

(19)日本国特許庁(JP)

(12)公開特許公報(A)

(11)公開番号
特開2024-86626
(P2024-86626A)

(43)公開日 令和6年6月27日(2024.6.27)

(51)国際特許分類

F I

G 0 6 F 18/23211(2023.01)

G 0 6 F 18/23211

G 0 6 N 20/00 (2019.01)

G 0 6 N 20/00

審査請求 未請求 請求項の数 19 O L (全30頁)

(21)出願番号	特願2023-206683(P2023-206683)	(71)出願人	500043574
(22)出願日	令和5年12月7日(2023.12.7)		ブラックベリー リミテッド
(31)優先権主張番号	18/083,102		BlackBerry Limited
(32)優先日	令和4年12月16日(2022.12.16)		カナダ国 エヌ2ケー 0エー7 オンタ
(33)優先権主張国・地域又は機関	米国(US)		リオ, ウォータールー, ユニバーシテ
			ィ アベニュー イースト 2200
			2200 University Ave
			nue East, Waterloo
			ON N2K 0A7, Canada
		(74)代理人	100107489
			弁理士 大塩 竹志
		(72)発明者	スティーブン ジョン ヘンケル
			カナダ国 エヌ2ケー 0エー7 オンタ
			リオ, ウォータールー, ユニバーシテ
			ィ アベニュー イースト 2200 気付

(54)【発明の名称】 インクリメンタル重心クラスタリングのための方法およびシステム

(57)【要約】 (修正有)

【課題】 インクリメンタル重心クラスタリングのための方法およびシステムを提供する。

【解決手段】 アノマリー検出のためのコンピューティングデバイスにおける方法であって、コンピューティングデバイスにおいて、複数のデータポイントに対するフルバッチモデルを格納することを含む。複数のデータポイントの各々は、複数のクラスタのうちの1つに関連付けられており、格納することは、複数のデータポイントを格納することなしに、複数のクラスタに関する情報を格納するためのテーブルを含む。方法はまた、新規のデータポイントをハードウェアセンサから受信することと、新規のデータポイントがフルバッチモデルの外にあることを決定し、これにより、アノマリーを検出することと、アノマリーに基づいて、アクションを実施することとを含む。

【選択図】 図 1 2

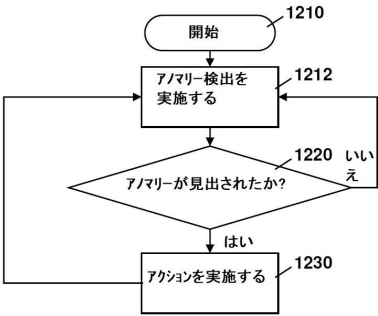


FIG. 12

【特許請求の範囲】**【請求項 1】**

アノマリー検出のためのコンピューティングデバイスにおける方法であって、前記方法は、

前記コンピューティングデバイスにおいて、複数のデータポイントに対するフルバッチモデルを格納することであって、前記複数のデータポイントの各々は、複数のクラスタのうちの 1 つに関連付けられており、前記格納することは、前記複数のデータポイントを格納することなしに、前記複数のクラスタに関する情報を格納するためのテーブルを含む、ことと、

新規のデータポイントをハードウェアセンサから受信することと、

10

前記新規のデータポイントが前記フルバッチモデルの外にあることを決定し、これにより、アノマリーを検出することと、

前記アノマリーに基づいて、アクションを実施することとを含む、方法。

【請求項 2】

前記コンピューティングデバイスは、

データポイントを選択することと、

前記データポイントがクラスタの中心までの平均距離の閾値内に入ることを決定することと、

前記データポイントを前記クラスタに追加することと、

20

データポイントトレーニングセット内の後続のデータポイントに対して前記決定することおよび追加することを反復的に実施することと

により、前記フルバッチモデルを作成する、請求項 1 に記載の方法。

【請求項 3】

前記データポイントを前記クラスタに追加することは、

前記クラスタ内のデータポイントの数を示すインデックスをインクリメントすることと

、前記データポイントに対する情報を前記クラスタに対する特徴の合計に追加することと

、前記クラスタの重心をアップデートすることと、

30

前記クラスタ内のポイント間の近似距離を含む値をアップデートすることとを含む、請求項 2 に記載の方法。

【請求項 4】

第 2 のデータポイントが前記クラスタの前記中心までの前記平均距離の前記閾値内に入らないことを決定することと、

前記データポイントに対する新規のクラスタを作成することと

をさらに含む、請求項 2 に記載の方法。

【請求項 5】

前記アノマリー検出システム内のクラスタの数が閾数を超えていることを決定することと、

40

前記アノマリー検出システムから前記クラスタ内に単一のデータポイントを有する全てのクラスタを除去することと、

前記閾値をより高い値にアップデートすることと

をさらに含む、請求項 4 に記載の方法。

【請求項 6】

前記閾数は、処理されるデータポイントの総数を下回る平方根の閾数である、請求項 5 に記載の方法。

【請求項 7】

前記コンピューティングデバイスは、各クラスタに関するインクリメンタル情報のみを格納する、請求項 1 に記載の方法。

50

【請求項 8】

前記アクションは、

アラートを提供することと、

前記コンピューティングデバイスと関連付けられたデバイスを自動的に制御することと

のうちの少なくとも 1 つを含む、請求項 1 に記載の方法。

【請求項 9】

前記コンピューティングデバイスは、IoT (internet of things) システム内のエッジデバイスである、請求項 1 に記載の方法。

【請求項 10】

アノマリー検出のためのコンピューティングデバイスであって、前記コンピューティングデバイスは、

プロセッサと、

通信サブシステムと

を備え、

前記コンピューティングデバイスは、

複数のデータポイントに対するフルバッチモデルを格納することであって、前記複数のデータポイントの各々は、複数のクラスタのうちの 1 つに関連付けられており、前記格納することは、前記複数のデータポイントを格納することなしに、前記複数のクラスタに関する情報を格納するためのテーブルを含む、ことと、

新規のデータポイントをハードウェアセンサから受信することと、

前記新規のデータポイントが前記フルバッチモデルの外にあることを決定し、これにより、アノマリーを検出することと、

前記アノマリーに基づいて、アクションを実施することと

を行うように構成されている、コンピューティングデバイス。

【請求項 11】

前記コンピューティングデバイスは、

データポイントを選択することと、

前記データポイントがクラスタの中心までの平均距離の閾値内に入ることを決定することと、

前記データポイントを前記クラスタに追加することと、

トレーニングデータポイントセット内の後続のデータポイントに対して前記決定することおよび追加することを反復的に実施することと

により、前記フルバッチモデルを作成するように構成されている、請求項 10 に記載のコンピューティングデバイス。

【請求項 12】

前記コンピューティングデバイスは、

前記クラスタ内のデータポイントの数を示すインデックスをインクリメントすることと、

前記データポイントに対する情報を前記クラスタに対する特徴の合計に追加することと、

前記クラスタの重心をアップデートすることと、

前記クラスタ内のポイント間の近似距離を含む値をアップデートすることと

により、前記データポイントを前記クラスタに追加するように構成されている、請求項 11 に記載のコンピューティングデバイス。

【請求項 13】

前記コンピューティングデバイスは、

第 2 のデータポイントが前記クラスタの前記中心までの前記平均距離の前記閾値内に入らないことを決定することと、

前記データポイントに対する新規のクラスタを作成することと

を行うようにさらに構成されている、請求項 1 1 に記載のコンピューティングデバイス。

【請求項 1 4】

前記コンピューティングデバイスは、
アノマリー検出のための内部のクラスタの数が閾数を超えていることを決定することと、

前記クラスタ内に単一のデータポイントを有する全てのクラスタを除去することと、
前記閾値をより高い値にアップデートすることと
を行うようにさらに構成されている、請求項 1 3 に記載のコンピューティングデバイス。

10

【請求項 1 5】

前記閾数は、処理されるデータポイントの総数を下回る平方根の閾数である、請求項 1 4 に記載のコンピューティングデバイス。

【請求項 1 6】

前記コンピューティングデバイスは、各クラスタに関するインクリメンタル情報のみを格納する、請求項 1 0 に記載のコンピューティングデバイス。

【請求項 1 7】

前記アクションは、
アラートを提供することと、
前記コンピューティングデバイスと関連付けられたデバイスを自動的に制御することと

20

のうちの少なくとも 1 つを含む、請求項 1 0 に記載のコンピューティングデバイス。

【請求項 1 8】

前記コンピューティングデバイスは、IoT システム内のエッジデバイスである、請求項 1 0 に記載のコンピューティングデバイス。

【請求項 1 9】

アノマリー検出のための命令コードを格納するためのコンピュータ格納媒体であって、前記命令コードは、コンピューティングデバイス上のプロセッサによって実行されると、前記コンピューティングデバイスに、

複数のデータポイントに対するフルバッチモデルを格納することであって、前記複数のデータポイントの各々は、複数のクラスタのうちの 1 つに関連付けられており、前記格納することは、前記複数のデータポイントを格納することなしに、前記複数のクラスタに関する情報を格納するためのテーブルを含む、ことと、

30

新規のデータポイントをハードウェアセンサから受信することと、

前記新規のデータポイントが前記フルバッチモデルの外にあることを決定し、これにより、アノマリーを検出することと

前記アノマリーに基づいて、アクションを実施することと
を行わせる、コンピュータ格納媒体。

【発明の詳細な説明】

【技術分野】

40

【0 0 0 1】

(開示の分野)

本開示は、アノマリー検出システムに関し、特に、アノマリー検出システムのための機械学習に関する。

【背景技術】

【0 0 0 2】

アノマリー検出は、それによってデータセット内の外れ値が識別され得るプロセスである。これは、例えば分散システム等の複雑なソフトウェアシステム内で役割を果たし、利益の中でもとりわけ、システムに対する脅威が検出されること、エラーの根本原因が識別されること、システムの健全性の監視、データのクリーニング等を可能にする。

50

【0003】

伝統的に、アノマリー検出システムは、手動的に構築されてきた。これは、相当なドメインの知見と、遭遇する可能性のある問題に関する先見の明とを伴うものであった。さらに、そのようなシステムは、スタティックである傾向があり、これは、システムに対する脅威が発展し得るときに望ましくない。

【0004】

これに関し、最近では、機械学習アルゴリズムが、そのようなアノマリー検出システムを作成するために使用されるようになってきている。そのような機械学習アルゴリズムは、概して、大きなデータセットを取り扱うことが可能であり、経時的に適応可能であり得、手動的な作成よりもより良好に機能し得るシステムを作成する。そのような機械学習アルゴリズムの例は、とりわけ、One Class SVM (Support Vector Method)、ランダムフォレスト、局所外れ値因子法等を含む。

