(19) Österreichisches Patentamt

(10) **AT 522276 B1 2021-01-15**

(12) **Patentschrift**

(21) Anmeldenummer: A 50291/2019
(22) Anmeldetag: 03.04.2019
(45) Veröffentlicht am: 15.01.2021

(51) Int. Cl.: ***G06F 21/64*** (2013.01)
H04L 9/32 (2006.01)

(56) Entgegenhaltungen:
US 2005235154 A1
EP 2437186 A1
WO 2019020194 A1
US 2015189005 A1
US 2019044726 A1

(73) Patentinhaber:
Tributech Solutions GmbH
4020 Linz (AT)

(74) Vertreter:
Hübscher & Partner Patentanwälte GmbH
4020 Linz (AT)

(54) Vorrichtung und Verfahren zur Integritätsprüfung von Sensordatenströmen

(57) Es wird ein Verfahren zur Integritätsprüfung von Sensordatenströmen (15) beschrieben. Damit auch einzelne Sensordatenstromabschnitte (11, 12, 13, 14) eines Sensordatenstromes (15) unabhängig von einer Weiterverarbeitung in bestehenden Infrastrukturen (26), insbesondere im Falle einer Übertragung über mehrere Infrastrukturknoten hinweg bei geringem Ressourcenverbrauch auf ihre Integrität überprüft werden können, wird vorgeschlagen, dass für einzelne Sensordatenstromabschnitte (11, 12, 13, 14) eines Sensordatenstromes (15) Hashwerte berechnet und in den Speicherbereichen (7, 8, 9, 10) der untersten Ebene eines Hashbaumspeichers (5) mit vorgegebener Struktur gespeichert werden, wobei bei Verfügbarkeit aller einem Elternspeicherbereich (16, 17, 18) unmittelbar untergeordneter Hashwerte aus diesen ein übergeordneter Hashwert berechnet und im Elternspeicherbereich (16, 17, 18) abgelegt wird, wonach die dem Elternspeicherbereich (16, 17, 18) untergeordneten Hashwerte gelöscht werden.

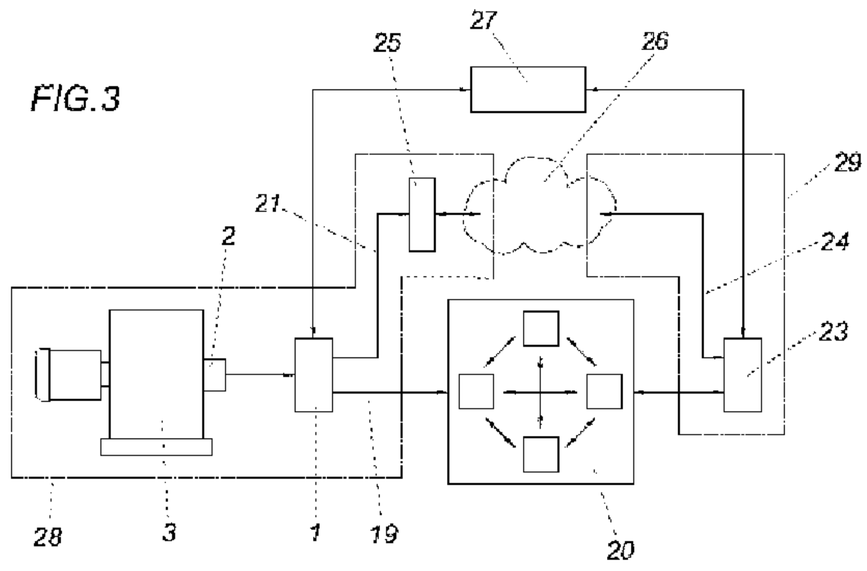

FIG.3

AT 522276 B1 2021-01-15

Beschreibung

[0001] Die Erfindung bezieht sich auf ein Verfahren zur Integritätsprüfung von Sensordatenströmen sowie auf eine Vorrichtung zur Durchführung eines solchen Verfahrens.

[0002] Zur Integritätsprüfung von Sensordaten, also zur Überprüfung des korrekten Inhaltes, des unmodifizierten Zustandes und der temporalen Korrektheit der Sensordaten wird herkömmlicherweise eine Verschlüsselung bzw. ein Transport über sichere Umgebungen eingesetzt (US 20130243189 A1) um zu verhindern, dass die Sensordaten während der Übertragung manipuliert werden können. Nachteilig ist daran allerdings, dass solche Verschlüsselungsverfahren nicht nur ressourcenaufwändig sind, sondern dass die vorliegenden Sensordaten auch nicht mehr im Klartext in bestehenden Infrastrukturen weiterverarbeitet werden können, was den Einsatz gerade im Bereich der Überwachung und Steuerung von Fahrzeugkomponenten oder Industriemaschinen erschwert.

[0003] Zur Absicherung der verwendeten Verschlüsselungsparameter sowie zur Beschleunigung der Verarbeitungsprozesse wurde zudem bereits vorgeschlagen (WO 2016049077 A1), Trusted Platform Module (TPM) einzusetzen.

[0004] Darüber hinaus sind aus der US 2005235154 A1 sind Verfahren zum Authentifizieren sowie Schützen der Integrität elektronischer Informationen unter Verwendung kryptographischer Techniken bekannt. Weiters offenbart die EP 2437186 A1 Verfahren zum Erzeugen sowie zum Auswerten eines sicheren Bilddatensatzes. Dabei werden zunächst digitale Bilddaten sowie dazugehörige Zusatzinformationen, wie z.B. Umgebungsinformationen, empfangen, wonach ein Datenobjekt erzeugt wird, das die Bilddaten mitsamt den Zusatzinformationen umfasst. Eine Auswertung der wenigstens einen Zusatzinformation der Bilddaten ermöglicht eine Plausibilitätsprüfung derselben. Zudem wird ein dem erzeugten Datenobjekt zugeordneter Zeitstempel empfangen und schließlich das Datenobjekt mit dem zugeordneten Zeitstempel in einer Datenbank gespeichert.

