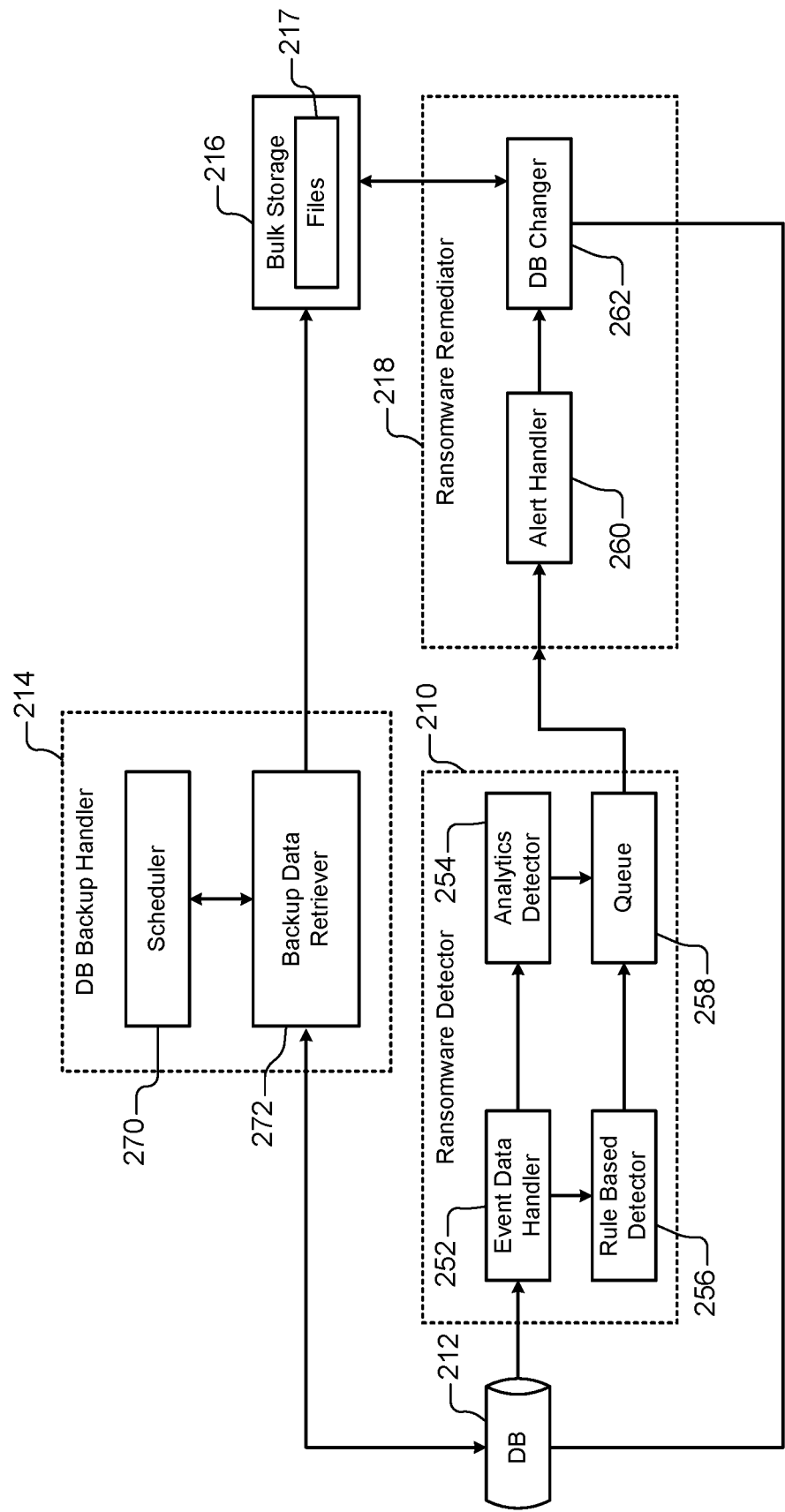
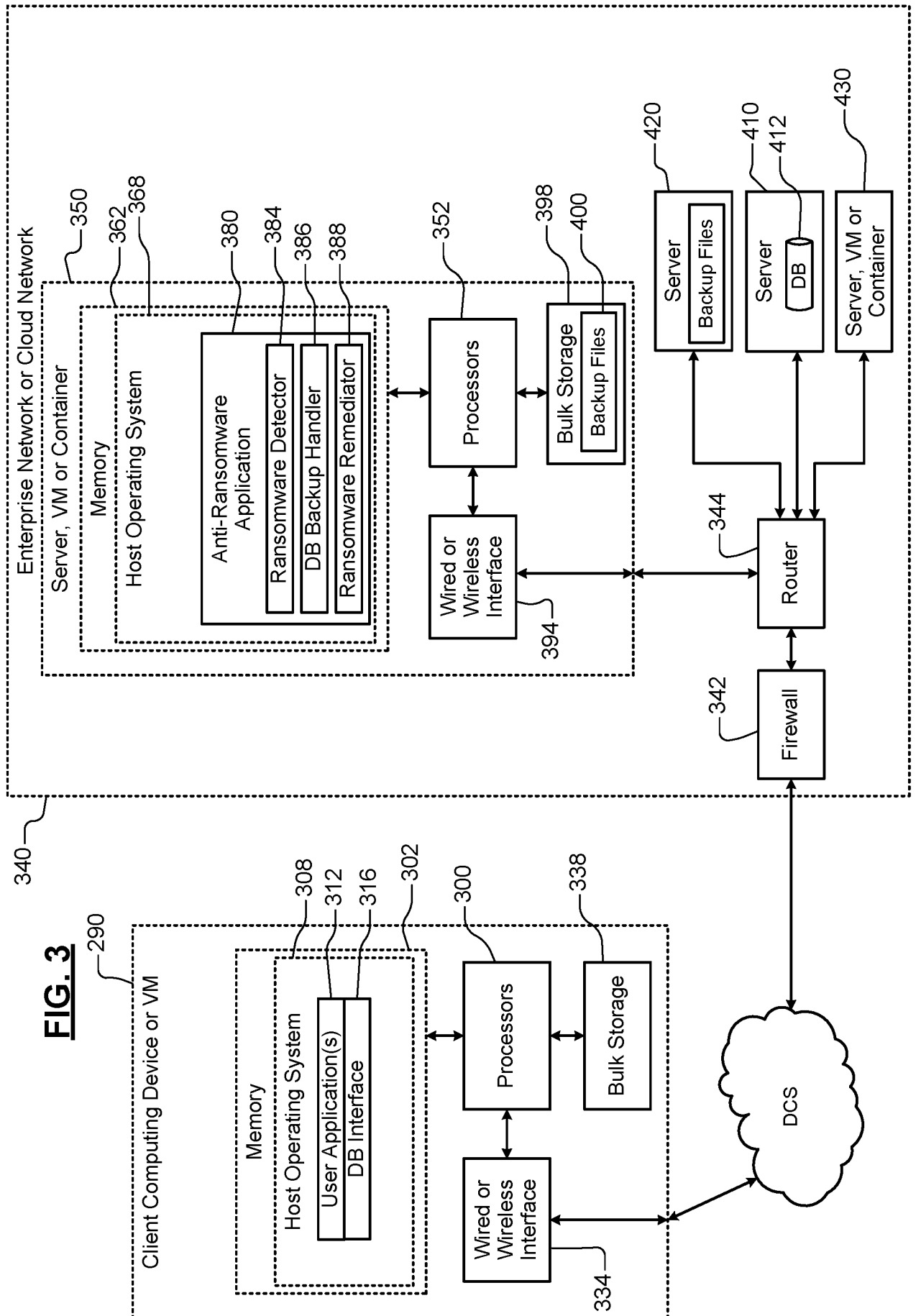
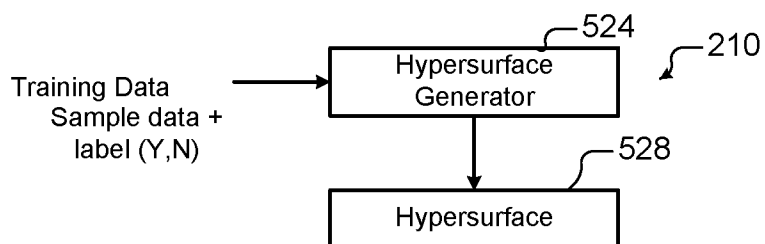