10

【0005】

しかしながら、そのような機械学習アルゴリズムは、処理およびメモリ要件の両方の観点で相当なオーバーヘッドを有する。それ故、これらのアルゴリズムは、分散システム内に実装されるためには実用的ではなく、そのようなシステムのエッジ上の処理モジュールは、そのようなアルゴリズムを効果的に実行するために必要なメモリまたは処理パワーを有していない可能性がある。

【発明の概要】

【課題を解決するための手段】

20

【0006】

本発明は、例えば、以下の項目を提供する。

(項目1)

アノマリー検出のためのコンピューティングデバイスにおける方法であって、前記方法は、

前記コンピューティングデバイスにおいて、複数のデータポイントに対するフルバッチモデルを格納することであって、前記複数のデータポイントの各々は、複数のクラスタのうちの1つに関連付けられており、前記格納することは、前記複数のデータポイントを格納することなしに、前記複数のクラスタに関する情報を格納するためのテーブルを含む、ことと、

30

新規のデータポイントをハードウェアセンサから受信することと、

前記新規のデータポイントが前記フルバッチモデルの外にあることを決定し、これにより、アノマリーを検出することと、

前記アノマリーに基づいて、アクションを実施することと

を含む、方法。

(項目2)

前記コンピューティングデバイスは、

データポイントを選択することと、

前記データポイントがクラスタの中心までの平均距離の閾値内に入ることを決定することと、

40

前記データポイントを前記クラスタに追加することと、

データポイントトレーニングセット内の後続のデータポイントに対して前記決定することおよび追加することを反復的に実施することと

により、前記フルバッチモデルを作成する、上記項目に記載の方法。

(項目3)

前記データポイントを前記クラスタに追加することは、

前記クラスタ内のデータポイントの数を示すインデックスをインクリメントすることと、

前記データポイントに対する情報を前記クラスタに対する特徴の合計に追加することと、

50

前記クラスタの重心をアップデートすることと、
前記クラスタ内のポイント間の近似距離を含む値をアップデートすることと
を含む、上記項目のいずれか 1 項に記載の方法。

(項目 4)

第 2 のデータポイントが前記クラスタの前記中心までの前記平均距離の前記閾値内に入らないことを決定することと、

前記データポイントに対する新規のクラスタを作成することと
をさらに含む、上記項目のいずれか 1 項に記載の方法。

(項目 5)

前記アノマリー検出システム内のクラスタの数が関数を超えていることを決定することと、

前記アノマリー検出システムから前記クラスタ内に単一のデータポイントを有する全てのクラスタを除去することと、

前記閾値をより高い値にアップデートすることと
をさらに含む、上記項目のいずれか 1 項に記載の方法。

(項目 6)

前記関数は、処理されるデータポイントの総数を下回る平方根の関数である、上記項目のいずれか 1 項に記載の方法。

(項目 7)

前記コンピューティングデバイスは、各クラスタに関するインクリメンタル情報のみを格納する、上記項目のいずれか 1 項に記載の方法。

(項目 8)

前記アクションは、
アラートを提供することと、

前記コンピューティングデバイスと関連付けられたデバイスを自動的に制御することと
のうちの少なくとも 1 つを含む、上記項目のいずれか 1 項に記載の方法。

(項目 9)

前記コンピューティングデバイスは、IoT (internet of things) システム内のエッジデバイスである、上記項目のいずれか 1 項に記載の方法。

(項目 10)

アノマリー検出のためのコンピューティングデバイスであって、前記コンピューティングデバイスは、

プロセッサと、
通信サブシステムと
を備え、

前記コンピューティングデバイスは、

複数のデータポイントに対するフルバッチモデルを格納することであって、前記複数のデータポイントの各々は、複数のクラスタのうちの 1 つに関連付けられており、前記格納することは、前記複数のデータポイントを格納することなしに、前記複数のクラスタに関する情報を格納するためのテーブルを含む、ことと、

新規のデータポイントをハードウェアセンサから受信することと、

前記新規のデータポイントが前記フルバッチモデルの外にあることを決定し、これにより、アノマリーを検出することと、

前記アノマリーに基づいて、アクションを実施することと
を行うように構成されている、コンピューティングデバイス。

(項目 11)

前記コンピューティングデバイスは、
データポイントを選択することと、

前記データポイントがクラスタの中心までの平均距離の閾値内に入ることを決定する

ことと、

前記データポイントを前記クラスタに追加することと、

トレーニングデータポイントセット内の後続のデータポイントに対して前記決定することおよび追加することを反復的に実施することと

により、前記フルバッチモデルを作成するように構成されている、上記項目のいずれか1項に記載のコンピューティングデバイス。

(項目12)

前記コンピューティングデバイスは、

前記クラスタ内のデータポイントの数を示すインデックスをインクリメントすることと、

前記データポイントに対する情報を前記クラスタに対する特徴の合計に追加することと、

前記クラスタの重心をアップデートすることと、

前記クラスタ内のポイント間の近似距離を含む値をアップデートすることと

により、前記データポイントを前記クラスタに追加するように構成されている、上記項目のいずれか1項に記載のコンピューティングデバイス。

(項目13)

前記コンピューティングデバイスは、

第2のデータポイントが前記クラスタの前記中心までの前記平均距離の前記閾値内に入らないことを決定することと、

前記データポイントに対する新規のクラスタを作成することと

を行うようにさらに構成されている、上記項目のいずれか1項に記載のコンピューティングデバイス。

(項目14)

前記コンピューティングデバイスは、

アノマリー検出のための内部のクラスタの数が閾数を超えていることを決定することと、

前記クラスタ内に単一のデータポイントを有する全てのクラスタを除去することと、

前記閾値をより高い値にアップデートすることと

を行うようにさらに構成されている、上記項目のいずれか1項に記載のコンピューティングデバイス。

(項目15)

前記閾数は、処理されるデータポイントの総数を下回る平方根の閾数である、上記項目のいずれか1項に記載のコンピューティングデバイス。

(項目16)

前記コンピューティングデバイスは、各クラスタに関するインクリメンタル情報のみを格納する、上記項目のいずれか1項に記載のコンピューティングデバイス。

(項目17)

前記アクションは、

アラートを提供することと、

前記コンピューティングデバイスと関連付けられたデバイスを自動的に制御することと

のうちの少なくとも1つを含む、上記項目のいずれか1項に記載のコンピューティングデバイス。

(項目18)

前記コンピューティングデバイスは、IoTシステム内のエッジデバイスである、上記項目のいずれか1項に記載のコンピューティングデバイス。

(項目19)

アノマリー検出のための命令コードを格納するためのコンピュータ格納媒体であって、前記命令コードは、コンピューティングデバイス上のプロセッサによって実行されると、

10

20

30

40

50

前記コンピューティングデバイスに、

複数のデータポイントに対するフルバッチモデルを格納することであって、前記複数のデータポイントの各々は、複数のクラスタのうちの1つに関連付けられており、前記格納することは、前記複数のデータポイントを格納することなしに、前記複数のクラスタに関する情報を格納するためのテーブルを含む、ことと、

新規のデータポイントをハードウェアセンサから受信することと、

前記新規のデータポイントが前記フルバッチモデルの外にあることを決定し、これにより、アノマリーを検出することと

前記アノマリーに基づいて、アクションを実施することと

を行わせる、コンピュータ格納媒体。

10

(摘要)

アノマリー検出のためのコンピューティングデバイスにおける方法であって、前記方法は、前記コンピューティングデバイスにおいて、複数のデータポイントに対するフルバッチモデルを格納することであって、前記複数のデータポイントの各々は、複数のクラスタのうちの1つに関連付けられており、前記格納することは、前記複数のデータポイントを格納することなしに、前記複数のクラスタに関する情報を格納するためのテーブルを含む、ことと、新規のデータポイントをハードウェアセンサから受信することと、前記新規のデータポイントが前記フルバッチモデルの外にあることを決定し、これにより、アノマリーを検出することと、前記アノマリーに基づいて、アクションを実施することを含む。

20

【図面の簡単な説明】

【0007】

本開示は、図面を参照することでより良く理解され得る。

【0008】

【図1】図1は、フルバッチアノマリー検出システムのための処理および格納を示すブロック図であり、処理および格納は、エッジデバイスにおいて行われる。

【0009】

【図2】図2は、フルバッチアノマリー検出システムのための処理および格納を示すブロック図であり、処理および格納は、クラウドデバイスにおいて行われる。

【0010】

【図3】図3は、フルバッチアノマリー検出システムのための処理および格納を示すブロック図であり、処理および格納は、クラウドデバイスにおいて行われ、フルバッチモデルは、エッジデバイスにプッシュされる。

30

【0011】

【図4】図4は、例示的な車両システムを示すブロック図である。

【0012】

【図5】図5は、インクリメンタル重心クラスタ情報を格納するための例示的なデータ構造を示すブロック図である。

【0013】

【図6】図6は、インクリメンタル重心クラスタモデルのためのトレーニングのための処理を示すプロセス図である。

40

【0014】

【図7】図7は、データポイントをクラスタに追加するためのプロセスを示すプロセス図である。

【0015】

【図8】図8は、アノマリー検出のためのインクリメンタル重心クラスタリングモデルのための処理および格納を示すブロック図であり、処理および格納は、エッジデバイスにおいて行われる。

【0016】

【図9】図9は、3次元において処理されている8個の例示的なクラスタを示すグラフである。

50

【0017】

【図10】図10は、図9のプロットからの良性データポイントのクラスタリングと、アノマリーの識別とを示すグラフである。

【0018】

【図11】図11は、例示的な混同行列のブロック図である。

【0019】

【図12】図12は、アノマリーの検出時にアクションを実施するためのプロセス図である。

【0020】

【図13】図13は、本開示の実施形態とともに使用されることが可能な簡略化されたコンピューティングデバイスのブロック図である。

10

【発明を実施するための形態】

【0021】

(図面の詳細な説明)

本開示は、アノマリー検出のためのコンピューティングデバイスにおける方法を提供し、方法は、コンピューティングデバイスにおいて、複数のデータポイントに対するフルバッチモデルを格納することであって、複数のデータポイントの各々は、複数のクラスタのうちの1つに関連付けられており、格納することは、複数のデータポイントを格納することなしに、複数のクラスタに関する情報を格納するためのテーブルを含む、ことと、新規のデータポイントをハードウェアセンサから受信することと、新規のデータポイントがフルバッチモデルの外にあることを決定し、これにより、アノマリーを検出することと、アノマリーに基づいて、アクションを実施することを含む。

