(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
20. Januar 2022 (20.01.2022)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2022/013213 A1

(51) Internationale Patentklassifikation:
G06F 21/62 (2013.01) *H04L 9/08* (2006.01)
G16H 10/60 (2018.01) *G06F 21/64* (2013.01)

(21) Internationales Aktenzeichen: PCT/EP2021/069452

(22) Internationales Anmeldedatum:
13. Juli 2021 (13.07.2021)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
20185651.5 14. Juli 2020 (14.07.2020) EP

(72) Erfinder; und
(71) Anmelder: **HEIL, Katharina** [AT/AT]; Am Arlandgrund 41/3.3, 8045 Graz (AT).

(74) Anwalt: **ROTHKOPF PATENT- UND RECHTSANWÄLTE**; Maximilianstraße 25, 80539 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: 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, IT, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (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).

(54) **Title:** COMPUTER-IMPLEMENTED METHOD FOR READING AND STORING PATIENT DATA

(54) **Bezeichnung:** COMPUTERIMPLEMENTIERTES VERFAHREN ZUM EINLESEN UND SPEICHERN VON PATIENTENDATEN

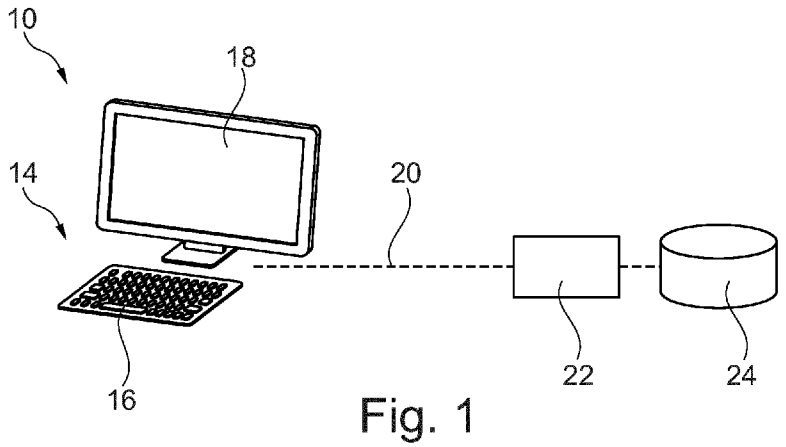

Fig. 1

(57) **Abstract:** The invention relates to a computer-implemented method for reading and storing patient data in a computer system by means of multiple users, having the steps of: setting up a study key, setting up a user key per user using the study key, allocating the user keys to the users, and reading patient data by means of the individual user using the respective user key, wherein the entered patient data is stored in the computer system in an encrypted manner using the user key.

(57) **Zusammenfassung:** Die Erfindung betrifft ein computerimplementiertes Verfahren zum Einlesen und Speichern von Patientendaten in einem Computersystem durch mehrere Nutzer mit den Schritten: Festlegen eines Studien-Schlüssels, Festlegen eines Nutzer-Schlüssels je Nutzers mittels des Studien-Schlüssels, Zuteilen der Nutzer-Schlüssel an die Nutzer sowie Einlesen von Patientendaten durch den einzelnen Nutzer mittels des jeweiligen Nutzer-Schlüssels, wobei die eingegebenen Patientendaten mittels des Nutzer-Schlüssels verschlüsselt im Computersystem gespeichert werden.

WO 2022/013213 A1

[Fortsetzung auf der nächsten Seite]

Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

— *in Schwarz-Weiss; die internationale Anmeldung enthielt in ihrer eingereichten Fassung Farbe oder Graustufen und kann von PATENTSCOPE heruntergeladen werden.*

Beschreibung

Computerimplementiertes Verfahren zum Einlesen und Speichern von Patientendaten

Hintergrund der Erfindung

Die Erfindung betrifft ein computerimplementiertes Verfahren zum Einlesen und Speichern von Patientendaten in einem Computersystem durch mehrere Nutzer.