[0005] Ferner offenbart die WO 2019020194 A1 insbesondere im Zusammenhang mit Content Delivery Netzwerken (CDN) Verfahren zum Verifizieren von Inhalten, wie beispielsweise Live-Videostreams. Dabei werden zu jedem Teilinhalt und den jeweils dazugehörigen Metadaten Hashes erzeugt, die wiederum zu übergeordneten Hashes kombiniert werden. Die dadurch erhaltenen, verifizierten Hashwerte dienen zur Verifizierung untergeordneter Hashes dienen, indem diese mit Referenzhashwerten verglichen werden.

[0006] Nachteilig an allen bekannten Vorrichtungen und Verfahren ist allerdings, dass durch die Absicherung per Verschlüsselung der Sensordatenströme ein Eingriff in die bestehende Übertragungsinfrastruktur vorgenommen werden muss und dass die eingesetzten kryptographischen Funktionen nicht zuletzt aus Sicherheitsgründen so aufwändig sind, dass sie bei eingebetteten Systemen geringer Leistung, die eine umfassende Verteilung zur Aufnahme vieler verschiedener Sensordatenströme mit unterschiedlichen Taktfrequenzen ermöglichen würden, nicht die erforderlichen Verarbeitungsraten erreichen.

[0007] Dazu kommt, dass gerade bei Sensordatenströmen nicht nur die Integritätsprüfung einzelner Sensordatenstromabschnitte in Form von Datenpaketen, sondern auch die Integritätsprüfung der Sensordatenstromabschnitte in Bezug auf den Sensordatenstrom ermöglicht werden soll, sodass überprüft werden kann, ob ein Sensordatenstromabschnitt tatsächlich an der angegebenen Position eines Sensordatenstromes aufgetreten, keine Sensordatenstromabschnitte vorher oder nachher hinzugefügt oder weggelassen und die Daten des Sensordatenstromabschnittes selbst nicht verändert worden sind.

[0008] Der Erfindung liegt somit die Aufgabe zugrunde, eine Vorrichtung und ein Verfahren der eingangs beschriebener Art so auszugestalten, dass auch einzelne Sensordatenstromabschnitte eines Sensordatenstromes unabhängig von einer Weiterverarbeitung in bestehenden Infrastrukturen, insbesondere im Falle einer Übertragung über mehrere Infrastrukturknoten hinweg bei geringem Ressourcenverbrauch auf ihre Integrität überprüft werden können.

[0009] Die Erfindung löst die gestellte Aufgabe dadurch, dass für einzelne Sensordatenstromabschnitte eines Sensordatenstromes Hashwerte berechnet und in den Speicherbereichen der untersten Ebene eines Hashbaumspeichers mit vorgegebener Struktur gespeichert werden, wobei bei Verfügbarkeit aller einem Elternspeicherbereich unmittelbar untergeordneter Hashwerte aus diesen ein übergeordneter Hashwert berechnet und im Elternspeicherbereich abgelegt wird, wonach die dem Elternspeicherbereich untergeordneten Hashwerte gelöscht werden. Zufolge dieser Maßnahmen können für einzelne Sensordatenstromabschnitte des Sensordatenstromes Hashwerte berechnet und in den Speicherbereichen der untersten Ebene eines Hashbaumspeichers mit vorgegebener Struktur, beispielweise in Form eines einfachen Binärbaumes abgespeichert werden. Bei Verfügbarkeit aller einem Elternspeicherbereich unmittelbar untergeordneter Hashwerte kann sodann aus diesen ein übergeordneter Hashwert berechnet und im Elternspeicherbereich abgelegt werden, wonach die untergeordneten Hashwerte nicht mehr benötigt werden und damit für einen geringen Speicherverbrauch gelöscht werden können. Während des Betriebes ist es somit nicht erforderlich, alle Hashwerte eines Hashbaumes im Hashbaumspeicher zu halten, sondern nur jeweils jene, die zur Berechnung eines übergeordneten Hashwertes im Hashbaum erforderlich sind. Wurde auf diese Weise der Wurzelhashwert eines Hashbaumes vorgegebener Struktur berechnet, kann dieser über den Wurzelhashausgang ausgegeben und danach aus dem Hashbaumspeicher gelöscht werden. Auf diese Weise kann die Taktfrequenz bzw. Datenrate des zu erfassenden Sensordatenstromes durch Anpassung insbesondere der Tiefe des Hashbaumes auch bei geringer Leistung der Steuereinrichtung erreicht werden. Beispielsweise konnten bei einem binären Hashbaum bei einer Tiefe von 1 - 10 Ebenen Sensordatenströme mit einfachen Zahlenwerten mit Taktfrequenzen von 1 Hz erfasst werden, während bei einer Tiefe von 10 - 27 Ebenen Taktfrequenzen von bis zu 50.000 Hz erfasst werden konnten. Schließlich muss erfindungsgemäß für den Fall, dass aufeinanderfolgende Wurzelhashwerte aus zeitlich aufeinanderfolgenden und sich nicht überschneidenden Sensordatenstromabschnitten gebildet werden, zu keinem Zeitpunkt der gesamte Hashbaumspeicher genutzt werden, sodass die Größe des Speichers entsprechend gering ausfallen kann, was auch die Zugriffszeiten auf einen solchen Speicher reduziert. Nimmt man einen größeren Speicherbereich in Kauf, ergibt sich der weitere Vorteil, dass die Berechnung der Hashwerte für einen nachfolgenden Sensordatenstromabschnitt bereits gestartet werden kann, während die Hashwerte des vorangegangenen Sensordatenstromabschnittes zwar noch nicht abgeschlossen ist, aber die tieferen Ebenen des Hashbaumspeichers nicht mehr belegt werden.

[0010] Das erfindungsgemäße Verfahren wird solange wiederholt, bis ein Wurzelhashwert des Hashbaumes berechnet wurde, der zur Überprüfung ausgegeben werden kann. Zur Integritätsprüfung des Sensordatenstromes wird das gesamte Verfahren wiederholt und der resultierende Prüfwurzelhashwert mit dem ursprünglich ausgegebenen Wurzelhashwert verglichen. Stimmen Prüfwurzelhashwert und ursprünglich ausgegebener Wurzelhashwert überein, ist die Integritätsprüfung erfolgreich, stimmen Prüfwurzelhashwert und ursprünglich ausgegebener Wurzelhashwert nicht überein, schlägt die Integritätsprüfung fehl.