20

【0022】

本開示は、アノマリー検出のためのコンピューティングデバイスをさらに提供し、コンピューティングデバイスは、プロセッサと、通信サブシステムとをさらに提供し、コンピューティングデバイスは、複数のデータポイントに対するフルバッチモデルを格納することであって、複数のデータポイントの各々は、複数のクラスタのうちの1つに関連付けられており、格納することは、複数のデータポイントを格納することなしに、複数のクラスタに関する情報を格納するためのテーブルを含む、ことと、新規のデータポイントをハードウェアセンサから受信することと、新規のデータポイントがフルバッチモデルの外にあることを決定し、これにより、アノマリーを検出することと、アノマリーに基づいてアクションを実施することとを行うように構成されている。

30

【0023】

本開示は、アノマリー検出のための命令コードを格納するためのコンピュータ格納媒体をさらに提供し、命令コードは、コンピューティングデバイス上のプロセッサによって実行されると、コンピューティングデバイスに、複数のデータポイントに対するフルバッチモデルを格納することであって、複数のデータポイントの各々は、複数のクラスタのうちの1つに関連付けられており、格納することは、複数のデータポイントを格納することなしに、複数のクラスタに関する情報を格納するためのテーブルを含む、ことと、新規のデータポイントをハードウェアセンサから受信することと、新規のデータポイントがフルバッチモデルの外にあることを決定し、これにより、アノマリーを検出することと、アノマリーに基づいて、アクションを実施することとを行わせる。

40

【0024】

本開示は、IoT (Internet of Things) デバイスに関する。例えば、そのようなデバイスは、自動車システムを含み得る。しかしながら、本明細書中に記載される方法およびシステムは、その他のシステム内でも等しく使用され得る。したがって、本開示の技術は、任意の特定のシステムに限定されるものではない。

【0025】

いくつかの場合、ソフトウェアプログラムは、例えばインターネット等のパブリックネットワークに接続されるかまたはパブリックネットワークを介してアクセス可能なシステ

50

ム内で実行され得る。悪意のある行為者は、ネットワーク接続されたソフトウェアプログラムの挙動に影響を与えるために、様々な悪用技術を使用し得る。その他の場合、システムに対するアクセスを有する悪意のある行為者は、ソフトウェアの挙動に影響を与えるために、悪意のあるコードをシステムソフトウェアに挿入し得る。

【0026】

特に、IoTデバイスの普及が進むにつれて、攻撃者が非道な目的のために標的とし得る脅威サーフェスも増加し続けている。保護ベースのメカニズムは、侵入の開始を防ぎ得るが、そのような方法が失敗した場合、エンドポイント上のアノマリー性挙動を検出し、エンドポイント、ビジネス、またはユーザを被害から保護するためのアクションを促す方法を有することが有益であり得る。

【0027】

例えば、現代の車両は、1億行を超えるソフトウェアコードを有し得る。車両内のソフトウェアが成長するにつれて、攻撃サーフェスも成長し、このことは、そのようなソフトウェアを攻撃に対して脆弱にする。ソフトウェアの各粗末に構成された部分が、攻撃者によって悪用され得る潜在的な脆弱性を表している。

【0028】

ハッカーをシステムに近づけないために使用される「キャッスルウォール」は、不十分であり得るか、または経時的に悪意のある行為者によって迂回され得る。システムは、いくつかの場合、侵害されたデバイスを検出することが可能でないことがあり得る。

【0029】

これに関し、アノマリーを検出するために、システム内のデータ（例えば、ログ等）を分析し得る方法およびシステムが提供される。そのようなシステムは、データアノマリーを見出すために、機械学習を使用し得る。

【0030】

さらに、例えばそのような車両等のエッジシステム上で、メモリ、通信、および処理における限定が存在し得る。例えば、IoTデバイスは、典型的には、ハードドライブ空間を最適化せず、このことは、データを格納するための性能が限定され得ることを意味している。さらに、IoTデバイスは、しばしば、限定された処理パワーを有し、全てのIoTデバイスが、常時クラウドに容易に接続することが可能ではないことがあり得る。

【0031】

ログの分析に関する問題を引き起こし得るさらなる因子は、IoTデバイスが様々な挙動を有し得ることである。特に、ユーザがどのようにIoTデバイスを使用するか、またはそれがシステム内でどのように構成されるかに依存して、通常の挙動は、類似したIoTデバイス間で異なって見え得る。

【0032】

本明細書中で使用されるとき、エッジデバイスおよびIoTデバイスは、同義的に使用される。

【0033】

現在のアノマリー検出システムは、「フルバッチモデル」アルゴリズムを使用し得る。そのようなモデルは、全てのデータに対して一度にトレーニングする必要があるアノマリー検出システムを参照し、例は、とりわけ、One Class SVM、分離フォレスト（Isolation Forest）、局所外れ値因子（Local Outlier Factor）を含み得る。そのようなモデルは、全ての良性データが処理のために格納されることを必要とする。これに関し、相当な量の格納空間が、エッジIoTデバイスにおいて必要とされ得、これは、存在しない可能性がある。

【0034】

特に、図1に対する参照がなされ、本図は、エッジトレーニング102、エッジ再トレーニング104、およびエッジ推論106の間に必要とされるステップを示しており、フルバッチモデルは、エッジデバイス上に配置される。

【0035】

10

20

30

40

50

図 1 の例は、例示的なエッジデバイスとして車両内インフォテインメントシステム（IVI）110を使用する。しかしながら、そのようなデバイスは、例証目的のために提供されているに過ぎず、本開示は、車両内インフォテインメントシステムに限定されない。

【0036】

IVI 110は、システムログ112を作成し、システムログから、特徴114を工作する。

【0037】

そのような特徴は、ブロック116において、特徴ベクトルに変換される。このことは、エッジトレーニング102、エッジ再トレーニング104、およびエッジ推論106の全てに対して起こる。

【0038】

エッジトレーニング102およびエッジ再トレーニング104に対し、エッジデバイスは、ブロック120において、ベクトルを格納する必要がある。このことは、最終的に集合体上でクラスタ化するために行われる。エッジデバイスに対し、エッジデバイス上にベクトルを格納する必要性は、所望のディスクアロケーションが過度に小さい場合、実行不可能な解決策につながり得る。このことは、モデルが再トレーニングされる必要がある場合に、悪化し得る。例えば、新規のソフトウェアアップデートがエッジデバイスに提供され、新規のアプリケーションがインストールされる場合、因子の中でもとりわけ、格納問題が追加される。

【0039】

格納されたベクトルから、ブロック122において、モデルがトレーニングされる。モデルは、全ての利用可能な良性データに対してトレーニングされる必要があり得る。いくつかのフルバッチモデル（例えば、One Class SVM等）では、このことは、長時間かかり得、トレーニングのために多くのリソースを要し得る。いくつかの場合、モデルは、失敗なしに全体のデータセットをトレーニングすることが可能ではないことがあり得る。その他のモデル（例えば、分離フォレスト等）は、このことに悩まされない可能性があるが、それらは典型的には、one class SVMと比較して有効性に悩まされる。

【0040】

ブロック122におけるトレーニングから、フルバッチモデル130が作成され得る。エッジ再トレーニング104に対し、再トレーニングされたモデル140が、アップデートされたフルバッチモデル130を作成するために使用され得る。

【0041】

フルバッチモデル130は、その後、ブロック150に示されている推論の間に使用され得、その後、これは、出力152を生成し得る。

【0042】

フルバッチモデルは、典型的に、モデルをインクリメンタルにトレーニングし得ないが、その代わりに、ゼロから開始する必要がある得、このことは、エッジデバイスが有し得るものよりも多くのリソースを要し得る。

【0043】

したがって、図 1 の実施形態に従うと、主要な問題のうちの1つは、エッジデバイスの空間の限定である。これに関し、格納および処理がクラウド解決策に移行された場合、代替的なアプローチが可能であり得る。ここで図 2 に対する参照がなされる。

【0044】

特に、エッジデバイスは、分析されるべきログデータの一定のストリームをクラウドサーバまたはサービスに送信し得るが、このことは、エッジデバイスからの通信チャネルを圧倒し得、それ故、実装するためには過度に高価になる。

【0045】

図 2 の場合では、4つのプロセスが示されており、特に、エッジデバイス上で起こるエッジ収集202、クラウド内で起こるクラウドトレーニング204、エッジデバイス上で

10

20

30

40

50

起こるエッジ再収集 206、およびエッジデバイス上で起こるエッジ推論 208（クラウドからの入力を伴う）が示されている。

【0046】

図1の実施形態と同様に、エッジデバイス I V I 110 は、システムログ 112 を作成し、システムログから、特徴 114 を工作する。

【0047】

そのような特徴は、ブロック 116 において、特徴ベクトルに変換される。このことは、エッジ収集 202、エッジ再収集 206、およびエッジ推論 208 の全てに対して起こる。

【0048】

エッジ収集 202 およびエッジ再収集 206 に対し、エッジデバイスは、ブロック 210 において、クラウド格納のためにベクトルをクラウドに提供する。

【0049】

格納されたベクトルから、ブロック 212 において、モデルがトレーニングされる。さらに、ブロック 212 におけるトレーニングから、フルバッチモデル 220 がクラウドにおいて作成され得る。

【0050】

フルバッチモデル 220 は、その後、ブロック 150 に示されている推論の間に使用され得、その後、これは、出力 152 を生成し得る。

【0051】

図2の実施形態は、エッジデバイスにおいて過度に多くのデータを格納するという問題を修正するが、このことは、クラウドと相互作用するコストとの引き換えであり得る。特に、エッジデバイスは、毎秒数千の記録を生成することが可能であり得る。因子の中でもとりわけ、いくつかのフィルタリング、集約が適用され得、このことは、エンドポイント毎に相当な量の帯域幅をもたらし得る。そのような通信コストは、データを伝送すると予想されるエンドポイントの数によってさらに膨らみ得る。

【0052】

さらに、エッジ再収集 206 の間の再トレーニングに対し、より多くのデータがクラウドに送信される必要があり、上記と同じ問題を有している。

【0053】

それ故、トレーニングおよび再トレーニングの両方に対し、トレーニングのために必要とされるデータの量を考えると、クラウド内のトレーニングに対するコストは法外なものとなり得る。

【0054】

さらに、いったんモデルがトレーニングされると、モデルは、推論のためにエンドポイントにデータを返送する必要がある、このことは、データを重くし、かつ推論のための遅延時間も増加させ得、いくつかの場合、潜在的に、推論に対するアクションを取ることを過度に遅くし得る。特に、クラウドとの通信は、各往復に対して遅延を追加し、クラウドへのインターネット接続性とクラウドからのインターネット接続性とを有するコンポーネントをさらに必要とする。攻撃者がエンドポイントをオフラインにすることが可能な場合、アノマリー検出機能は機能しなくなり得る。