Bei der computergestützten Verarbeitung von medizinischen Patientendaten bestehen hinsichtlich des Datenschutzes besonders hohe Anforderungen und besonders strenge rechtliche Vorgaben. Bei den Patientendaten handelt es sich regelmäßig um personenbezogene Daten, für die ein besonders hohes Niveau an Datensicherheit zu gewährleisten ist.

Für Studien im medizinischen Bereich ist es erforderlich, dass solche Patientendaten auch über viele Standorte und dabei auch international verteilt erfasst sowie verarbeitet werden können. Zugleich sind umfangreiche Daten zu erfassen, um eine angemessene Dokumentation und Protokollierung solcher Studien zu gewährleisten.

Gerade bei der Erfassung bzw. dem Einlesen solcher Patientendaten im Rahmen von medizinischen Studien besteht noch viel Handlungsbedarf hinsichtlich der Digitalisierung solcher Prozesse.

Zugrundeliegende Aufgabe

Der Erfindung liegt die Aufgabe zugrunde, ein computerimplementiertes Verfahren zum Einlesen und Speichern von Patientendaten in einem Computersystem durch mehrere Nutzer sowie ein zugehöriges Computersystem zu schaffen, mittels denen standortübergreifend Patientendaten auf besonders hohem Sicherheitsniveau eingelesen und gespeichert werden können.

Erfindungsgemäße Lösung

Diese Aufgabe ist erfindungsgemäß mit einem computerimplementierten Verfahren zum Einlesen und Speichern von Patientendaten in einem Computersystem durch mehrere Nutzer geschaffen, bei dem die folgenden Schritte abgehandelt werden: Erstens Festlegen eines Studien-Schlüssels, zweitens Festlegen eines Nutzer-Schlüssels je Nutzer mittels des Studien-Schlüssels, drittens Zuteilen der Nutzer-Schlüssel an die Nutzer sowie viertens Einlesen von Patientendaten durch den einzelnen Nutzer mittels des jeweiligen Nutzer-Schlüssels, wobei die eingegebenen Patientendaten mittels des Nutzer-Schlüssels verschlüsselt im Computersystem gespeichert werden. Dabei sollen vorliegend gemäß der Erfindung mit dem Begriff "Studie" jede Art von Studie bzw. Untersuchung und auch andere Arten von Projekten mit inhaltlich zusammengehörigen Daten, also nicht nur medizinische oder etwa pharmazeutische Studien, verstanden werden.

Die Besonderheit der derartigen erfindungsgemäßen Vorgehensweise liegt darin, dass die Verschlüsselung beim Einlesen der Patientendaten auf einer zweistufigen Generierung von Schlüsseln, nämlich eines Studien-Schlüssels für die medizinische Studie selbst und eines Nutzer-Schlüssels für jeden der Nutzer beruht, wobei der jeweilige Nutzer-Schlüssel zusätzlich auf Basis bzw. Grundlage des Studien-Schlüssels erzeugt wird. Gemäß der Erfindung ist also der Studien-Schlüssel mit in dem Nutzer-Schlüssel verarbeitet bzw. integriert, so dass dieser

jeweilige Nutzer-Schlüssel in verschlüsselter Weise auch die Information des Studien-Schlüssels enthält.

Aufgrund dieser besonderen Schlüssel-Systematik ist es gemäß der Erfindung möglich, dass die vom jeweiligen Nutzer eingegebenen Daten grundsätzlich sofort verschlüsselt werden und damit ausschließlich in verschlüsseltem Zustand im Computersystem gespeichert werden. Das Computersystem enthält also keinerlei nicht-verschlüsselte Information, wodurch das so genannte Konzept des Zero-Knowledge-Proof sichergestellt ist. Mit diesem Konzept ist also sichergestellt, dass der Anbieter bzw. Administrator des erfindungsgemäßen Computersystems selbst keinen Einblick in die gespeicherten Daten der Nutzer haben kann.

Darüber hinaus bietet diese Vorgehensweise gemäß der Erfindung den Vorteil, dass die Patientendaten weitestgehend unbedenklich auch verteilt an diversen Standorten und/oder auf verschiedenen Rechnern bzw. Servern gespeichert sowie selbst in so genannten Cloud-Speichern gehalten werden können, ohne dass ein Sicherheitsrisiko besteht.