[0011] Damit über einen längeren Zeitraum auftretende, gleichbleibende Sensordaten nicht zu vorhersehbaren Wurzelhashwerten führen können, wird vorgeschlagen, dass die einzelnen Sensordatenstromabschnitte mit einem Zeitstempel versehen werden, der bei der Berechnung des Hashwertes berücksichtigt wird.

[0012] Wie bereits erwähnt, kann jeder neu berechnete Wurzelhashwert eines Hashbaumes mit einer die Erfassungseinheit identifizierenden elektronischen Signatur versehen werden, was neben einer Integritätsprüfung der Sensordatenabschnitte auch eine Überprüfung der Herkunft der Sensordatenabschnitte ermöglicht.

[0013] Schließlich wird die Überprüfung von Sensordatenabschnitten wie bereits oben näher erläutert erleichtert, wenn jeder neu berechnete Wurzelhashwert eines Hashbaumes in einem konsensbasierten, dezentralen Prüfspeicher abgelegt und die Adresse des Wurzelhashwertes im Prüfspeicher gemeinsam mit eine Referenz auf die für die Berechnung des Wurzelhashwertes herangezogenen Sensordatenabschnitte umfassenden Berechnungsparametern ausgegeben wird.

[0014] Zur Integritätsprüfung kann die Adresse des Wurzelhashwertes gemeinsam mit den Berechnungsparametern aus dem Sensordatenstrom extrahiert, der an dieser Adresse hinterlegte Wurzelhashwert abgerufen und anhand der Sensordatenabschnitte des Sensordatenstromes und den Berechnungsparametern ein Prüfwurzelhashwert zum Vergleich ermittelt werden. Alternativ können die Berechnungsparameter auch von einer Administrationseinheit abgefragt werden.

[0015] Stimmt der ermittelte Prüfwurzelhashwert mit dem angerufenen Wurzelhashwert überein, ist die Integritätsprüfung erfolgreich. Stimmt der Prüfwurzelhashwert nicht mit dem angerufenen Wurzelhashwert überein oder wurde an der angegebenen Adresse kein Wurzelhashwert gefunden, schlägt die Integritätsprüfung fehl. Für den Fall eines mit einer elektronischen Signatur versehenen Wurzelhashwertes kann zusätzlich noch überprüft werden, ob die Signatur mit beispielsweise in der Administrationseinheit hinterlegten Vorgaben übereinstimmt.

[0016] Die Erfindung bezieht sich auch auf eine Vorrichtung zur Durchführung eines erfindungsgemäßen Verfahrens. Die Vorrichtung umfasst eine Erfassungseinheit, die eine mit dem Sensordateneingang und einem Hashbaumspeicher verbundene Steuereinrichtung zur Berechnung und Speicherung von Hashwerten auf Basis einzelner Sensordatenstromabschnitte sowie auf Basis von untergeordneten Hashwerten des Hashbaumes umfasst. Die Steuereinrichtung weist zudem einen Wurzelhashausgang zur Ausgabe des zuletzt berechneten Wurzelhashwertes auf.

[0017] Um zusätzlich zur Integrität auch die Authentizität des Sensordatenstromes überprüfen zu können, wird vorgeschlagen, dass die Steuereinrichtung mit einem der Steuereinrichtung eindeutig zugeordneten kryptographischen Schlüsselspeicher zum elektronischen Signieren der Wurzelhashwerte verbunden ist. Durch die damit ermöglichte Signatur des ausgegebenen Wurzelhashwertes kann in weiterer Folge beispielsweise über eine Public-Key-Infrastruktur überprüft werden, ob ein Wurzelhashwert von einer bestimmten Steuereinrichtung und damit auch einer bestimmten Erfassungseinheit ausgegeben wurde. Weil die Erfassungseinheit aufgrund der geringen Leistungsanforderungen räumlich und strukturell nahe an dem den Sensordatenstrom erzeugenden Sensor angeordnet werden kann, wird damit die Möglichkeit einer Fälschung der Authentizität deutlich erschwert. Aufgrund dessen, dass für eine Authentizitätsprüfung jeweils nur der Wurzelhashwert, nicht aber die einzelnen Sensordatenstromabschnitte signiert werden müssen, kann darüber hinaus trotz der geringen Leistungsanforderungen an die Erfassungseinheit ein entsprechend laufzeitaufwändiges Signaturverfahren zum Einsatz kommen, was eine Fälschung gerade von Echtzeitdaten ebenfalls unwahrscheinlich macht. Ein Schlüsselspeicher kann beispielsweise eine sichere bzw. vertrauenswürdige Laufzeitumgebung wie beispielsweise ein Trusted Platform Module (TPM) sein, an die der Wurzelhashwert für die Signatur übermittelt wird und von der die Signatur abgerufen werden kann, ohne dass der hierfür verwendete private Teil des kryptographische Schlüssel den Schlüsselspeicher verlässt.

[0018] Zur manipulationssicheren Aufbewahrung der Wurzelhashwerte und zur einfachen Übermittlung und Abfrage derselben zur Integritätsprüfung kann der Wurzelhashausgang der Steuereinrichtung mit einem konsensbasierten, dezentralen und adressierbaren Prüfspeicher verbunden sein. Demzufolge werden die Wurzelhashwerte selbst nicht im grundsätzlich manipulierbaren Sensordatenstrom übertragen, sondern lediglich deren Adresse als Referenz zu einem Speicherbereich im Prüfspeicher, der aufgrund seiner dezentralen, konsensbasierten Ausgestaltung für einen einzelnen Angreifer nicht oder nur mit großem Aufwand manipulierbar ist. Um die Synchronisation der Hashbaumberechnung zwischen der Erfassungseinheit und einer im folgenden beschriebenen Abfrageeinheit zu erleichtern, wird vorgeschlagen, dass die Adresse des Wurzelhashwertes im Prüfspeicher gemeinsam mit einer Referenz auf die für die Berechnung des Wurzelhashwertes herangezogenen Sensordatenabschnitte ausgegeben wird. Die Steuereinrichtung kann zu diesem Zweck einen Sensordatenausgang zur Ausgabe der Sensordatenstromabschnitte und der Adressen der Wurzelhashwerte im Prüfspeicher gemeinsam mit einer Referenz auf die für die Berechnung des Wurzelhashwertes herangezogenen Sensordatenabschnitte aufweisen. Werden in einer besonders günstigen Ausführungsform die Adressen der Wurzelhashwertes zwischen Sensordatenstromabschnitten eingefügt, die jeweils das Ende bzw. den Beginn eines Hashbaumes markieren, kann eine gesonderte Referenz auf die für die Berechnung