【0055】

上記に基づいて、エッジデバイスに対する別のアプローチは、いったんトレーニングが完了すると、フルバッチモデルをエッジに移行させることである。ここで図3に対する参照がなされる。

【0056】

図3の場合では、4つのプロセスが示されており、特に、エッジデバイス上で起こるエッジ収集 302、クラウド内で起こるクラウドトレーニング 304、エッジデバイス上で起こるエッジ再収集 306、およびエッジデバイス上で起こるエッジ推論 308 が示されている。

10

20

30

40

50

【0057】

図1および2の実施形態と同様に、エッジデバイスI V I 1 1 0上で、システムログ1 1 2を作成し、システムログから、特徴1 1 4を工作する。

【0058】

そのような特徴は、ブロック1 1 6において、特徴ベクトルに変換される。このことは、エッジ収集3 0 2、エッジ再収集3 0 6、およびエッジ推論3 0 8の全てに対して起こる。

【0059】

エッジ収集3 0 2およびエッジ再収集3 0 6に対し、エッジデバイスは、ブロック2 1 0において、クラウド格納のためにベクトルをクラウドに提供する。

【0060】

格納されたベクトルから、ブロック2 1 2において、モデルがトレーニングされる。さらに、ブロック2 1 2におけるトレーニングから、フルバッチモデル2 2 0がクラウドにおいて作成され得る。

【0061】

フルバッチモデル2 2 0は、その後、ブロック3 1 0で示されるように、エッジに展開され得、その後、これは、ブロック3 3 0に示されている推論の間に使用され得るフルバッチモデル3 2 0を作成し得、その後、これは、出力3 3 2を生成し得る。

【0062】

図3の実施形態は、推論の間に、インターネット接続性をオフにすることによってアノマリー検出メカニズムを停止させる性能を低減させるが、このアプローチには懸念とするエリアが依然として存在する。特に、エンドポイントからクラウドに相当量のデータを送信するという問題が存在し、このことは、通信機能性およびコストの観点で法外になり得る。さらに、再トレーニングは、図2の実施形態と同じ問題に悩まされる。終了トレーニングも、全てのフルバッチモデルに対して同じ限定に直面する。

【0063】

したがって、本開示は、複雑なシステム上でのアノマリー検出のためのインクリメンタル重心クラスタリング方法およびシステムを提供する。

【0064】

車両ソフトウェアシステム

【0065】

本開示のインクリメンタル重心クラスタリング方法およびシステムは、任意のコンピューティングシステム（例えば、IoTシステム等）上で使用され得るが、一実施形態において、それは、車両システム内で使用され得る。しかしながら、本開示は、車両システムに限定されず、車両システムは、本明細書中では、例証目的のために提供されているに過ぎない。

【0066】

ここで図4に対する参照がなされ、本図は、例示的な車両システムを示している。

【0067】

図4の実施形態において、車両4 0 0は、コンピューティングシステムおよび通信システムを装備され得る。コンピューティングシステムの一部は、ドメイン4 1 0を含み得、これは、ログデータを作成するアプリケーションを有し得る。さらに、車両4 0 0上のコンピューティングシステムの一部は、下記に記載されるように、アノマリー検出を実施する。

【0068】

図4の例において、車両4 0 0は、通信システムを利用して、図4においてe N B 4 2 0として示されているセルラー基地局と通信する。基地局は、コアネットワーク4 3 0と通信し得、その後、これは、ネットワーク4 3 2を通してクラウドサービスプロバイダ4 4 0に通信を転送し得る。ネットワーク4 3 2は、例えば、ワイドエリアネットワーク（例えば、インターネット等）であり得る。

10

20

30

40

50

【0069】

その他の実施形態において、コアネットワーク430ではなく、特定のセルラー通信プロトコルまたは無線通信プロトコルに関連付けられた任意の技術が使用され得る。

【0070】

いくつかの実施形態において、クラウドサービス440は、ドメインに対する処理を提供し得るか、またはドメイン内で使用される情報を提供し得る。

【0071】

さらに、車両ではなく、デバイス460が、アノマリー検出のために使用され得る。デバイス460は、任意のコンピューティングデバイスであり得、オプションの中でもとりわけ、IoTデバイス、モバイルデバイス、医療用機器、車両、または車両に関連付けられた機器等を含み得る。デバイス460は、様々な有線技術または無線技術（限定されるものではないが、オプションの中でもとりわけ、イーサネット（登録商標）、ファイバ、セルラー、Wi-Fi、衛星等）を利用して、ネットワーク432を通して通信し得る。

【0072】

図4の実施形態において、車両400上のドメイン410およびデバイス450は、いくつかの場合、エッジデバイスとして考えられ得、限定された格納および／または処理を有する。

【0073】

インクリメンタル重心クラスタリング

【0074】

上述のように、エッジデバイス上の既存の機械学習モデルの使用は、非実用的である。特に、既存の機械学習アノマリー検出アルゴリズムを利用して、ログまたはテーブル形式データを分析するとき、主要な問題は、そのようなアルゴリズムに対して必要とされる情報を格納するための十分な空間が存在しないこと、フルバッチモデルを作成するために十分な処理が存在しないこと、および／または全てのデータをクラウドに提供するために十分な通信性能が存在しないことである。さらに、データは前もって必要とされ、インクリメンタルにアップデートすることは困難である。

【0075】

これに関し、インクリメンタル重心クラスタリングのためのアルゴリズムが本明細書中に記載される。下記に詳細に記載されるように、第1のデータポイントは、クラスタを作成するために使用され得、その後、後続のポイントが分析され得、そのクラスタ内の全てのポイントの相互間の平均距離の閾値距離内にそれらが存在するかどうかを決定し得る。そうである場合、新規のデータポイントがクラスタに追加され、クラスタの形状は、新規の追加に基づいて調整され得る。そうではない場合、新規のクラスタが形成される。

【0076】

さらに、いくつかの実施形態において、クラスタの数は、推論時間が過大にならないように、処理されるポイントの数に比例するように限定され得る。この場合、小さなクラスタ（例えば、典型的には外れ値であるサイズ1のもの等）が、所望の最大クラスタプロポーション閾値が超過された場合に、機会を見て除去され得る。これが起こると、閾値は、新規クラスタがより少なく作成されることを助長するために、閾値調整因子によって増加され得る。

【0077】

いったんモデルがトレーニングされると、既存のクラスタの閾値距離内で予測されるものは全て、良性として考えられ、そうではない場合、アノマリー性として考えられる。

【0078】

インクリメンタル重心クラスタリングモデルにおいて、格納されるデータは、最大で処理されるポイントの数の平方根の関数であるクラスタのみである、または、各クラスタは、アルゴリズムが機能するための全ての情報を含む単一のベクトルを含有する。

【0079】

さらに、インクリメンタル重心クラスタリングは、インクリメンタルである。クラスタ

10

20

30

40

50

リングを実施するために全てのデータを必要とするのとは対照的に、インクリメンタル重心クラスタリングは、一度に1つのデータポイントをクラスタリングし得る。

【0080】

下記に記載されるように、そのようなアルゴリズムの有効性は、その他の機械学習アルゴリズムと比較してテストされ、テストされた最良のフルバッチアルゴリズムに近いが、またはより良好であることが見出された。

【0081】

ここで図5に対する参照がなされる。図5の実施形態は、クラスタに関する情報を格納するためのデータ構造の例を示している。しかしながら、図5の例は、そのような情報を格納するための1つのオプションに過ぎない。例示的なデータ構造内に格納される情報は、クラスタに対して格納され得る情報のタイプの例証である。

10

【0082】

図5の例において、複数のクラスタを有するシステムは、テーブル内に表され得、ここでは、各行は、1つのクラスタに関する情報を有する。情報は、それに対して情報が処理される特定の次元または特徴に対するクラスタの重心に関するデータを含み得る。図5の例において、「n」の次元または特徴が処理され、したがって、列1～nは、その特定の次元または特徴に対するクラスタに対する重心に関するデータを含む。集合的に、これらの列は、図5において列510として示されている。

【0083】

次のn列は、クラスタに属する全てのポイントにわたる全ての特徴の合計を提供する値を格納する。特に、下記により詳細に記載されるように、列520として表される列n+1～2nは、分析される次元または特徴の各々に対し、クラスタに対して特徴の合計を累積的に提供する。

20

【0084】

列530は、クラスタ内のポイントの数を提供する。換言すると、そのクラスタ内で分析されており格納されているデータポイントの数は、列530によって表される。

【0085】

列540は、クラスタ内のポイント間の近似の合計距離を提供する。換言すると、データポイント間の距離測定は、新規のデータポイントがクラスタに追加された際に、アップデートされ得る。

30

【0086】

図5のデータ構造または類似のデータ構造は、図6の実施形態にしたがってインクリメンタル重心クラスタリングアルゴリズムをトレーニングすることにおいて使用され得る。

【0087】

特に、図6のプロセスは、ブロック610から開始し、ブロック612に進み、そこでは、データポイントが選択される。当業者によって理解され得るように、データポイント選択は、オプションの中でもとりわけ、上記の図1～3に記載されているように、ログファイル内のラインを使用すること、データが作成された際にデータを処理すること、特徴ベクトルを使用することを伴い得る。いくつかの場合、データポイントは、センサ（例えば、車両センサ、または車両からのセンサのグループ）からのデータを表す。いくつかの場合、データポイントは、センサ、電子制御ユニット（ECU）、または処理されるべきその他のコンピューティングユニットから直接的に受信され得る。いくつかの場合、センサまたはECUからのデータは、ログファイル内に格納され得、事前に何らかの処理が実施され得る。その他のオプションも可能である。

40

【0088】

ブロック612から、プロセスはブロック620に進み、そこでは、ブロック612からの選択されたデータポイントが、インクリメンタル重心クラスタリングアルゴリズムに対する第1のデータポイントであるかどうかを決定するためのチェックがなされる。はいの場合、プロセスはブロック630に進み、そこでは、データポイントは、新規のクラスタに割り当てられる。特に、図5における列510に対する値は、アルゴリズムに渡され

50

るデータポイントに対して分析されている n 個の特徴または次元に対応する。

【0089】

さらに、列520は、処理されているデータポイントの n 個の特徴に対応する値でポピュレートされる。これは、次元内の特徴の合計が1つのデータポイントのみを有し得、したがって、合計が元の値となるからである。