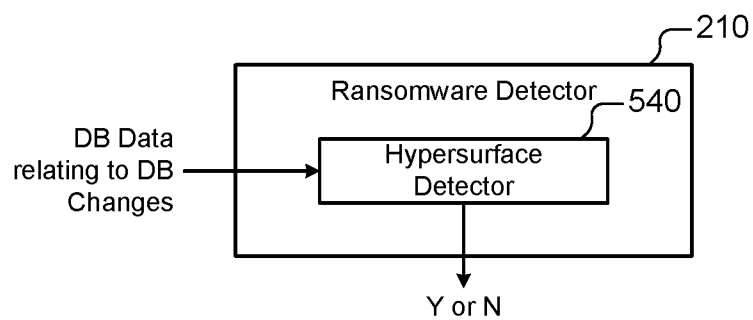
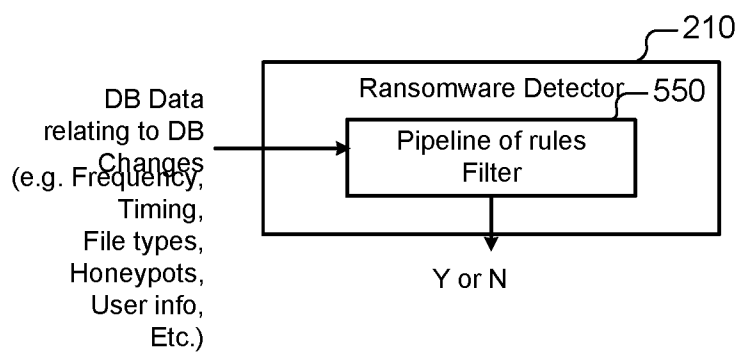