des Wurzelhashwertes herangezogenen Sensordatenabschnitte entfallen. Besonders einfache Übertragungs- und Prüfungsbedingungen ergeben sich, wenn neben einer Referenz auf die für die Berechnung des Wurzelhashwertes herangezogenen Sensordatenabschnitte auch Informationen über die Struktur des Hashbaumes, insbesondere über dessen Tiefe und des verwendeten Verfahrens zur Hashbildung gemeinsam mit den Sensordatenstromabschnitten ausgegeben werden, weil dann die Struktur des Hashbaumes genauso wie das Verfahren zur Hashbildung an die aktuellen Parameter des Sensordatenstromes, wie beispielsweise die Datenübertragungsrate angepasst werden kann und zur Übermittlung dieser Berechnungsparameter keine gesonderte Übertragung erfolgen muss.

[0019] Damit Sensordatenstromabschnitte unabhängig von der Erfassungseinheit auf ihre Integrität überprüft werden können, kann erfindungsgemäß eine Abfrageeinheit vorgesehen sein, die einen Sensordateneingang für Sensordatenstromabschnitte und eine mit dem Sensordateneingang und einem Hashbaumspeicher verbundene Steuereinrichtung zur Berechnung und Speicherung von Hashwerten auf Basis einzelner Sensordatenstromabschnitte sowie auf Basis von untergeordneten Hashwerten des Hashbaumes umfasst, wobei die Steuereinrichtung mit dem konsensbasierten, dezentralen und adressierbaren Prüfspeicher zur Abfrage von Wurzelhashwertes verbunden ist. Die Steuereinrichtung und der Hashbaumspeicher können dabei in gleicher Weise wie jene der Erfassungseinheit aufgebaut sein, sodass grundsätzlich keine Berechnungsparameter, also Informationen zur Berechnung der Hashwerte sowie zur Struktur des Hashbaumes von der Erfassungseinheit an die Abfrageeinheit übermittelt werden müssen. Sollen beispielsweise zur Anpassung an die Taktfrequenz der Sensordatenströme unterschiedliche Hashbaumstrukturen oder Verfahren zur Berechnung der Hashwerte zum Einsatz kommen, kann eine zentrale Administrationseinheit vorgesehen sein, in der diese Berechnungsparameter je Sensordatenstrom bzw. je Erfassungseinheit abgespeichert und von den Abfrageeinheiten abgerufen werden können. Wie oben beschrieben, können diese Berechnungsparameter aber auch direkt gemeinsam mit den Adressen der Wurzelhashwerte im Prüfspeicher in den Datenstrom integriert werden.

[0020] In einer besonders bevorzugten Ausführungsform der Erfindung ist es möglich, nicht nur zeitlich versetzt Datenstromabschnitte abzufragen und einer Integritätsprüfung zu unterziehen, sondern auch mehrere Datenstromabschnitte in Bezug auf Ihre Integrität zu prüfen, aus denen für sich kein vollständiger Hashbaum gebildet und damit kein Wurzelhashwert berechnet werden kann. Dies kann dadurch erreicht werden, dass die Erfassungseinheit mit einem Datenspeicher zur Aufzeichnung von Sensordatenstromabschnitten verbunden ist, der eine mit einem Hashbaumspeicher verbundene Steuereinrichtung zur Berechnung und Speicherung von Hashwerten auf Basis einzelner Sensordatenstromabschnitte sowie auf Basis von untergeordneten Hashwerten des Hashbaumes umfasst. Eine Abfrageeinheit kann somit nicht nur die unmittelbar in Echtzeit von einer Erfassungseinheit ausgegebenen, sondern beliebige Datenstromabschnitte von diesem Datenspeicher abfragen. Können aus den abgefragten Datenstromabschnitten keine vollständigen Hashbäume gebildet werden, berechnet die Steuereinrichtung des Datenspeichers, die analog zu der Steuereinrichtung der Erfassungseinheit und damit auch der Abfrageeinheit aufgebaut sein kann, die im Hashbaum jeweils dem Wurzelhashwert am nächsten liegenden Zwischenhashwerte, die auf Basis der abgefragten Datenstromabschnitte nicht von der Abfrageeinheit berechnet werden können, und übermittelt diese gemeinsam mit den abgefragten Datenstromabschnitten an die Abfrageeinheit. Die Steuereinrichtung der Abfrageeinheit kann diese Zwischenhashwerte dann im Hashbaumspeicher ablegen und auf diese Weise den Wurzelhashwert anhand der übermittelten Sensordatenstromabschnitte ermitteln. Wurden dabei nicht an die Abfrageeinheit übermittelte Datenstromabschnitte manipuliert, so übermittelt der Datenspeicher fehlerhafte Zwischenhashwerte an die Abfrageeinheit, wo die Integritätsprüfung wie oben beschreiben ebenfalls fehlschlägt. Dies hat zum Vorteil, dass auch Manipulationen vor oder nach den abgefragten Datenstromabschnitten aufgedeckt werden können, die die Integrität der abgefragten Datenstromabschnitte ebenfalls in Frage stellen.

[0021] In der Zeichnung ist der Erfindungsgegenstand beispielsweise dargestellt. Es zeigen

[0022] Fig. 1 eine schematische Darstellung einer erfindungsgemäßen Erfassungseinheit,

[0023] Fig. 2 eine ebenfalls schematisch dargestellte Speicherstruktur eines Hashbaumspeichers einer solchen Erfassungseinheit und

[0024] Fig. 3 eine erfindungsgemäße Vorrichtung mit einer Erfassungseinheit der Fig. 1, ebenfalls in einer schematischen Darstellung in größerem Maßstab.

[0025] Eine erfindungsgemäße Vorrichtung zur Integritätsprüfung von Sensordatenströmen umfasst eine Erfassungseinheit 1, mit Hilfe derer die Sensordaten eines Sensors 2 erfasst werden können. Der Sensor 2 kann beispielsweise an einer Maschine 3 angeordnet sein und deren Temperatur oder ähnliche Parameter messen. Die Erfassungseinheit 1 selbst umfasst neben einer Steuereinrichtung 4 einen Hashbaumspeicher 5.