【0090】

行530は、1の値を割り当てられ、単一のデータポイントを示している。

【0091】

列540は、0の値を割り当てられ、現在のところクラスタ内のデータポイント間で距離が存在しないことを示している。特に、1つのデータポイントのみが存在するので、データポイント間の距離は0である。

10

【0092】

図6を再び参照すると、ブロック630から、プロセスはブロック632に進み、そこでは、新規のクラスタがシステムのためのテーブルに追加される。

【0093】

逆に、ブロック620から、データポイントがシステムのための第1のデータポイントではない場合、プロセスはブロック640に進み、そこでは、データポイントがシステム内の任意の既存のクラスタのクラスタ中心までの平均距離の閾値内にあるかどうかを決定するためのチェックがなされる。

【0094】

クラスタ中心までの平均距離は、0から開始する。クラスタを構築することを開始するために、大域的変数（本明細書中では、「クラスタ距離」として参照される）が使用され得、これは、新規のポイントから最も近いクラスタまでの距離を監視する。第1のデータポイントを過ぎた各反復で、新規のデータポイントと最も近いクラスタとの間の距離が、0から開始して、この変数に追加される。

20

【0095】

第2の変数（本明細書中では「カウント」として参照される）は、システムに対してセーブされるデータポイントの総数を示し得る。

【0096】

ブロック640におけるチェックは、「閾値距離」に、「クラスタ距離」を「カウント」で割った値を乗じる。このように、「クラスタ距離」を「カウント」で割ったものは、最も近いクラスタまでの各ポイントの平均距離を表すことを意図される。これは、有用であり、なぜなら、「閾値距離」のハイパーパラメータに対する良好な選択を前もって決定することは困難であり得、クラスタが経時的により密になったりより密にならなかったりする場合、条件はよりフレキシブルになり得るからである。

30

【0097】

そのような大域的変数は、いくつかの場合、全てのトレーニングに対して使用され得る。その他の場合、大域的変数は、クラスタがその中に十分なポイントを持つまで、使用され得る。このことの後、ブロック640におけるチェックは、その後、「閾値距離」に、列540の値を列530におけるカウントで割った値を乗じる。特に、列540の値を列530の値で割ったものは、そのクラスタ中心までの各ポイントの平均距離を表すことを意図される。

40

【0098】

換言すると、ブロック640におけるチェックは、データポイントがそれらの最も近いクラスタまでのポイントの平均距離の閾値距離内にあるかどうかを見出す。

【0099】

いくつかの場合、閾値距離は、システムに割り当てられる値であり得、これは、下記に記載されるように、いくつかの場合においては調整され得る。さらに、いくつかの実施形態において、使用されている距離は、ユークリッド距離である。

【0100】

50

ブロック 6 4 0 において、データポイントがクラスタ中心までの平均距離の閾値内にないことが決定された場合、プロセスはブロック 6 3 0 に進み、そこでは、データポイントは、新規のクラスタに割り当てられ、その後、ブロック 6 3 2 に進み、そこでは、新規のクラスタがシステムに追加される。

【 0 1 0 1 】

逆に、ブロック 6 4 0 において、データポイントがクラスタ中心までの平均距離の閾値内にいることが決定された場合、プロセスはブロック 6 4 2 に進み、そこでは、データポイントは最も近いクラスタにマッピングされる。特に、マッピングは、図 7 の実施形態にしたがって行われ得る。

【 0 1 0 2 】

図 7 を参照すると、プロセスはブロック 7 1 0 において開始し、ブロック 7 2 0 に進み、そこでは、クラスタにマッピングされる新規のデータポイントに対する値が計算され、列 5 2 0 の特徴の合計に追加される。この新規の合計は、その後、列 5 2 0 に格納される。

【 0 1 0 3 】

プロセスは、次に、ブロック 7 3 0 に進み、そこでは、列 5 3 0 における値は、1 だけインクリメントされ、クラスタが現在、追加的データポイントを有していることを示している。

【 0 1 0 4 】

プロセスは次にブロック 7 4 0 に進み、そこでは、ブロック 7 2 0 において格納された特徴値の合計が、ブロック 7 3 0 において格納されたデータポイントの総数で割られる。これらの値は、その後、重心値として列 5 1 0 に格納される。

【 0 1 0 5 】

プロセスは、その後、ブロック 7 5 0 に進み、そこでは、新規のデータポイントの距離値が、以前のクラスタ中心に追加される。これらの値は、その後、ブロック 7 3 0 において格納されたデータポイントの総数で割られ、その後、クラスタ中心までの全てのポイントの間の平均距離に対する近似を作成するために平均化され、これはその後、列 5 4 0 に格納され得る。

【 0 1 0 6 】

図 6 を再び参照すると、クラスタを表す列は、それ故、ブロック 6 4 2 において新規のデータポイントでアップデートされ得る。

【 0 1 0 7 】

ブロック 6 3 2 から、新規のクラスタが追加されている場合、1 つのオプションの実施形態では、データポイントの総数と比較したときに、最大クラスタカウントが予め決定された閾値を超えるかどうかを見るために、チェックがなされ得る。特に、最大クラスタプロポーションを示す機械学習インクリメンタル重心クラスタリングアルゴリズムに対するハイパーパラメータが設定され得る。一実施形態において、クラスタの総数が処理されている総ポイントを下回る平方根の関数を超える場合、ブロック 6 5 0 におけるチェックは真となる。

【 0 1 0 8 】

ブロック 6 5 0 から、チェックが真である場合、プロセスはブロック 6 5 2 に進み、そこでは、クラスタの数が低減され得る。いくつかの場合、クラスタの数は、サイズ 1 の全てのクラスタを除去することによって低減され得る（なぜなら、これらは外れ値を示すからである）。

【 0 1 0 9 】

さらに、サイズ 1 を有するクラスタの数の将来的な成長を軽減するために、閾値距離を取り扱うハイパーパラメータは、増加され得る。特に、ブロック 6 4 0 におけるチェックのために使用される閾値距離は、データポイントがより長距離においてクラスタ内に配置されることを可能にするために、一定量だけ増加され得る。

【 0 1 1 0 】

10

20

30

40

50

閾値の増加は、いくつかの場合、例えば閾値調整ハイパーパラメータとして指定された予め設定された因子によるものであり得る。いくつかの場合、増加は、増加の列挙されたリストに基づき得る。いくつかの場合、増加は、データセットのサイズまたは処理されているデータポイントの数の何らかの関数に基づき得る。サイズの増加のためのその他のオプションも可能である。

【0111】

最大クラスタプロポーションを超えていない場合、ブロック642、652、またはブロック650から、プロセスはブロック660に進み、そこでは、より多くの処理されているデータポイントが存在するかどうかを決定するためのチェックがなされる。はいの場合、プロセスはブロック662に進み、そこでは、次のデータポイントが選択され、プロセスはその後、ブロック640に戻るよう進む。

10

【0112】

逆に、分析するためのさらなるデータポイントが存在しない場合、プロセスはブロック670に進み、終了する。

【0113】

したがって、図6のプロセスは、インクリメンタル重心クラスタリングアルゴリズムのためのトレーニングステップを示している。いったんトレーニングが完了すると、推論の間、データポイントが分析され得、それがモデル内の既存のクラスタのうちの任意のものの距離閾値内にある場合、クラスタに属することが見出され得る。この場合、データポイントは、良性と考えられ得る。逆に、データポイントがクラスタに属しない場合、それはアノマリー性と考えられ得る。

20

【0114】

図6および7のプロセスを利用すると、ディスク使用に関し、ディスクにセーブする必要があるコンポーネントはインクリメンタルモデルのみであり、インクリメンタル重心クラスタリングのためのその他のデータは格納される必要がない。

【0115】

さらに、インクリメンタル重心クラスタリングモデルは、一度に1つの記録を処理し得、そのピークリソース要件を実行可能な限り低く保ち得る。

【0116】

さらに、図6および7の実施形態は、全てのトレーニングおよび推論はエッジデバイス上で起こるので、クラウド接続性を必要としない。

30

【0117】

さらに、別個のモデルが、各エッジデバイスに対してトレーニングされ得る。

【0118】

例えば、図8を参照すると、3つのプロセスが示されており、エッジトレーニング802、エッジ再トレーニング804、およびエッジ推論806として参照されており、これらの全ては、エッジデバイスにおいて起こる。

【0119】

図8の例は、例示的なエッジデバイスとして、車両内インフォテインメントシステム（IVI）110を使用する。しかしながら、そのようなデバイスは、例証目的のために提供されているに過ぎず、本開示は、車両内インフォテインメントシステムに限定されない。

40

【0120】

IVI110は、システムログ112を作成し、システムログから、特徴114を工作する。

【0121】

そのような特徴は、ブロック116において、特徴ベクトルに変換される。このことは、エッジトレーニング802、エッジ再トレーニング804、およびエッジ推論806の全てに対して起こる。

【0122】

50

各記録は、その後、インクリメンタルに処理されるので、図 1 に示されている格納は必要とされない。その代わりに、特徴ベクトル 1 1 6 は、ブロック 8 1 0 に示されているようにモデルをトレーニングするために、または、ブロック 8 3 0 に示されているようにモデルをアップデートするために使用される。トレーニングまたはアップデートされたモデルは、フルバッチモデル 8 2 0 のために（図 5 のテーブルとして）格納され得る。

【0 1 2 3】

フルバッチモデル 8 2 0 は、その後、ブロック 8 4 0 に示されているように推論の間に使用され得、これはその後、出力 8 4 2 を生成し得る。

【0 1 2 4】

したがって、図 8 の実施形態にしたがって、フルバッチモデルの限定は軽減される。

【0 1 2 5】

さらに、エンドポイントが非常に類似した良性の挙動を有している可能性が高い場合、インクリメンタルモデルは、デバイスにフェデレートされ、モデルのアップデートが、そのエンドポイントの任意の挙動をテラリングするために適用され得る。モデルとして、さらなるカンマは、ゼロからトレーニングする必要がなく、それらは、観察される任意の新規の挙動で既存のモデルをアップデートし得る。

【0 1 2 6】

テスト

【0 1 2 7】

テストのために、図 9 の実施形態に示されているように、図 6 のプロセスは、3 次元の特徴を有する 8 個のクラスタを有するデータセットに対して使用された。特に、図 9 の実施形態は、8 個のクラスタをグレースケールで示しており、グラフ 9 1 0、グラフ 9 2 0、グラフ 9 3 0 は、3 つの軸のうちの 1 つに沿った回転を伴って示されている同じ 8 個のクラスタである。