Eine bevorzugte Ausführungsform des erfindungsgemäßen Verfahrens umfasst ferner die Schritte: Festlegen von Nutzer-Rechten zum Verarbeiten von gespeicherten Patientendaten in dem Nutzer-Schlüssel und Verarbeiten von gespeicherten Patientendaten im Computersystem durch einen Nutzer in Abhängigkeit von in dessen Nutzer-Schlüssel festgelegten Nutzer-Rechten zum Verarbeiten von gespeicherten Patientendaten. Der erfindungsgemäß vorgesehene Nutzer-Schlüssel enthält damit nicht nur zugleich die Verschlüsselungsinformation des Studien-Schlüssels sondern definiert als solcher auch noch Nutzer-Rechte, mittels denen ein Zugriff auf Patientendaten im Computersystem geregelt ist. Diese Rechte-Zuweisung kann dabei wiederum in sich verschlüsselt sein, insbesondere mittels des Studien-Schlüssels, so dass eine Manipulation dieser Rechtezuweisung durch Unbefugte ebenfalls weitestgehend ausgeschlossen ist.

Beim Festlegen der Nutzer-Rechte zum Verarbeiten von gespeicherten Patientendaten wird besonders bevorzugt festgelegt, dass der jeweilige Nutzer die von ihm selbst eingegebenen Daten stets verarbeiten darf. So kann sehr einfach der Zugriff auf "eigene" Daten des jeweiligen Nutzers sichergestellt werden.

Das erfindungsgemäße, computerimplementierte Verfahren umfasst gemäß derselben, oben erläuterten erfindungsgemäßen Idee ferner vorzugsweise die Schritte: Festlegen von Nutzer-Rechten zum Auslesen von gespeicherten Patientendaten in dem Nutzer-Schlüssel und Auslesen von gespeicherten Patientendaten im Computersystem durch einen Nutzer in Abhängigkeit von in dessen Nutzer-Schlüssel festgelegten Nutzer-Rechten zum Auslesen von gespeicherten Patientendaten. Dabei wird in ähnlicher Weise beim Festlegen der Nutzer-Rechte zum Auslesen von gespeicherten Patientendaten besonders vorteilhaft festgelegt, dass der jeweilige Nutzer die von ihm selbst eingegeben Daten stets auslesen darf.

Das computerimplementierte Verfahren gemäß der Erfindung kann darüber hinaus besonders sicher gestaltet werden, indem die gespeicherten Patientendaten fragmentiert im Computersystem gespeichert werden.

Ferner können mit der erfindungsgemäßen Vorgehensweise die gespeicherten Patientendaten vorzugsweise auch in einem Cloud-Speicher des Computersystems gespeichert werden.

Die Erfindung ist vorzugsweise auch auf ein derartiges computerimplementiertes Verfahren mit folgendem Schritt gerichtet: Verarbeiten von im Computersystem gespeicherten Patientendaten zu Ergebnisdaten, wobei die Ergebnisdaten mittels des Studien-Schlüssels und/oder mittels des jeweiligen Nutzer-Schlüssels verschlüsselt im Computer-System gespeichert werden. Die erfindungsgemäße, zweistufige und in sich verschachtelte Verschlüsselung wird damit vorzugsweise

auch für die Verarbeitung von Patientendaten zu Ergebnisdaten und deren Speicherung verwendet.

Darüber hinaus betrifft die Erfindung vorteilhaft ein solches computerimplementiertes Verfahren, wobei Änderungen an Patientendaten und/oder Ergebnisdaten mittels einer Signierung mit dem Blockchain-Prinzip protokolliert werden. Änderungen an Daten können so revisionssicher rückverfolgt werden.

Schließlich ist die Erfindung auch auf ein Computersystem gerichtet, dass zum Ausführen eines solchen computerimplementierten Verfahrens gemäß der Erfindung angepasst ist.