[0026] Die Speicherstruktur innerhalb des Hashbaumspeichers 5 wird im Folgenden näher anhand der Fig. 2 erläutert: In der vorliegenden Ausführungsform ist der Hashbaum in Form eines einfachen Binärhashbaumes 6 ausgebildet. Dieser Binärhashbaum 6 hat jeweils einzelne Speicherbereiche 7, 8, 9, 10 in die Hashwerte von Sensordatenstromabschnitten 11, 12, 13, 14 eines Sensordatenstromes 15 gespeichert werden können. Die Speicherbereiche 7 und 8 sind einem übergeordneten Elternspeicherbereich 16 für einen Zwischenhash, die Speicherbereiche 9 und 10 einem übergeordneten Elternspeicherbereich 17 für einen Zwischenhash zugeordnet. Die Speicherbereiche 16 und 17 sind wiederum einem übergeordneten Elternspeicherbereich 18 zugeordnet, in den der Wurzelhashwert des Binärhashbaumes 6 gespeichert werden kann.

[0027] Zufolge dieser Maßnahmen können für einzelne Sensordatenstromabschnitte 11, 12, 13, 14 des Sensordatenstromes Hashwerte berechnet und in den Speicherbereichen 7, 8, 9, 10 der untersten Ebene eines Hashbaumspeichers 5 mit vorgegebener Struktur, beispielweise in Form eines einfachen Binärbaumes 6 abgespeichert werden. Bei Verfügbarkeit aller einem Elternspeicherbereich 16, 17 unmittelbar untergeordneter Hashwerte kann sodann aus diesen ein übergeordneter Hashwert berechnet und im Elternspeicherbereich 16, 17 abgelegt werden, wonach die untergeordneten Hashwerte nicht mehr benötigt werden und die Speicherbereiche 7, 8, 9, 19 damit für einen geringen Speicherverbrauch gelöscht werden können. Die Hashwerte für die Elternspeicherbereiche 16 und 17 können dabei entweder parallel oder nacheinander berechnet werden, wobei letztere Vorgehensweise die Löschung der Speicherbereiche 7 und 8 unabhängig von der Löschung der Speicherbereiche 9 und 10 möglich macht. Schließlich wird bei Verfügbarkeit der Zwischenhashwerte in den Elternspeicherbereichen 16 und 17 ebenfalls ein übergeordneter Wurzelhashwert berechnet und im Elternspeicherbereich 18 abgelegt. Danach können wiederum die Elternspeicherbereiche 16 und 17 gelöscht werden. Aus der Fig. 2 ist damit ersichtlich, dass grundsätzlich zur Berechnung eines vollständigen Hashbaumes sämtliche Sensordatenstromabschnitte 11, 12, 13, 14 des Sensordatenstromes 15 erforderlich sind. Der Hashbaum kann aber auch dann berechnet werden, wenn beispielsweise neben den Sensordatenstromabschnitten 11, 12 der Zwischenhashwert des Elternspeicherbereiches 17 oder aber wenn neben den Sensordatenstromabschnitten 13, 14 der Zwischenhashwert des Elternspeicherbereiches 16 vorhanden ist.

[0028] Zur Ausgabe des jeweils zuletzt berechneten Wurzelhashwertes weist die Steuereinrichtung 4 der Erfassungseinheit 1 einen Wurzelhashausgang 19 auf, der mit einem symbolisch dargestellten, konsensbasierten, dezentralen und adressierbaren Prüfspeicher 20 zur sicheren Ablage der Wurzelhashwerte verbunden sein kann, wie dies in den Figs. 1 und 3 abgebildet ist.

[0029] Neben dem Wurzelhashausgang 19 kann die Steuereinrichtung 4 auch einen Sensordatenausgang 21 zur Ausgabe der Sensordatenstromabschnitte 11, 12, 13, 14 und der Adressen der Wurzelhashwerte im Prüfspeicher 20 gemeinsam mit einer Referenz auf die für die Berechnung des Wurzelhashwertes herangezogenen Sensordatenabschnitte aufweisen.

[0030] In einer besonders bevorzugten Ausführungsform der Erfindung umfasst die Erfassungseinheit 1 einen der Steuereinrichtung 4 eindeutig zugeordneten kryptographischen Schlüsselspeicher 22 zum elektronischen Signieren der Wurzelhashwerte.

[0031] Neben der Erfassungseinheit 1 kann auch eine Abfrageeinheit 23 vorgesehen sein, die einen Sensordateneingang 24 für Sensordatenstromabschnitte 11, 12, 13, 14 und eine mit dem

Sensordateneingang 24 und einem nicht näher dargestellten Hashbaumspeicher verbundene, ebenfalls nicht dargestellte Steuereinrichtung zur Berechnung und Speicherung von Hashwerten auf Basis einzelner Sensordatenstromabschnitte sowie auf Basis von untergeordneten Hashwerten des Hashbaumes umfasst. Der Aufbau der Abfrageeinheit 23 kann daher dem Aufbau der Erfassungseinheit 1 entsprechen. Darüber hinaus ist die Steuereinrichtung der Abfrageeinheit 23 mit dem konsensbasierten, dezentralen und adressierbaren Prüfspeicher 20 zur Abfrage von Wurzelhashwertes verbunden.

[0032] Um nicht nur zeitlich versetzt Sensordatenstromabschnitte 11, 12, 13, 14 abzufragen und einer Integritätsprüfung zu unterziehen, sondern auch mehrere Sensordatenstromabschnitte 13, 14 in Bezug auf Ihre Integrität zu prüfen, aus denen für sich kein vollständiger Hashbaum gebildet und damit kein Wurzelhashwert berechnet werden kann, wird erfindungsgemäß vorgeschlagen, dass die Erfassungseinheit 1 mit einem Datenspeicher 25 zur Aufzeichnung von Sensordatenstromabschnitten 11, 12, 13, 14 verbunden ist. Dieser Datenspeicher 25 umfasst ebenfalls eine, nicht dargestellte mit einem Hashbaumspeicher verbundene Steuereinrichtung zur Berechnung und Speicherung von Hashwerten auf Basis einzelner Sensordatenstromabschnitte 11, 12, 13, 14 sowie auf Basis von untergeordneten Hashwerten des Hashbaumes. Der Datenspeicher 25 kann somit abgesehen von einem Speicherbereich für die Sensordatenstromabschnitte 11, 12, 13, 14 ebenfalls analog zur Erfassungseinheit 1 aufgebaut sein.