【0 1 2 8】

テストケースにおいて、部分的に参照番号 9 4 0 で示されているクラスタ（クラスタ内のポイントは、「x」で示されている）は、アノマリー性挙動として指定され、残りの 7 個のクラスタは、良性挙動として指定された。したがって、図 6 のプロセスは、良性挙動に対するトレーニングモデルとして実行された。

【0 1 2 9】

推論プロセスは、その後、残りのデータポイントに対して実行された。この場合、図 1 0 のグラフが作成され、グラフ 1 0 1 0、1 0 2 0、および 1 0 3 0 は、異なる次元の軸のうちの 1 つに沿って回転された同じクラスタを示している。特に、図 1 0 において見られるように、多くのオーバーラップしているクラスタは、良性のアクティビティをカバーしているが、視覚的に、「x」のシンボルで示され、一般的に参照番号 1 0 4 0 で指定されているアノマリー性の挙動は、ほとんど触れられていない。

【0 1 3 0】

プロセスは、図 1 1 に関して示されているもののよう、混同行列に基づいて評価され得る。特に、図 1 1 に見られるように、行列は、予測結果と実際の結果とを比較している。データポイントに対する予測値と実際の値との両方が、データポイントが良性であることである場合、これは、真陽性 1 1 1 0 として分類される。

【0 1 3 1】

予測が、データポイントがアノマリー性であることであるが、データポイントに対する実際の値が、データポイントが良性であることである場合、これは、偽陰性 1 1 2 0 として分類される。

【0 1 3 2】

予測が、データポイントが良性であることであるが、データポイントに対する実際の値が、データポイントがアノマリー性であることである場合、これは、偽陽性 1 1 3 0 として分類される。

【0 1 3 3】

10

20

30

40

50

データポイントに対する予測値および実際の値の両方が、データポイントがアノマリー性であることである場合、これは、真陰性 1 1 4 0 として分類される。

【 0 1 3 4 】

図 1 1 の混同行列に基づいて、システムのゴールは、真陽性 1 1 1 0 および真陰性 1 1 4 0 の値を最大化し、その一方で偽陰性 1 1 2 0 および偽陽性 1 1 3 0 を最小化することである。

【 0 1 3 5 】

図 5 および 6 の例に対し、混同行列は、以下のものであることが見出された。

【表 1】

	数
真陽性	375
偽陰性	2
偽陽性	3
真陰性	30

表 1: テストケースに対する混同行列

10

【 0 1 3 6 】

それ故、表 1 から、良性データポイントに対する精度は、99.2% であり、アノマリー性データポイントに対する精度は、93.3% であった。

20

【 0 1 3 7 】

さらに、テストの再現率、特に、全陽性のうち何パーセントが陽性と予測されるかは、良性データポイントに対しては 99.5% であり、アノマリー性データポイントに対しては 90.9% である。

【 0 1 3 8 】

テストの F1 スコアは、偽陽性および偽陰性の両方を考慮し、精度および再現率の調和平均である。これは、以下の式 1 のように表され得る。

【化 1】

$$F1\ score = \frac{2}{\frac{1}{Precision} + \frac{1}{Recall}} \quad (1)$$

30

【 0 1 3 9 】

良性データポイントに対する F1 スコアは、99.3 であり、アノマリー性データポイントに対しては 92.3 である。

【 0 1 4 0 】

したがって、テストの一般的な精度は、98.8% であり、調和 F1 スコアは、95.7 であり、分類有効性が高かったことを示す。

40

【 0 1 4 1 】

それ故、モデルは、限定された格納および／処理を有するコンピューティングデバイス上で、高い有効性で使用され得る。必要とされる格納は、複数のクラスタに対するテーブルに関するもののみである。特に、格納されるデータは、最大で処理されたポイントの数の平方根の関数であるクラスタのみである、または、各クラスタは、プロセスが機能するための全ての情報を含む単一のベクトルを含有する。

【 0 1 4 2 】

クラスタプロポーションが閾値を超えたときにクラスタの数を減らすことによって、そしてその後、使用される距離閾値のサイズを増加させることによって、処理が支援され得る。これは、アルゴリズムのパラメータをチューニングすることをさらに支援する。

50

【0143】

プロセスは、インクリメンタルであり、クラスタリングを実施するために全てのデータを必要とはしない。特に、方法は、一度の1つのデータポイントをクラスタリングし得る。

【0144】

比較

【0145】

テストにおいて、本開示のインクリメンタル重心クラスタリングの有効性は、テストされるフルバッチアルゴリズムの最良に近いが、またはそれよりも良好であることが見出された。

【0146】

特に、上述のものに対するさらなるテストにおいて、インクリメンタル重心クラスタリングモデルは、One Class SVMモデルに対してテストされた。同じトレーニングデータ、検証データ、およびテストデータが使用された。トレーニングデータは、各モデルをトレーニングするために使用された。検証データは、アノマリー検出の適切な分離をもたらしたハイパーパラメータの最良の選択を見出すために使用され、テストデータは、結果を比較するために使用された。

【0147】

One class SVMモデルに対し、以下のハイパーパラメータがチューニングされた。

【表2】

ハイパーパラメータ	値
カーネル(使用されるカーネルタイプを特定する)	['linear', 'poly', 'rbf', 'sigmoid']
ディグリー(選択された場合の多項式カーネルのディグリー)	[3, 4, 5]
Nu (コンタミネーション因子として考えられ得る)	[0.001, 0.01, 0.05, 0.1, 0.2, 0.3, 0.4, 0.5]
ガンマ('rbf', 'poly'および'sigmoid'に対するカーネル係数)	['scale', 'auto']
Tol (停止基準に対するトレランス)	[1e-2, 1e-3, 1e-4]

表2:One Class SVMに対するハイパーパラメータ

【0148】

インクリメンタル重心クラスタリングに対し、以下のハイパーパラメータがチューニングされた。

【表 3】

ハイパーパラメータ	値
閾値(そのクラス内の全てのポイントの間の平均距離に比例する重心からの距離)	[0.3, 0.5, 0.7, 1]
最大のクラスアップロケーション(クラスが処理された総ポイントを下回る平方根の関数のままであることを保証する)	[0.5, 0.6, 0.7, 0.75, 0.8, 0.85]
閾値調整(クラスの数最大のクラスアップローションを超えたとき、閾値をどれだけ増加させるべきか)	[1.05, 1.1, 1.15, 1.2, 1.3, 1.4, 1.5]
距離閾値(いったんクラスが定義されると、クラスに属するポイントが重心からどれだけ離れ得るかを予測することが所望される)	[1.5, 1.8, 2.0, 2.2, 2.5]

表3:インクリメンタル重心クラスタリングに対するハイパーパラメータ

【0149】

ハイパーパラメータを変動させて複数回テストを実行したところ、ガンマを ‘ s c a l e ’ に設定し、トレランスは「取るに足らない」であったとし、Nuを0.001に設定したRBFカーネルに対し、One Class SVMに対するデータセットに対して最高の性能が見出された。ハイパーパラメータのこの設定に対し、以下の混同行列が見出された。

【表 4】

	数
真陽性	344
偽陰性	3
偽陽性	12
真陰性	18

表4:One Class SVMに対する混同行列

【0150】

上記から、良性データに対する精度は、96.6であり、アノマリー性データに対する精度は、85.7であった。良性データに対する再現率は、99.1であり、アノマリー性データに対する再現率は、60.0であった。良性データに対するF1スコアは、97.9であり、アノマリー性データに対するF1スコアは、70.6であった。

【0151】

全体として、One Class SVMに対する精度は、96.0であり、調和F1は82.0であり、曲線下面積（AUC）は、79.6であった。

【0152】

同様に、ハイパーパラメータを変動させてテストを複数回実施したところ、閾値が過度

10

20

30

40

50

に低く（0.3）、クラスタプロポーションが過度に高い（> 0.8）場合、モデルは悪化した。このモデルに対し、以下の混同行列が見出された。

【表 5】

	数
真陽性	345
偽陰性	2
偽陽性	5
真陰性	25

表5:インクリメンタル重心クラスタリングに対する混同行列

10

【0153】

上記から、良性データに対する予測は、98.6であり、アノマリー性データに対する予測は、92.6であった。良性データに対する再現率は、99.4であり、アノマリー性データに対する再現率は、83.3であった。良性データに対するF1スコアは、99.0であり、アノマリー性データに対するF1スコアは、87.7であった。

【0154】

全体として、インクリメンタル重心クラスタリングの精度は、98.1であり、調和F1は93.0であり、AUCは91.46であった。

20

【0155】

これらの結果に基づくと、インクリメンタル重心クラスタリングモデルをチューニングした後、適合がOne Class SVMよりもより正確になった。さらに、インクリメンタル重心クラスタリングは、One Class SVMモデルよりもより迅速に実行することが見出された。

【0156】

アノマリー検出の使用

【0157】

実際には、アノマリー検出の使用は、エッジデバイス、サーバ、クラウド、および／またはその他のコンピューティングデバイスのいずれかで様々なアクションを実施するために行われ得る。特に、ここで図12に対する参照がなされる。

30

【0158】

図12の実施形態は、ブロック1210において開始し、ブロック1212に進み、ここでは、アノマリー検出が実施される。この場合、実施されるアノマリー検出は、上述された図6および7の実施形態において作成されるフルバッチモデルを使用し得る。新規のデータポイントが、その後、例えばログファイルから受信され、これは、ハードウェアセンサからの入力に基づいて作成され得るか、または、いくつかの場合においては、ソフトウェアプロセッサに基づいて作成され得る。

40

【0159】

新規のデータポイントは、ポイントがフルバッチモデル内の任意の既存のクラスタから距離閾値にあるかどうかを決定することにより、それがフルバッチモデルに入るかどうかを決定するためにチェックされ得る。はいの場合、データポイントは、良性データポイントであると考えられる。いいえの場合、データポイントは、アノマリー性データポイントであると考えられる。このことは、オプションの中でもとりわけ、ログファイルコンテンツに基づいて、データポイントが作成されるたびに繰り返される。

【0160】

いったんアノマリー検出が実施されると（または、それが連続的な分析を実施するシステム内で実施されると）、プロセスはブロック1220に進み、ここでは、何らかのアノ

50

マリーが処理されているデータ内で見出されたかどうかを決定するためのチェックがなされる。いいえの場合、プロセスはブロック1212に進み、アノマリー検出を実施することを継続し得る。