FIG. 2B



4/8

**FIG. 4A****FIG. 4B****FIG. 4C**

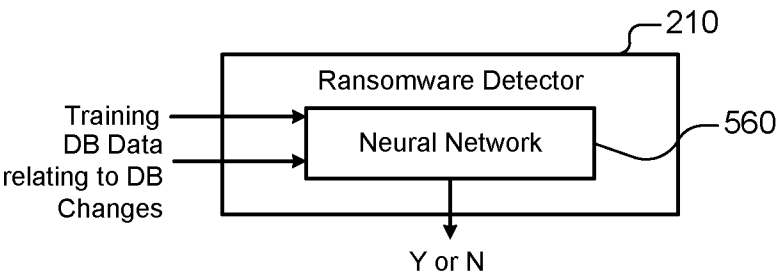


FIG. 4D

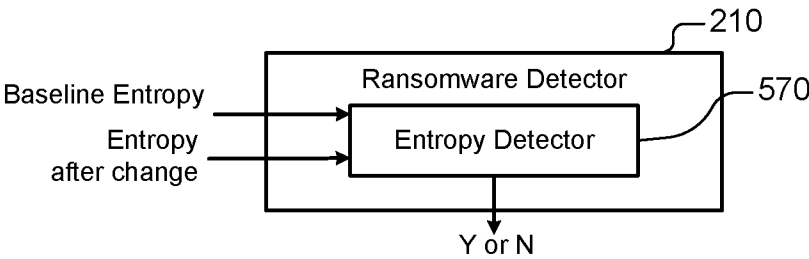


FIG. 4E

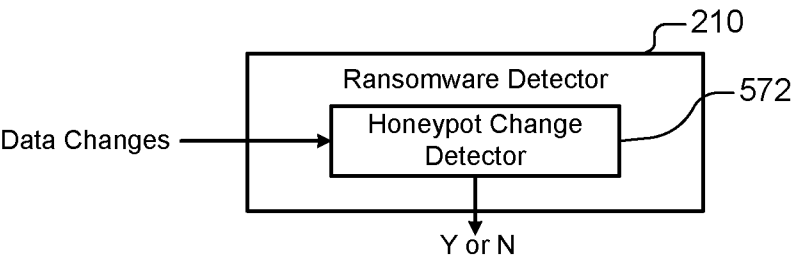


FIG. 4F