[0033] Die Übertragung der Sensordatenstromabschnitte 11, 12, 13, 14 von der Erfassungseinheit 1 zur Abfrageeinheit 23 kann grundsätzlich über jede beliebige, auch ungesicherte Infrastruktur 26, beispielsweise über das Internet erfolgen. Dabei können die Berechnungsparameter für die Ermittlung der Hashwerte sowie für die Struktur der zu verwendenden Hashbäume vorab fest vorgegeben werden, in den Sensordatenstrom integriert oder aber über eine dafür vorgesehene Administrationseinheit 27 vorgegeben bzw. abgefragt werden.

[0034] Wie insbesondere der Fig. 3 entnommen werden kann, ermöglicht die erfindungsgemäße Vorrichtung und das erfindungsgemäße Verfahren damit, einen von einem Sensor 2 gemessenen Sensordatenstrom über eine Erfassungseinheit 1 in einer ersten Sicherheitsdomäne 28 zu erfassen und über eine Abfrageeinheit 23 in einer zweiten Sicherheitsdomäne 29 über eine unsichere Infrastruktur 26 abzufragen, wobei die Sensordaten zwar im Klartext erhalten und weiterverarbeitet werden können, eine Modifikation der Sensordaten aber dazu führt, dass die Integritätsprüfung auf Seiten der Abfrageeinheit 23 fehlschlägt. Darüber hinaus ist es nicht nur möglich, den Sensordatenstrom vom Sensor 2 in Echtzeit abzufragen, sondern auch beliebige aufgezeichnete Sensordatenstromabschnitte 11, 12 vom Datenspeicher 25 mit Integritätsprüfung abzufragen.

Patentansprüche

1. Verfahren zur Integritätsprüfung von Sensordatenströme (15), **dadurch gekennzeichnet**, dass für einzelne Sensordatenstromabschnitte (11, 12, 13, 14) eines Sensordatenstromes (15) Hashwerte berechnet und in den Speicherbereichen (7, 8, 9, 10) der untersten Ebene eines Hashbaumspeichers (5) mit vorgegebener Struktur gespeichert werden, wobei bei Verfügbarkeit aller einem Elternspeicherbereich (16, 17, 18) unmittelbar untergeordneter Hashwerte aus diesen ein übergeordneter Hashwert berechnet und im Elternspeicherbereich (16, 17, 18) abgelegt wird, wonach die dem Elternspeicherbereich (16, 17, 18) untergeordneten Hashwerte gelöscht werden.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, dass die einzelnen Sensordatenstromabschnitte (11, 12, 13, 14) mit einem Zeitstempel versehen werden, der bei der Berechnung des Hashwertes berücksichtigt wird.

3. Verfahren nach Anspruch 1 oder 2 **dadurch gekennzeichnet**, dass jeder neu berechnete Wurzelhashwert eines Hashbaumes mit einer die Erfassungseinheit (1) identifizierenden elektronischen Signatur versehen wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet**, dass jeder neu berechnete Wurzelhashwert eines Hashbaumes in einem konsensbasierten, dezentralen Prüfspeicher (20) abgelegt und die Adresse des Wurzelhashwertes im Prüfspeicher (20) gemeinsam mit einer Referenz auf die für die Berechnung des Wurzelhashwertes herangezogenen Sensordatenabschnitte (11, 12, 13, 14) umfassenden Berechnungsparametern ausgegeben wird.

5. Verfahren nach Anspruch 4, **dadurch gekennzeichnet**, dass die Adresse des Wurzelhashwertes gemeinsam mit den Berechnungsparametern aus dem Sensordatenstrom (15) extrahiert, der an dieser Adresse hinterlegte Wurzelhashwert abgerufen und anhand der Sensordatenabschnitte (11, 12, 13, 14) des Sensordatenstromes (15) und den Berechnungsparametern ein Prüfwurzelhashwert zum Vergleich ermittelt wird.

6. Vorrichtung zur Durchführung eines Verfahrens nach einem der vorangegangenen Ansprüche, mit einer Erfassungseinheit (1), die einen Sensordateneingang aufweist, **dadurch gekennzeichnet**, dass die Erfassungseinheit (1) eine mit dem Sensordateneingang und einem Hashbaumspeicher (5) verbundene Steuereinrichtung (4) zur Berechnung und Speicherung von Hashwerten auf Basis einzelner Sensordatenstromabschnitte (11, 12, 13, 14) sowie auf Basis von untergeordneten Hashwerten des Hashbaumes umfasst, und dass die Steuereinrichtung (4) einen Wurzelhashausgang (19) zur Ausgabe des zuletzt berechneten Wurzelhashwertes aufweist.

7. Vorrichtung nach Anspruch 6, **dadurch gekennzeichnet**, dass die Steuereinrichtung (4) mit einem der Steuereinrichtung (4) eindeutig zugeordneten kryptographischen Schlüsselspeicher (22) zum elektronischen Signieren der Wurzelhashwerte verbunden ist.

8. Vorrichtung nach Anspruch 6 oder 7, **dadurch gekennzeichnet**, dass der Wurzelhashausgang (19) der Steuereinrichtung (4) mit einem konsensbasierten, dezentralen und adressierbaren Prüfspeicher (20) verbunden ist und dass die Steuereinrichtung (4) einen Sensordatenausgang (21) zur Ausgabe der Sensordatenstromabschnitte (11, 12, 13, 14) und der Adressen der Wurzelhashwerte im Prüfspeicher (20) aufweist.

9. Vorrichtung nach Anspruch 8, **dadurch gekennzeichnet**, dass eine Abfrageeinheit (23) einen Sensordateneingang (24) für Sensordatenstromabschnitte (11, 12, 13, 14) und eine mit dem Sensordateneingang (24) und einem Hashbaumspeicher verbundene Steuereinrichtung zur Berechnung und Speicherung von Hashwerten auf Basis einzelner Sensordatenstromabschnitte (11, 12, 13, 14) sowie auf Basis von untergeordneten Hashwerten des Hashbaumes umfasst, und dass die Steuereinrichtung mit dem konsensbasierten, dezentralen und adressierbaren Prüfspeicher (20) zur Abfrage von Wurzelhashwerten verbunden ist.