Kurzbeschreibung der Zeichnung

Nachfolgend wird ein Ausführungsbeispiel einer erfindungsgemäßen Lösung anhand der beigefügten schematischen Zeichnung näher erläutert. Es zeigt:

Fig. 1 ein Ausführungsbeispiels eines Computersystems gemäß der Erfindung und
Fig. 2 ein Ablaufschema eines Ausführungsbeispiels des Verfahrens gemäß der Erfindung.

Detaillierte Beschreibung des Ausführungsbeispiels

In der Fig. 1 ist ein Computersystem 10 veranschaulicht, mittels dem ein Verfahren 12 (siehe Fig. 2) durchzuführen ist.

Das Computersystem 10 umfasst eine Mehrzahl an Ein- und Ausgabeeinheiten 14, von denen beispielhaft nur eine dargestellt ist. Die Ein- und Ausgabeeinheit 14 umfasst in der Art eines Terminals zumindest eine Tastatur 16 sowie einen

Bildschirm 18. Vorzugsweise umfasst die Ein- und Ausgabeeinheit 14 ferner eine Rechnereinheit bzw. Computereinheit (nicht näher veranschaulicht).

Angeschlossen ist die Ein- und Ausgabeeinheit 14 mittels einer Leitung 20, die drahtgebunden oder auch drahtlos gestaltet sein kann, an eine (weitere) Rechnereinheit 22. An diese Rechnereinheit 22 ist seinerseits eine Speichereinheit 24 betrieblich angekoppelt.

Mittels des Computersystems 10 ist das Verfahren 12 auszuführen, welches in Fig. 2 dargestellt ist. Bei dem Verfahren 12 wird zunächst in einem Schritt 26 von einem Administrator (nicht dargestellt) des Computersystems 10 ein Studien-Schlüssel in Gestalt einer ersten Kodierung bzw. eines ersten Codes über einen vom Computersystem 10 ausgeführten, ersten Algorithmus zur Schlüsselgenerierung festgelegt. Danach werden in einem Schritt 28 vom Administrator mittels des Computersystems 10 für mehrere Nutzer (nicht dargestellt) mehrere Nutzer-Schlüssel ebenfalls mittels eines zweiten Algorithmus festgelegt. Bei dieser Festlegung der Nutzer-Schlüssel wird der zuvor generierte Studien-Schlüssel innerhalb des zweiten Algorithmus berücksichtigt. Insbesondere werden die Nutzer-Schlüssel mittels des Studien-Schlüssels selbst verschlüsselt und/oder es wird in die Nutzer-Schlüssel die Information des Studien-Schlüssels integriert. Die Schlüssellänge beträgt dabei insbesondere 128 Bits bzw. 16 Bytes gemäß dem AES256-Standard.

Dann werden in einem Schritt 30 diese Nutzer-Schlüssel insbesondere in Form von QR-Codes per separater Schlüsselkarte dem jeweiligen Nutzer persönlich zugestellt. Der Nutzer kann sich dann nachfolgend in einem Schritt 32 mit seiner Ein- und Ausgabeeinheit und dem Nutzer-Schlüssel an dem Computersystem 10 anmelden. Der Nutzer kann dort dann in einem Schritt 34 Patientendaten einlesen und ggf. auch auslesen. Für das Einlesen werden die Patientendaten sofort in dem Schritt 34 bei der Eingabe mittels des Nutzer-Schlüssels verschlüsselt und in einem Schritt 36 ausschließlich verschlüsselt über die Leitung 20 an die

Recheneinheit 22 bzw. die Speichereinheit 24 übermittelt. Alternativ können die Patientendaten auch derart verschlüsselt auf der Ein- und Ausgabeeinheit 14 selbst oder einem anderen Rechner bzw. Speicher, insbesondere einem Cloud-Rechner bzw. Cloud-Speicher vorgehalten werden.

Mittels der Ein- und Ausgabeeinheit 14 kann dann dieser Nutzer oder aber ein anderer Nutzer in einem Schritt 38 an einer anderen Ein- und Ausgabeeinheit 14 diese Patientendaten abrufen und/oder verarbeiten. Dabei ist der Zugriff auf die Patientendaten mittel des jeweiligen Nutzer-Schlüssels geregelt. Weil in dem Nutzer-Schlüssel jeweils zugleich auch die Information des Studien-Schlüssels enthalten ist, können die von einem ersten Nutzer eingegebenen und von diesem verschlüsselten Patientendaten oder zugehörige Ergebnisdaten auch von einem zweiten Nutzer in dem Schritt 38 ausgelesen und dabei entschlüsselt werden.