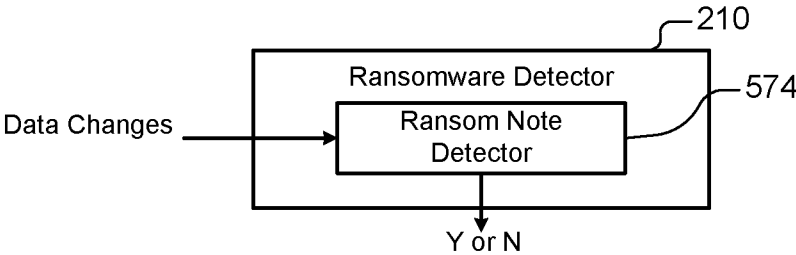
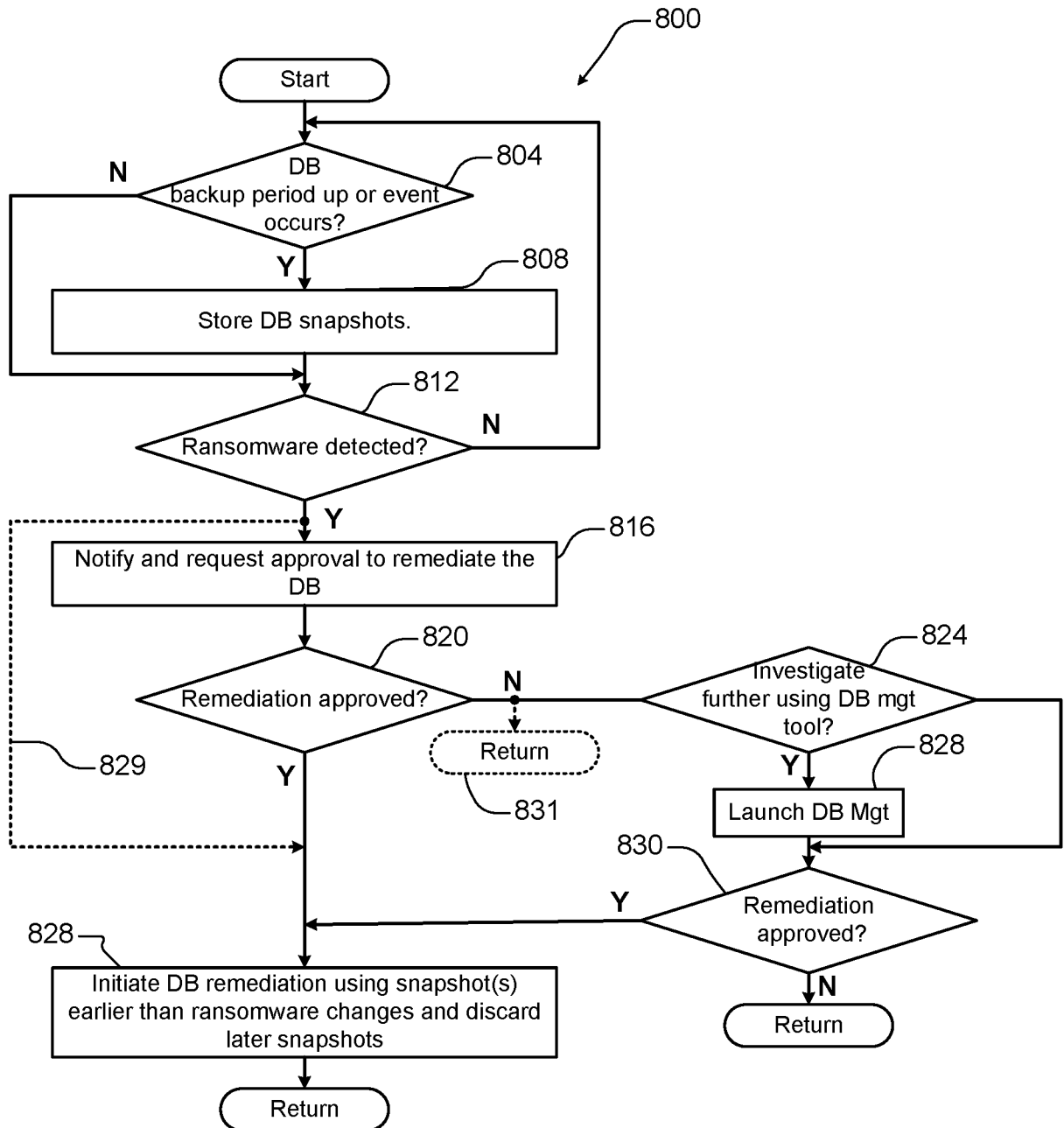
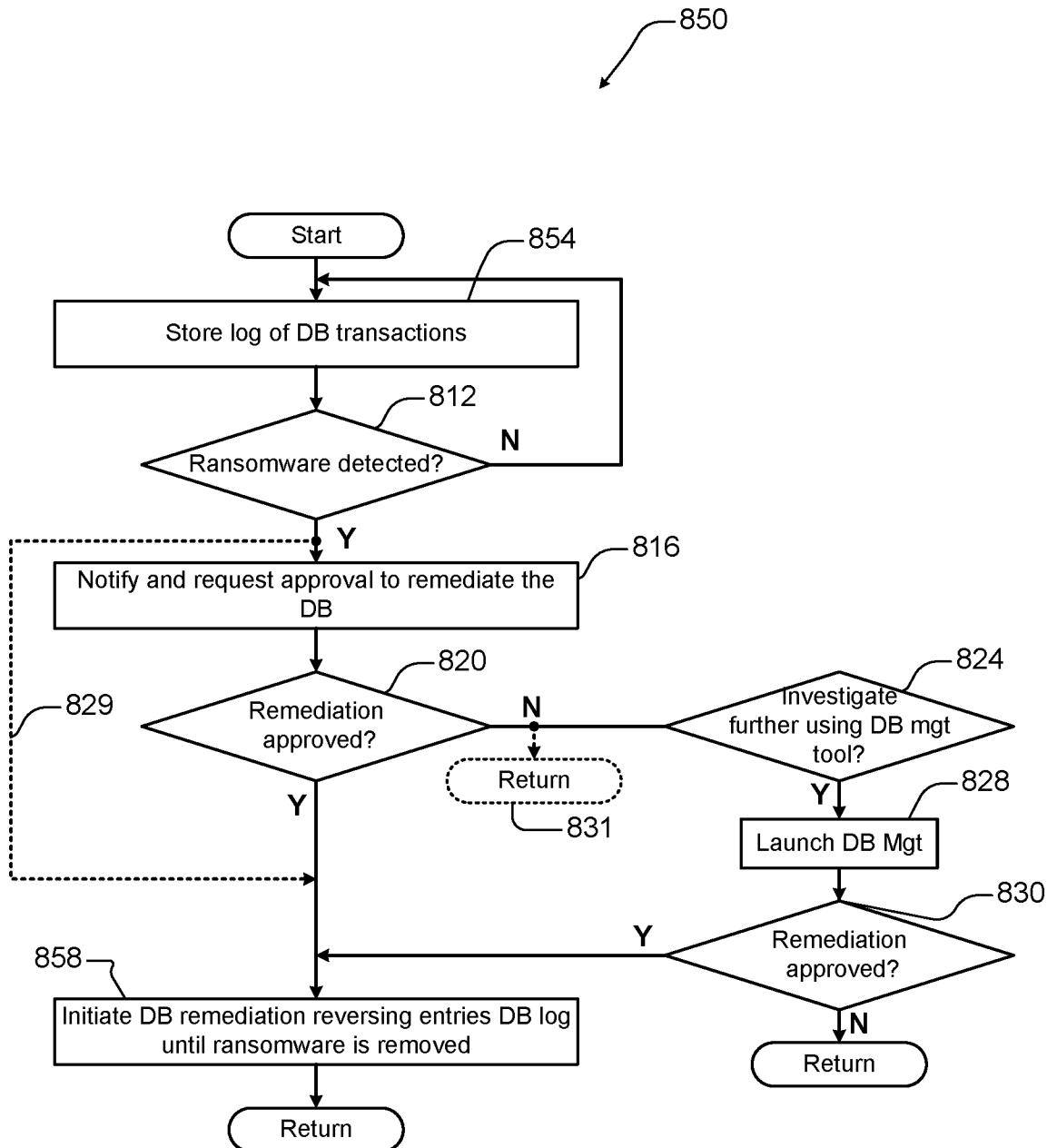


