



(12) **Veröffentlichung der Patentansprüche**

der europäischen Patentanmeldung mit der  
(97) Veröffentlichungsnummer: **EP 4 228 205**  
in deutscher Übersetzung (Art. II § 2 Abs. 1 IntPatÜbkG)  
(96) Europäisches Aktenzeichen: **22 18 1554.1**  
(96) Europäischer Anmeldetag: **28.06.2022**  
(97) Veröffentlichungstag  
der europäischen Anmeldung: **16.08.2023**  
(46) Veröffentlichungstag der Patentansprüche  
in deutscher Übersetzung: **02.11.2023**

(51) Int Cl.: **H04L 9/40 (2022.01)**  
**G06N 3/02 (2006.01)**

(30) Unionspriorität:  
**202263309646 P**      **14.02.2022**      **US**  
**202217829382**      **01.06.2022**      **US**

(74) Vertreter:  
**2K Patentanwälte Blasberg Kewitz & Reichel**  
**Partnerschaft mbB, 60325 Frankfurt, DE**

(71) Anmelder:  
**BlackBear (Taiwan) Industrial Networking**  
**Security Ltd., Jubei, Hsinchu, TW**

(72) Erfinder:  
**Chan, Yuan Chen, 302058 Jubei, Hsinchu, TW;**  
**Hsu, Po-Chih, 500 Changhua City, TW; Tsai, Chun-**  
**Hsien, 310 Hsinchu County, TW**

**Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.**

(54) Bezeichnung: **VERFAHREN ZUR SICHEREN DATENÜBERTRAGUNG UND SYSTEM, DAS DASSELBE VERWENDET**

(57) Hauptanspruch: System (10) zur sicheren Datenübertragung, das Folgendes umfasst:  
eine programmierbare Logikvorrichtung (200); und  
einen Server (100), der mit der programmierbaren Logikvorrichtung (200) gekoppelt ist, wobei der Server (100) konfiguriert ist, zum:  
Empfang eines ersten Datenpakets;  
Eingabe des ersten Datenpakets in ein maschinelles Lernmodell (121), um einen Protokolltyp und einen Befehlstyp des ersten Datenpakets vorherzusagen;  
Überprüfen, ob der Protokolltyp und der Befehlstyp korrekt sind,  
Hinzufügen des ersten Datenpakets zu einem Datenpaket-Informationssatz in Reaktion darauf, dass der Protokolltyp und der Befehlstyp korrekt sind; und  
Erzeugen einer Filterregel gemäß dem Datenpaket-Informationssatz und Einsetzen der Filterregel in der programmierbaren Logikvorrichtung (200),  
wobei die programmierbare Logikvorrichtung (200) die sichere Datenübertragung gemäß der Filterregel durchführt.

## Patentansprüche

1. System (10) zur sicheren Datenübertragung, das Folgendes umfasst:

eine programmierbare Logikvorrichtung (200); und einen Server (100), der mit der programmierbaren Logikvorrichtung (200) gekoppelt ist, wobei der Server (100) konfiguriert ist, zum:

Empfang eines ersten Datenpakets;

Eingabe des ersten Datenpakets in ein maschinelles Lernmodell (121), um einen Protokolltyp und einen Befehlstyp des ersten Datenpakets vorherzusagen; Überprüfen, ob der Protokolltyp und der Befehlstyp korrekt sind,

Hinzufügen des ersten Datenpakets zu einem Datenpaket-Informationssatz in Reaktion darauf, dass der Protokolltyp und der Befehlstyp korrekt sind; und

Erzeugen einer Filterregel gemäß dem Datenpaket-Informationssatz und Einsetzen der Filterregel in der programmierbaren Logikvorrichtung (200),

wobei die programmierbare Logikvorrichtung (200) die sichere Datenübertragung gemäß der Filterregel durchführt.

2. System (10) nach Anspruch 1, wobei der Server (100) die Filterregel erzeugt, durch:

Erhalten einer Vielzahl von Datenpaketen aus dem Datenpaket-Informationssatz, die dem Protokolltyp und dem Befehlstyp entsprechen;

Erhalten einer Vielzahl von Merkmalswerten aus der Vielzahl von Datenpaketen, die jeweils der Vielzahl von Datenpaketen entsprechen, wobei die Vielzahl von Merkmalswerten mindestens einen ersten Merkmalswert und mindestens einen zweiten Merkmalswert umfasst;

Auswählen des mindestens einen ersten Merkmalswerts aus dem mindestens einen ersten Merkmalswert und dem mindestens einen zweiten Merkmalswert als ausgewählter Merkmalswert in Reaktion darauf, dass eine erste Zahl des mindestens einen ersten Merkmalswerts größer ist als eine zweite Zahl des mindestens einen zweiten Merkmalswerts; und

Generieren der Filterregel, die dem Protokolltyp und dem Befehlstyp entspricht, entsprechend dem ausgewählten Merkmalswert.

3. System (10) nach Anspruch 2, wobei der ausgewählte Merkmalswert mindestens eines der folgenden Merkmale umfasst: eine Internetprotokolladresse, eine Medienzugriffskontrolladresse und eine Portnummer des Übertragungskontrollprotokolls.

4. System (10) nach Anspruch 2 oder 3, wobei die Filterregel umfasst:

Verwerfen eines zweiten Datenpakets, das dem Protokolltyp und dem Befehlstyp entspricht, in Reaktion auf einen Merkmalswert des zweiten Datenpa-

kets, der nicht mit dem ausgewählten Merkmalswert übereinstimmt.