Abschließend sei angemerkt, dass sämtlichen Merkmalen, die in den Anmeldungsunterlagen und insbesondere in den abhängigen Ansprüchen genannt sind, trotz des vorgenommenen formalen Rückbezugs auf einen oder mehrere bestimmte Ansprüche, auch einzeln oder in beliebiger Kombination eigenständiger Schutz zukommen soll.

Bezugszeichenliste

10 Computersystem
12 Verfahren
14 Ein- und Ausgabeeinheit
16 Tastatur
18 Bildschirm
20 Leitung
22 Recheneinheit
24 Speichereinheit
26 Schritt Erstellen Studien-Schlüssel
28 Schritt Erstellen Nutzer-Schlüssel
30 Schritt Zustellen Nutzer-Schlüssel
32 Schritt Anmelden Nutzer
34 Schritt Einlesen und Verschlüsseln Patientendaten
36 Schritt Übermitteln Patientendaten
38 Schritt Entschlüsseln und Auslesen der Patientendaten oder Ergebnisdaten

Ansprüche

1. Computerimplementiertes Verfahren (12) zum Einlesen und Speichern von Patientendaten in einem Computersystem (10) durch mehrere Nutzer mit den Schritten:
- Festlegen (26) eines Studien-Schlüssels,
- Festlegen (28) eines Nutzer-Schlüssels je Nutzers mittels des Studien-Schlüssels,
- Zuteilen (30) der Nutzer-Schlüssel an die Nutzer,
- Einlesen (34) von Patientendaten durch den einzelnen Nutzer mittels des jeweiligen Nutzer-Schlüssels, wobei die eingegebenen Patientendaten mittels des Nutzer-Schlüssels verschlüsselt im Computersystem (10) gespeichert werden.

2. Computerimplementiertes Verfahren nach Anspruch 1,
mit den Schritten:
- Festlegen von Nutzer-Rechten zum Verarbeiten von gespeicherten Patientendaten in dem Nutzer-Schlüssel und
- Verarbeiten von gespeicherten Patientendaten im Computersystem (10) durch einen Nutzer in Abhängigkeit von in dessen Nutzer-Schlüssel festgelegten Nutzer-Rechten zum Verarbeiten von gespeicherten Patientendaten.

3. Computerimplementiertes Verfahren nach Anspruch 2,
wobei beim Festlegen der Nutzer-Rechte zum Verarbeiten von gespeicherten Patientendaten festgelegt wird, dass der jeweilige Nutzer die von ihm selbst eingegeben Daten stets verarbeiten darf.

4. Computerimplementiertes Verfahren einem der Ansprüche 1 bis 3,
mit den Schritten:
- Festlegen von Nutzer-Rechten zum Auslesen (42) von gespeicherten Patientendaten in dem Nutzer-Schlüssel und

- Auslesen (42) von gespeicherten Patientendaten im Computersystem (10) durch einen Nutzer in Abhängigkeit von in dessen Nutzer-Schlüssel festgelegten Nutzer-Rechten zum Auslesen (42) von gespeicherten Patientendaten.

5. Computerimplementiertes Verfahren nach Anspruch 4,
wobei beim Festlegen der Nutzer-Rechte zum Auslesen (42) von gespeicherten Patientendaten festgelegt wird, dass der jeweilige Nutzer die von ihm selbst eingegeben Daten stets auslesen darf.

6. Computerimplementiertes Verfahren nach einem der Ansprüche 1 bis 5,
wobei die gespeicherten Patientendaten fragmentiert im Computersystem (10) gespeichert werden.

7. Computerimplementiertes Verfahren nach einem der Ansprüche 1 bis 6,
wobei die gespeicherten Patientendaten in einem Cloud-Speicher des Computersystems (10) gespeichert werden.