10. Vorrichtung nach einem der Ansprüche 6 bis 9, **dadurch gekennzeichnet**, dass die Erfassungseinheit (1) mit einem Datenspeicher (25) zur Aufzeichnung von Sensordatenstromabschnitten (11, 12, 13, 14) verbunden ist, der eine mit einem Hashbaumspeicher verbundene Steuereinrichtung zur Berechnung und Speicherung von Hashwerten auf Basis einzelner Sensordatenstromabschnitte (11, 12, 13, 14) sowie auf Basis von untergeordneten Hashwerten des Hashbaumes umfasst.

Hierzu 3 Blatt Zeichnungen

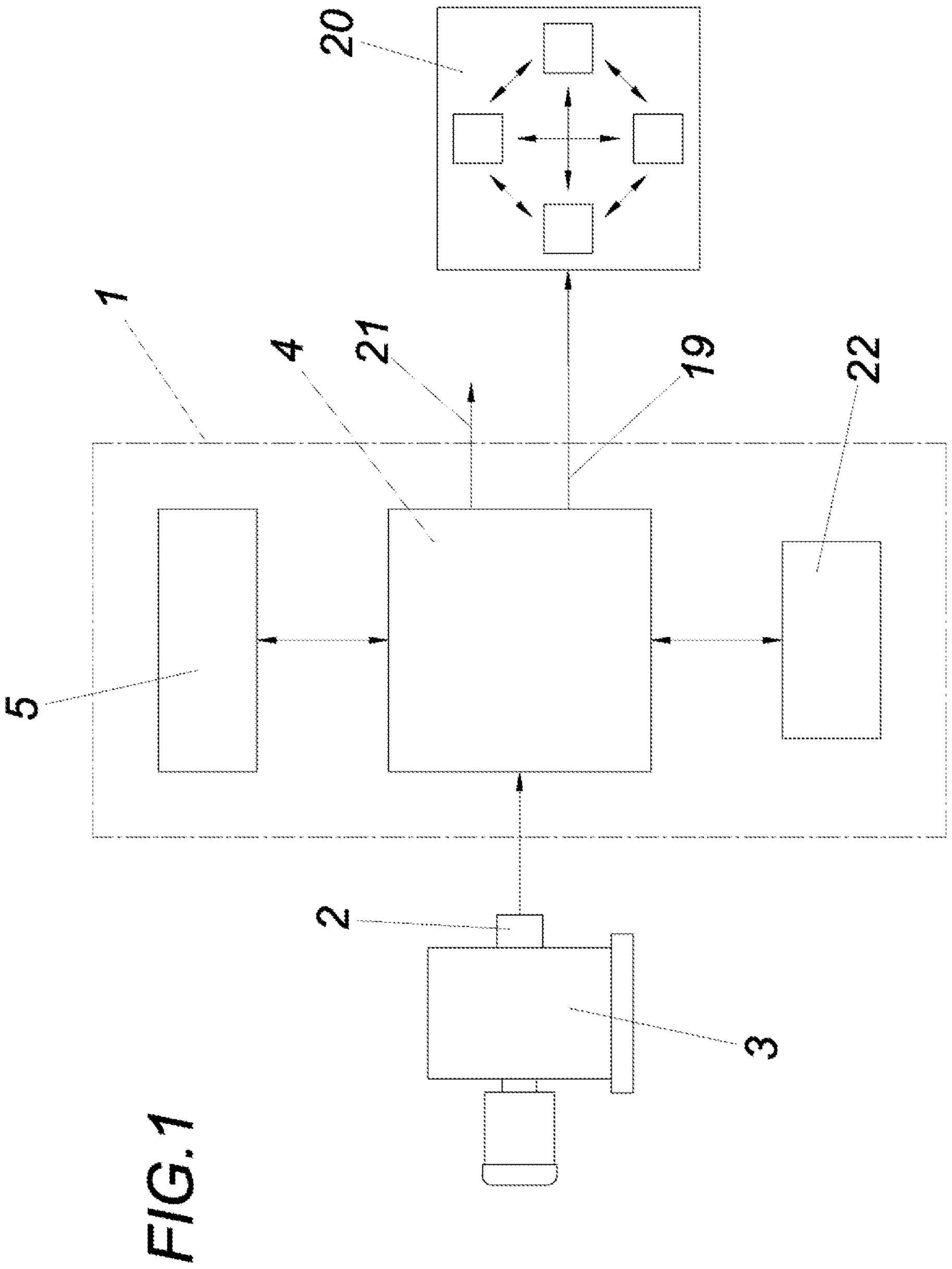

FIG.1

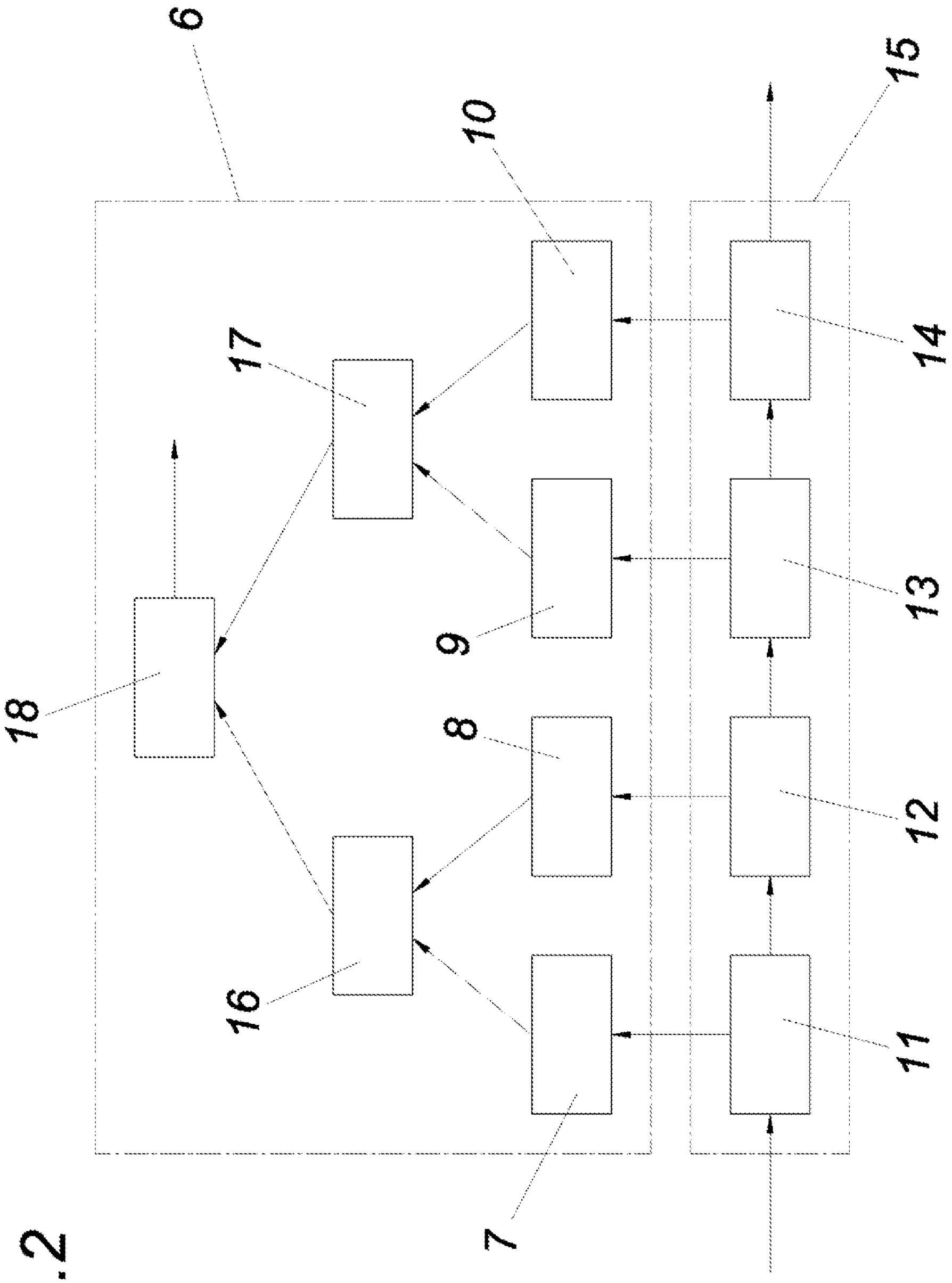

FIG.2

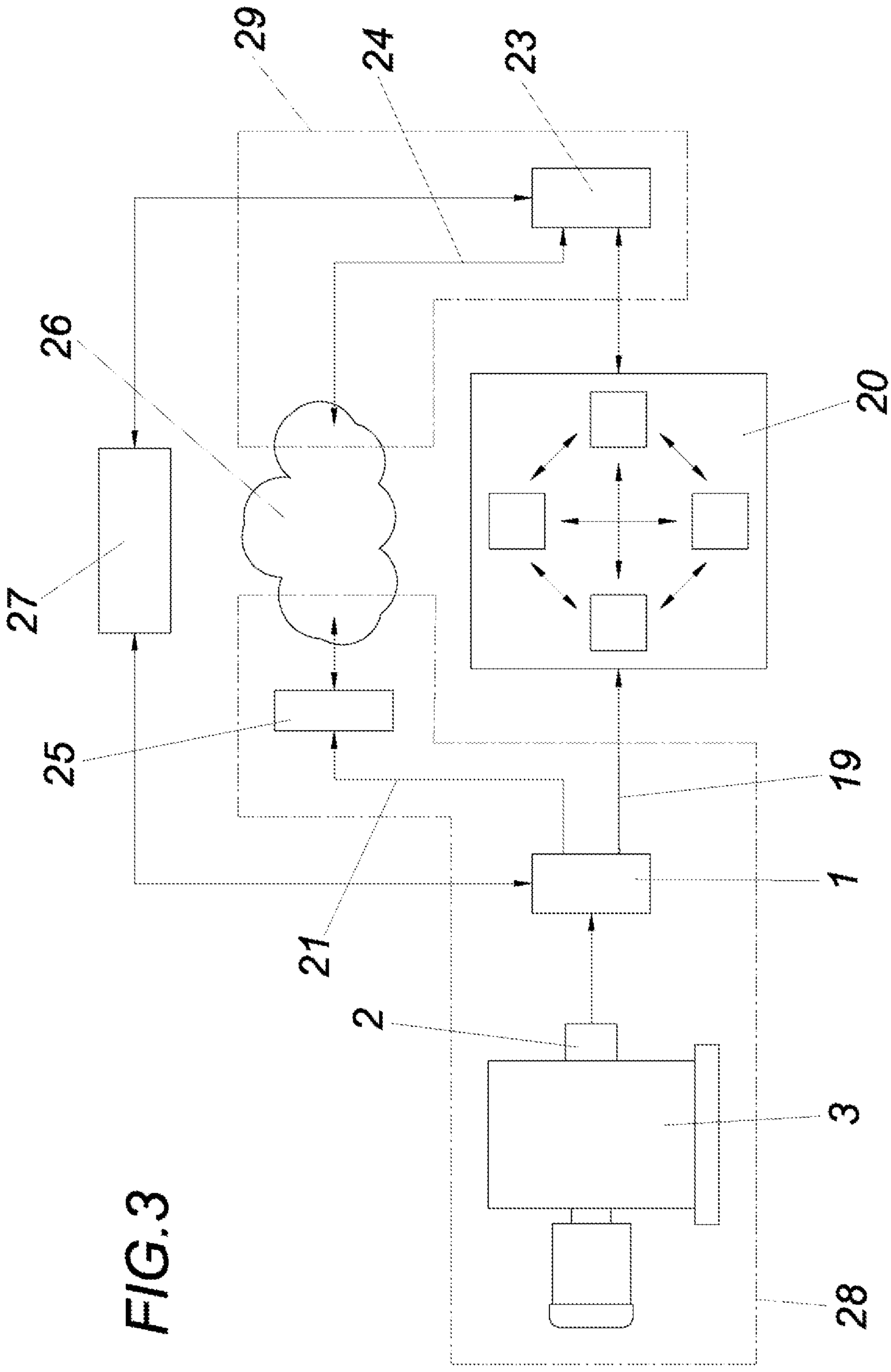

FIG.3