【0161】

逆に、アノマリーがブロック1220において見出された場合、プロセスはブロック1230に進み得、そこでは、アクションが実施され得る。実施されるアクションは、エッジデバイスが展開されるアプリケーションのタイプに特有であり得る。例えば、車両システムにおいて、アノマリーが検出された場合、1つの可能性のあるアクションは、車両のドライバにアラートを提供することであり得る。例えば、アラートは、オプションの中でもとりわけ、インフォテイメントシステム上、車両のダッシュボード上のメッセージ、ドライバへのオーディオアラート、ステアリングホイールに対するハプティックフィードバックを含み得る。アラートは、オプションの中でもとりわけ、ドライバが車両を整備すべき、車両を停めて運転をやめるべき、製造業者またはディーラーに連絡すべき、システムをリセットすべき等を示し得る。

10

【0162】

その他の場合、アクションは、ドライバではなく、第三者に対するアラートであり得る。そのようなアラートは、オプションの中でもとりわけ、車両の製造業者、ディーラー、フリートオペレータ、企業IT部門等に送信され得る。アラートは、そのような情報の中でもとりわけ、アノマリーを引き起こしたデータ、アノマリーの周辺のコンテキスト、その他の車両センサ読み取り値等を含み得る。このことは、第三者が、車両に関する決定（例えば、そのようなアクションの中でもとりわけ、車両を整備させるべきかどうか、車両を道路から除去するかどうか、車両上のソフトウェアをリセットするかどうか、ソフトウェアアップデートが車両にプッシュされるべきかどうか等）を行うことを可能にする。

20

【0163】

いくつかの場合、アクションは、車両自体がアクションを自動的に行うことを伴い得る。例えば、そのようなアクションの中でもとりわけ、車両は、車両が自律機能性を有している場合に停まり得、車両はいくつかの場合においてアノマリー性センサ読み取り値を無視し得、車両はいくつかの場合において速度が限定され得る。

【0164】

非車両シチュエーションに対し、アクションは同様に、アノマリー性データ検出に基づいて、ユーザ、第三者にアラートすること、または、エッジデバイス上の何らかの機能性を実施することを含み得る。

30

【0165】

いくつかの場合、アクションは、モデルを再トレーニングすることにおいて、新規のデータポイントを使用するためのものであり得る。

【0166】

本開示は、アノマリーの検出に基づいて実施され得る任意の特定のアクションに限定されることを意図されるものではなく、上記の例は、例証のみのために提供されている。

【0167】

コンピューティングデバイス

40

【0168】

上記のドメイン、ネットワーク要素、IoTまたはエッジデバイス、クラウドサービス、ノード、およびその他のコンピューティングプラットフォームは、任意のコンピューティングデバイスを使用して実装され得る。コンピューティングデバイスの1つの簡略図が、図13に関して示されている。図13のコンピューティングデバイスは、任意の固定コンピューティングデバイスまたはモバイルコンピューティングデバイスであり得る。

【0169】

図13において、デバイス1310は、プロセッサ1320および通信サブシステム1330を含み、プロセッサ1320および通信サブシステム1330は、上述された実施形態の方法を実施するために協働する。通信サブシステム1330は、デバイス1310

50

がその他のデバイスまたはネットワーク要素と通信することを可能にし、実施される通信のタイプに基づいて変動し得る。さらに、通信サブシステム 1330 は、複数の通信技術（任意の有線または無線通信技術を含む）を含み得る。

【0170】

プロセッサ 1320 は、プログラム可能論理を実行するように構成され、これは、データとともにデバイス 1310 上に格納され得、図 13 の例ではメモリ 1332 として示されている。メモリ 1332 は、命令コードを格納する任意の有形、非一過性のコンピュータ読み取り可能な格納媒体であり得、上記命令は、プロセッサ 1320 によって実行されると、デバイス 1310 に、本開示の方法を実施させる。コンピュータ読み取り可能な格納媒体は、例えば光学（例えば、CD、DVD 等）、磁気（例えば、テープ）、フラッシュ

10

【0171】

代替的に、またはメモリ 1332 に加えて、デバイス 1310 は、例えば通信サブシステム 1330 を通して、外部格納媒体からデータまたはプログラム可能論理にアクセスし得る。

【0172】

図 13 の例において、1つ以上のセンサ 1340 は、コンピューティングデバイスと関連付けられ得る。しかしながら、これは、オプションであり、いくつかの場合、コンピューティングデバイス 1310 は、センサとは関連付けられていない可能性がある。

20

【0173】

デバイス 1310 の様々な要素間の通信は、1つの実施形態では、内部バス 1360 を通じたものであり得る。しかしながら、その他の形式の通信も可能である。

【0174】

本明細書中に記載されている実施形態は、本願の技術の要素に対応する要素を有している構造、システム、方法の例である。本明細書の記載は、当業者が本願の技術の要素に対応する代替的な要素を有する実施形態を構成および使用することを可能にし得る。本願の技術の意図された範囲は、それ故、本明細書に記載された本願の技術とは異ならないその他の構造、システムまたは方法を含み、本明細書に記載された本願の技術からの非実質的な差異を有するその他の構造、システムまたは方法をさらに含む。

30

【0175】

動作は、特定の順序で図面に描写されているが、これは、所望の結果を達成するために、そのような動作が示されている特定の順序または連続的順序で実施されるべきであること、または、全ての例証されている動作が実施されるべきであることを必要としているとして理解されるべきではない。或る状況において、マルチタスク処理および並列処理が、採用され得る。さらに、上述された実装における様々なシステムコンポーネントの分離は、全ての実装においてそのような分離を必要としているとして理解されるべきではなく、記載されたプログラムコンポーネントおよびシステムは、概して、単一のソフトウェア製品内に一緒に統合され得るか、または、複数のソフトウェア製品にパッケージ化され得ることが理解されるべきである。

40

【0176】

また、離散的または分離的であるとして様々な実装において記載され、例証された技術、システム、サブシステム、および方法は、その他のシステム、モジュール、技術、または方法と組み合わせられ得るか、または統合され得る。相互に結合されるかまたは直接的に結合されるかまたは通信するとして示されるかまたは議論されたその他のアイテムは、電氣的、機械的、またはその他に関わらず、いくつかのインターフェース、デバイス、または中間コンポーネントを通して間接的に結合され得るかまたは通信し得る。その他の変更、置換、および代替は、当業者によって確かめられることができ、構成され得る。

【0177】

上記の詳細な記載は、様々な実装に適用されるものとして本開示の基本的な新規な特徴

50

を示し、記載し、指摘してきたが、例証されたシステムの形式および詳細における様々な省略、置換、および変更が、当業者によってなされ得ることが理解され得る。加えて、方法ステップの順序は、それらが特許請求の範囲内に現れる順序によって示唆されてはいない。

【0178】

メッセージが電子デバイスに送信される／電子デバイスから送信されるとき、そのような動作は、即時的なものまたはサーバから直接的なものではない可能性がある。それらは、本明細書に記載されるデバイス／方法／システムをサポートするサーバまたはその他のコンピューティングシステムインフラストラクチャから、同期的または非同期的に送達され得る。上述のステップは、全体的または部分的に、デバイス／インフラストラクチャに対する／デバイス／インフラストラクチャからの同期的／非同期的通信を含み得る。さらに、電子デバイスからの通信は、ネットワーク上の1つ以上のエンドポイントに対するものであり得る。これらのエンドポイントは、例えばサーバ、分散コンピューティングシステム、ストリームプロセッサ等によってサービス提供され得る。また、コンテンツ配信ネットワーク（CDN）は、電子デバイスに通信を提供し得る。例えば、典型的なサーバ応答とは異なり、サーバは、コンテンツ配信ネットワーク（CDN）に対するデータを提供するかまたは示し得、例えば電子デバイスの後続のアクティビティ等の後の時間における電子デバイスによるダウンロードを待機し得る。それ故、データは、サーバから直接的に送信され得るか、または、システムの一部として、またはシステムとは別個に、その他のインフラストラクチャ（例えば、分散インフラストラクチャまたはCDN等）から送信され得る。

10

20

【0179】

典型的には、格納媒体は、半導体メモリデバイス（例えば、ダイナミックまたはスタティックランダムアクセスメモリ（DRAMまたはSRAM）、消去可能およびプログラム可能リードオンリーメモリ（EPROM）、電氣的消去可能およびプログラム可能リードオンリーメモリ（EEPROM）、およびフラッシュメモリ等）、磁気ディスク（例えば、固定ディスク、フロッピー（登録商標）ディスク、リムーバブルディスク等）、テープを含む別の磁気媒体、光学媒体（例えば、コンパクトディスク（CD）またはデジタルビデオディスク（DVD）等）、または別のタイプの格納デバイスのうちの任意のまたはいくつかの組み合わせを含み得る。上述された命令は、1つのコンピュータ読み取り可能または機械読み取り可能な格納媒体上に提供され得、または、代替的に、複数のノードを有している可能性がある大きなシステム内に分散された複数のコンピュータ読み取り可能または機械読み取り可能な格納媒体上に提供され得る。そのようなコンピュータ読み取り可能または機械読み取り可能な格納媒体または複数のコンピュータ読み取り可能または機械読み取り可能な格納媒体は、品物（または製品）の一部であると考えられる。品物または製品は、任意の製造された単一のコンポーネントまたは複数のコンポーネントを参照し得る。格納媒体または複数の格納媒体は、機械読み取り可能な命令を実行する機械内に配置され得るか、または、そこから機械読み取り可能な命令が実行のためにネットワークにわたってダウンロードされ得る遠隔サイトに配置され得る。

30

【0180】

上述の記載では、多数の詳細が本明細書中に開示された対象の理解を提供するために述べられている。しかしながら、実装は、これらの詳細のうちのいくつかを伴わずに実践され得る。その他の実装は、上述された詳細からの改変またはバリエーションを含み得る。添付の特許請求の範囲は、そのような改変およびバリエーションをカバーすることが意図されている。