8. Computerimplementiertes Verfahren nach einem der Ansprüche 1 bis 7,
mit dem Schritt:
Verarbeiten von im Computersystem (10) gespeicherten Patientendaten zu Ergebnisdaten,
wobei die Ergebnisdaten mittels des Studien-Schlüssels und/oder mittels des jeweiligen Nutzer-Schlüssels verschlüsselt im Computer-System (10) gespeichert werden.

9. Computerimplementiertes Verfahren nach einem der Ansprüche 1 bis 8,
wobei Änderungen an Patientendaten und/oder Ergebnisdaten mittels einer Signierung mit dem Blockchain-Prinzip protokolliert werden.

10. Computersystem (10) angepasst zum Ausführen eines computerimplementierten Verfahrens nach einem der Ansprüche 1 bis 9.

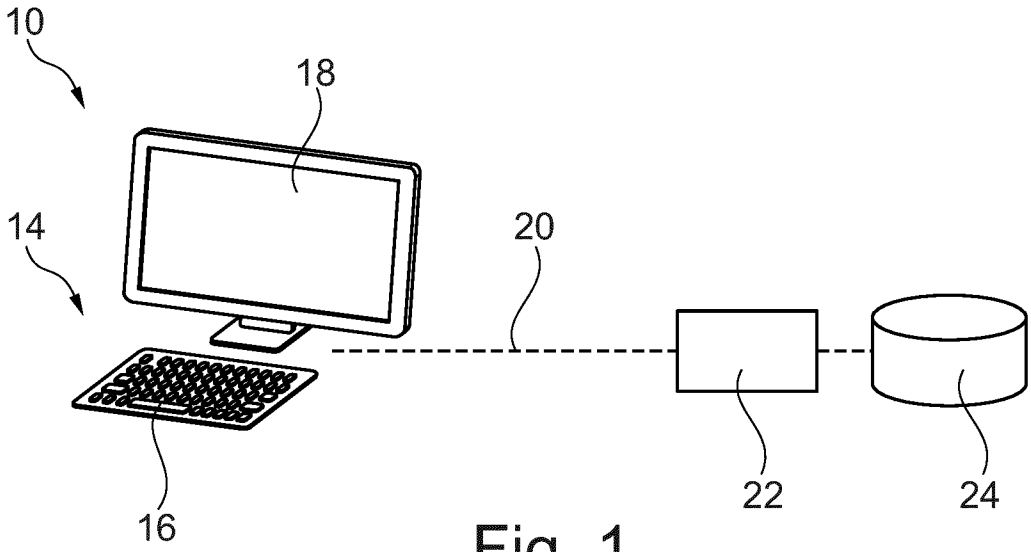

Fig. 1

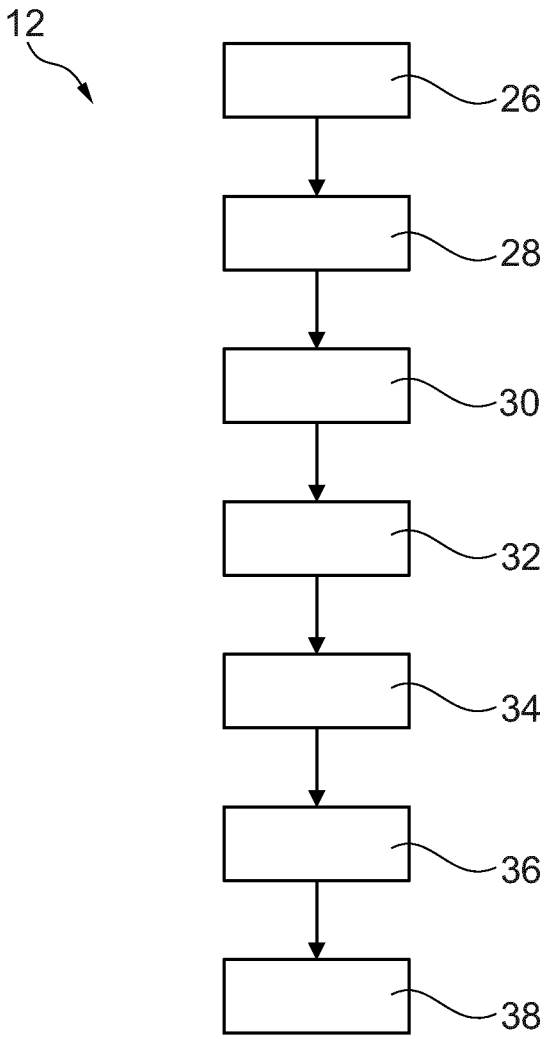

Fig. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2021/069452

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/62(2013.01)i; ***G16H 10/60***(2018.01)i; ***H04L 9/08***(2006.01)i; ***G06F 21/64***(2013.01)i

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; G16H; H04L

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	MAHESWARI S ET AL. "Secure sharing of personal health records in Jelastic cloud by attribute based encryption" *2017 4TH INTERNATIONAL CONFERENCE ON ADVANCED COMPUTING AND COMMUNICATION SYSTEMS (ICACCS), IEEE,* 06 January 2017 (2017-01-06), pages 1-4 DOI: 10.1109/ICACCS.2017.8014725 XP033144795 abstract sections I, III, IV	1-10
A	US 2003140043 A1 (HOTCHKISS ROBERT N [US] ET AL) 24 July 2003 (2003-07-24) abstract paragraph [0010] - paragraph [0029] paragraph [0072] - paragraph [0103]	1-10
A	US 2018167200 A1 (HIGH DONALD R [US] ET AL) 14 June 2018 (2018-06-14) abstract paragraph [0005] - paragraph [0008] paragraph [0019] - paragraph [0045]	1-10

☐ 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	Date of mailing of the international search report
31 August 2021	**10 September 2021**
Name and mailing address of the ISA/EP **European Patent Office** **p.b. 5818, Patentlaan 2, 2280 HV Rijswijk** **Netherlands** Telephone No. **(+31-70)340-2040** Facsimile No. **(+31-70)340-3016**	Authorized officer **Jakob, Gregor** Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/EP2021/069452