FIG. 4G

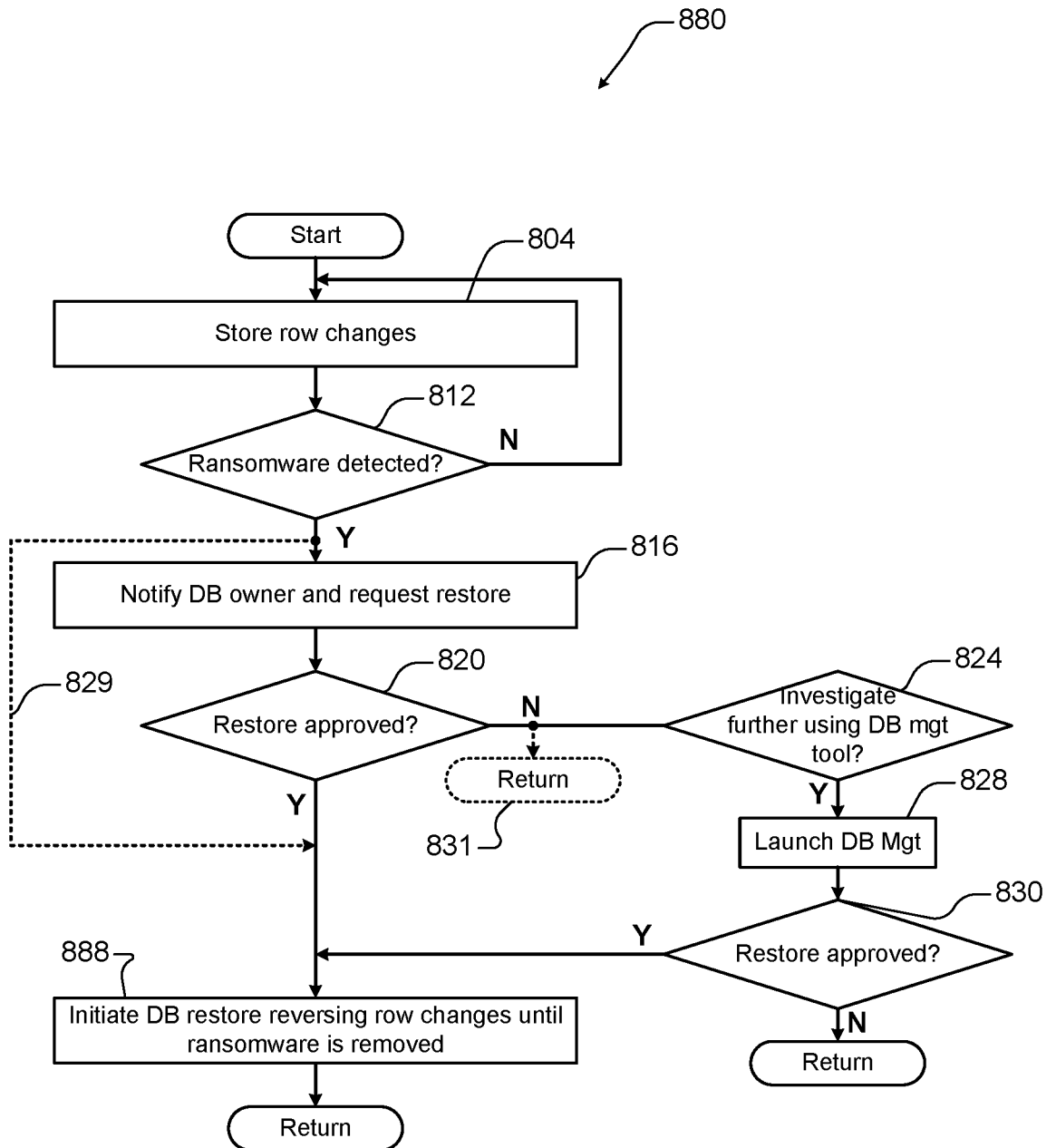
6/8

**FIG. 5**

7/8

**FIG. 6**

8/8

**FIG. 7**

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2017/067450

A. CLASSIFICATION OF SUBJECT MATTER
 INV. G06F21/56
 ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 9 317 686 B1 (YE HUA [CN] ET AL) 19 April 2016 (2016-04-19) abstract column 3, line 35 - column 4, line 19 column 5, line 1 - column 7, line 50 figures 1, 2	1-15
X	EP 3 107 024 A1 (AO KASPERSKY LAB [RU]) 21 December 2016 (2016-12-21) abstract paragraph [0020] - paragraph [0055] claims 1, 3, 4 figures 1, 2	1-15
E	WO 2018/020362 A1 (CISCO TECH INC [US]) 1 February 2018 (2018-02-01) the whole document	1-15



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

28 February 2018

Date of mailing of the international search report

08/03/2018

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040,
 Fax: (+31-70) 340-3016

Authorized officer

Bae, Jun-Young

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2017/067450

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 9317686	B1	19-04-2016	NONE
EP 3107024	A1	21-12-2016	CN 106257481 A 28-12-2016
			EP 3107024 A1 21-12-2016
			JP 2017010531 A 12-01-2017
			US 2016371152 A1 22-12-2016
WO 2018020362	A1	01-02-2018	US 2018024893 A1 25-01-2018
			WO 2018020362 A1 01-02-2018