40

【図面】
【図 1】

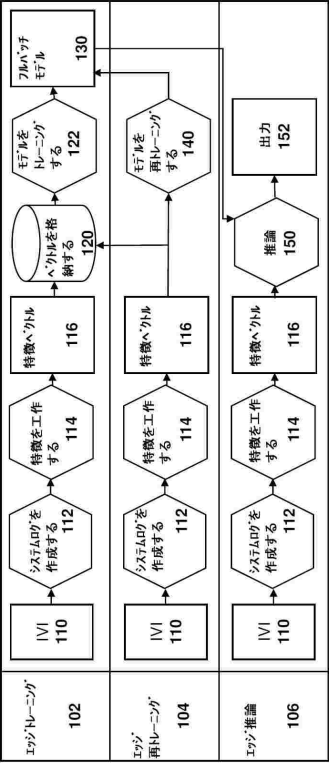


FIG. 1

【図 2】

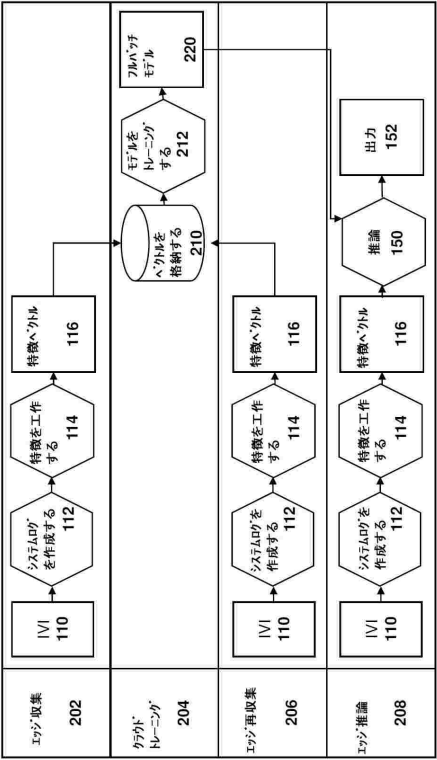


FIG. 2

【図 3】

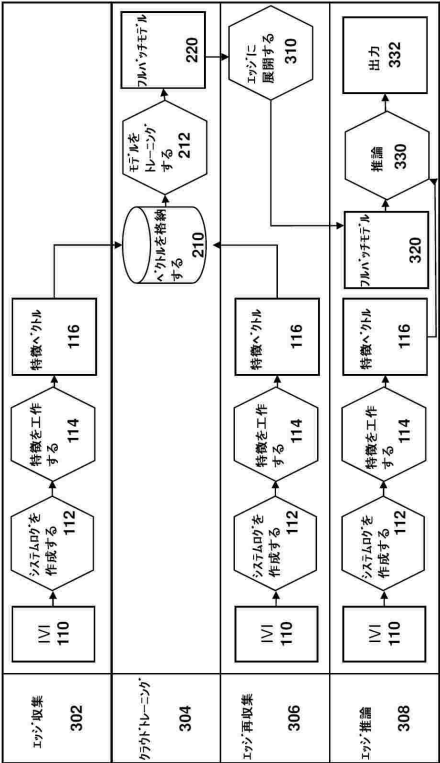


FIG. 3

【図 4】

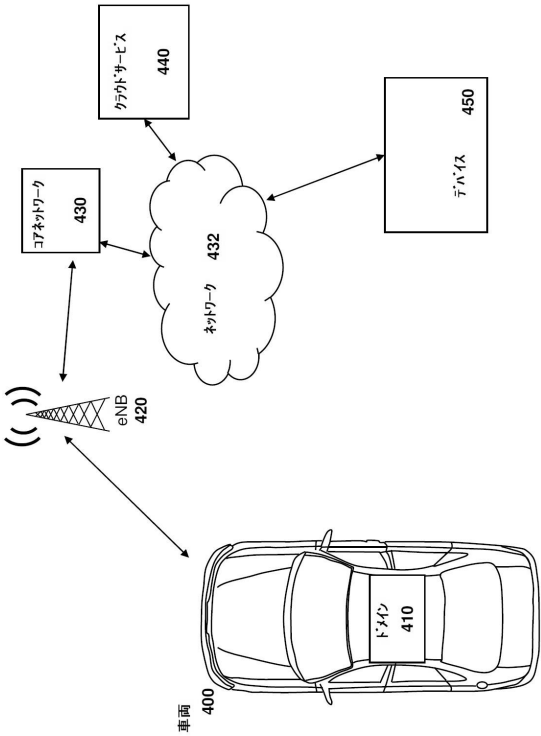


FIG. 4

10

20

30

40

50

【図 5】

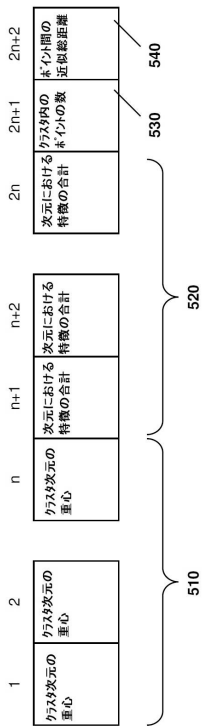


FIG. 5

【図 6】

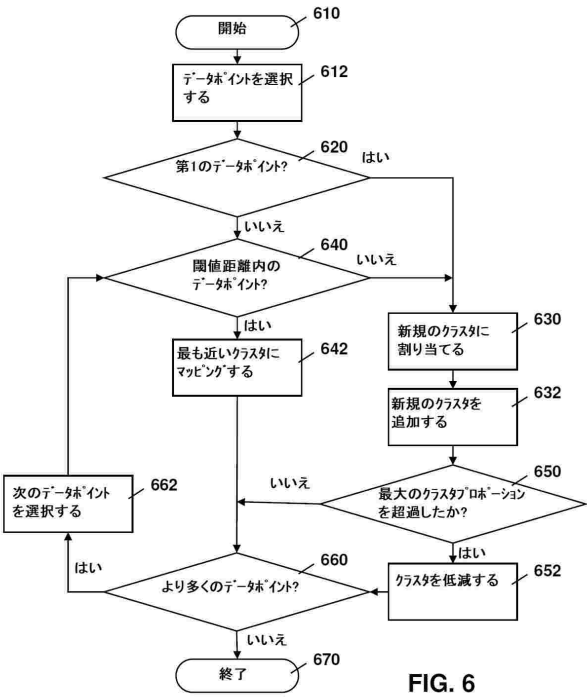


FIG. 6

【図 7】

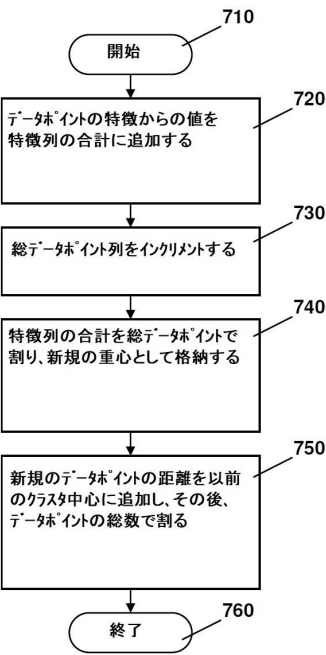


FIG. 7

【図 8】

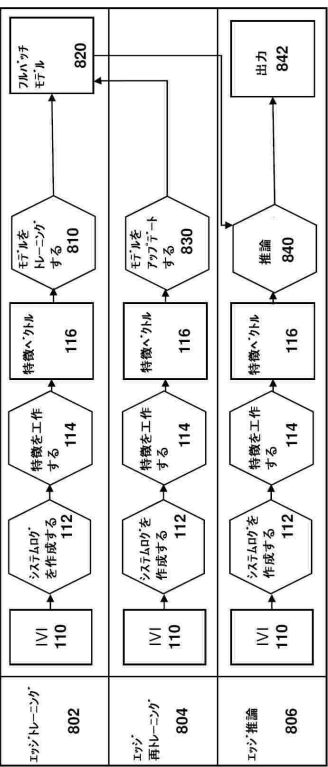


FIG. 8

【図 9】

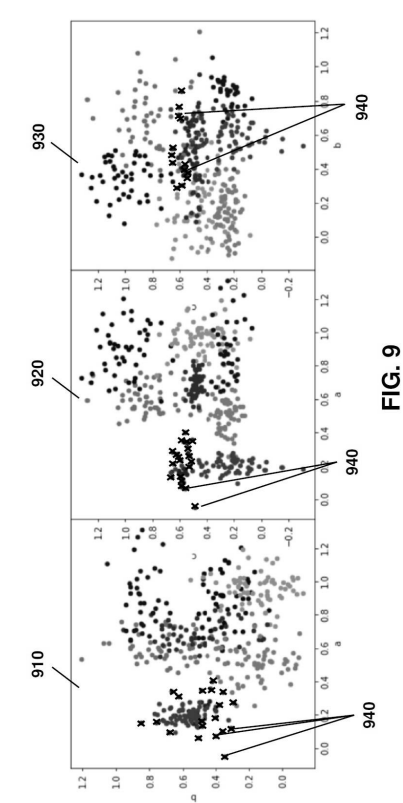


FIG. 9

【図 10】

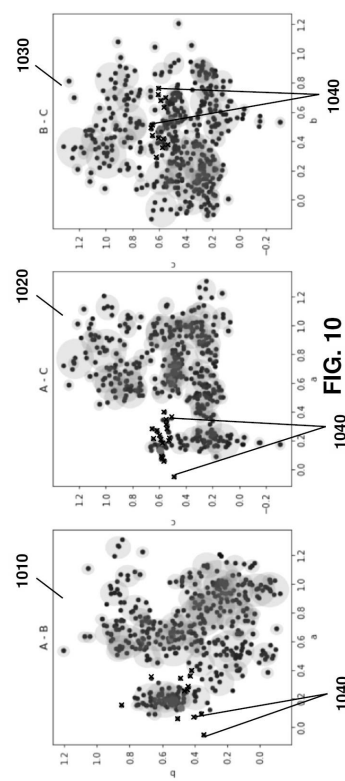


FIG. 10

【図 11】

		予測	
		良性	アノマリー性
実際	良性	真陽性 1110	偽陰性 1120
	アノマリー性	偽陽性 1130	真陰性 1140

FIG. 11

【図 12】

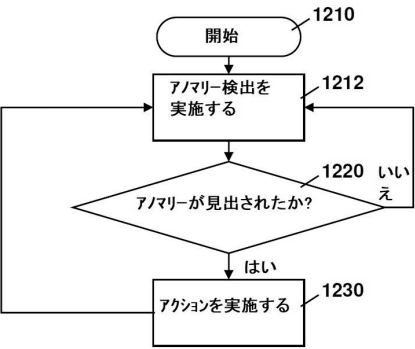


FIG. 12

10

20

30

40

50

【図 13】

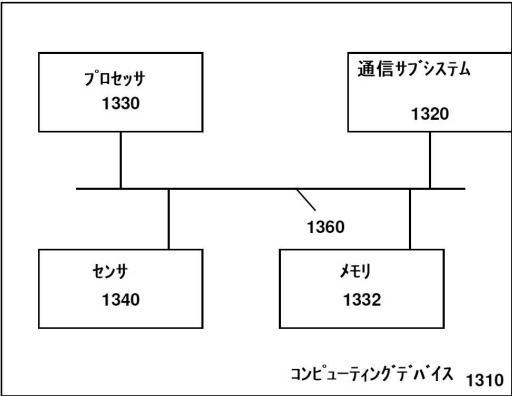


FIG. 13

10

20

30

40

50