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2003140043 A1	24 July 2003	EP 1483692 A1	08 December 2004
		JP 2005516286 A	02 June 2005
		US 2003140043 A1	24 July 2003
		WO 03063031 A1	31 July 2003
US 2018167200 A1	14 June 2018	CA 3046218 A1	21 June 2018
		GB 2571869 A	11 September 2019
		US 2018167200 A1	14 June 2018
		WO 2018112035 A1	21 June 2018

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2021/069452

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G06F21/62 G16H10/60 H04L9/08 G06F21/64
ADD.

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G06F G16H H04L

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	MAHESWARI S ET AL: "Secure sharing of personal health records in Jelastic cloud by attribute based encryption", 2017 4TH INTERNATIONAL CONFERENCE ON ADVANCED COMPUTING AND COMMUNICATION SYSTEMS (ICACCS), IEEE, 6. Januar 2017 (2017-01-06), Seiten 1-4, XP033144795, DOI: 10.1109/ICACCS.2017.8014725 Zusammenfassung Sections I, III, IV -----	1-10
A	US 2003/140043 A1 (HOTCHKISS ROBERT N [US] ET AL) 24. Juli 2003 (2003-07-24) Zusammenfassung Absatz [0010] - Absatz [0029] Absatz [0072] - Absatz [0103] -----	1-10

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
31. August 2021	10/09/2021

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Jakob, Gregor

1

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2021/069452

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 2018/167200 A1 (HIGH DONALD R [US] ET AL) 14. Juni 2018 (2018-06-14) Zusammenfassung Absatz [0005] - Absatz [0008] Absatz [0019] - Absatz [0045] -----	1-10

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2021/069452

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2003140043 A1	24-07-2003	EP 1483692 A1	08-12-2004
		JP 2005516286 A	02-06-2005
		US 2003140043 A1	24-07-2003
		WO 03063031 A1	31-07-2003
US 2018167200 A1	14-06-2018	CA 3046218 A1	21-06-2018
		GB 2571869 A	11-09-2019
		US 2018167200 A1	14-06-2018
		WO 2018112035 A1	21-06-2018