5. System (10) nach Anspruch 4 ferner umfassend:

ein erstes Gateway (300), das mit der programmierbaren Logikvorrichtung (200) verbunden ist, wobei das erste Gateway (300) das zweite Datenpaket empfängt und das zweite Datenpaket an die programmierbare Logikvorrichtung (200) weiterleitet.

6. System (10) nach Anspruch 5, wobei das erste Gateway (300) mit dem Server (100) gekoppelt ist, wobei das erste Gateway (300) das erste Datenpaket empfängt und das erste Datenpaket an den Server (100) spiegelt.

7. System (10) nach Anspruch 5 oder 6, wobei das erste Gateway (300) das erste Datenpaket und das zweite Datenpaket von einem ersten Kommunikationsprotokoll in ein zweites Kommunikationsprotokoll umwandelt.

8. System (10) nach Anspruch 7 ferner umfassend:

ein zweites Gateway (500), das mit der programmierbaren Logikvorrichtung (200) gekoppelt ist, wobei das zweite Gateway (500) ein Datenpaket von der programmierbaren Logikvorrichtung (200) über die sichere Datenübertragung empfängt und das Datenpaket von dem zweiten Kommunikationsprotokoll in das erste Kommunikationsprotokoll umwandelt.

9. System (10) nach einem der Ansprüche 4 bis 8, ferner umfassend:

eine Diagnosevorrichtung (400), die mit der programmierbaren Logikvorrichtung (200) gekoppelt ist, wobei die Diagnosevorrichtung (400) das zweite Datenpaket empfängt, das von der programmierbaren Logikvorrichtung (200) verworfen wurde, und einen Bericht entsprechend dem zweiten Datenpaket erzeugt.

10. System (10) nach einem der vorhergehenden Ansprüche, wobei das maschinelle Lernmodell (121) ein faltbares neuronales Netz umfasst.

11. System (10) nach einem der vorhergehenden Ansprüche, wobei der Server (100) überprüft, ob der Protokolltyp und der Befehlstyp korrekt sind, durch:

Erhalten eines ersten Wertes von einem ersten Feld in dem ersten Datenpaket, wobei das erste Feld mit dem Protokolltyp verknüpft ist; und

Feststellen, dass der Protokolltyp korrekt ist, in Reaktion auf beide, den ersten Wert als auch einer Datenlänge des ersten Datenpakets, die mit dem Protokolltyp übereinstimmen.

12. System (10) nach einem der vorhergehenden Ansprüche, wobei der Server (100) überprüft, ob der Protokolltyp und der Befehlstyp korrekt sind, durch:

Erhalten eines zweiten Wertes von einem zweiten Feld in dem ersten Datenpaket, wobei das zweite Feld mit dem Befehlstyp verknüpft ist, der dem Protokolltyp entspricht;

Feststellen, dass der Befehlstyp korrekt ist in Reaktion darauf, dass der zweite Wert mit dem Befehlstyp übereinstimmt.

13. System (10) nach einem der vorhergehenden Ansprüche, wobei der Server (100) die Filterregel als Reaktion auf eine Anzahl von Datenpaketen in der Datenpaket-Informationssatzmenge erzeugt, die größer als ein Schwellenwert ist.

14. Verfahren zur sicheren Datenübertragung, umfassend:

Koppeln einer programmierbaren Logikeinheit mit einem Server;

Empfangen eines ersten Datenpakets durch den Server;

Eingeben des ersten Datenpakets in ein maschinelles Lernmodell, um einen Protokolltyp und einen Befehlstyp des ersten Datenpakets durch den Server vorherzusagen;

Überprüfen, ob der Protokolltyp und der Befehlstyp vom Server korrekt sind;

Hinzufügen des ersten Datenpakets zu einem Datenpaket-Informationssatz als Reaktion darauf, dass der Protokolltyp und der Befehlstyp vom Server korrekt sind;

Erzeugen einer Filterregel gemäß dem Datenpaket-Informationssatz und Bereitstellen der Filterregel in der programmierbaren Logikvorrichtung durch den Server; und

Durchführen der sicheren Datenübertragung gemäß der Filterregel durch die programmierbare Logikvorrichtung.

### geänderte Fassung

1. System (10) zur sicheren Datenübertragung, das Folgendes umfasst:

eine programmierbare Logikvorrichtung (200); und einen Server (100), der mit der programmierbaren Logikvorrichtung (200) gekoppelt ist, wobei der Server (100) konfiguriert ist, zum:

Empfang eines ersten Datenpakets;

Eingabe des ersten Datenpakets in ein maschinelles Lernmodell (121), um einen Protokolltyp und einen Befehlstyp des ersten Datenpakets vorherzusagen; Überprüfen, ob der Protokolltyp und der Befehlstyp korrekt sind, durch:

Erhalten eines ersten Wertes von einem ersten Feld in dem ersten Datenpaket und

Erhalten eines zweiten Wertes von einem zweiten Feld in dem ersten Datenpaket, wobei das erste

Feld mit dem Protokolltyp verknüpft ist und das zweite Feld mit dem Befehlstyp verknüpft ist, der dem Protokolltyp entspricht;

Feststellen, dass der Protokolltyp korrekt ist, in Reaktion darauf, dass beide, der erste Wert als auch eine Datenlänge des ersten Datenpakets mit dem Protokolltyp übereinstimmen; und

Feststellen, dass der Befehlstyp korrekt ist, wenn der zweite Wert mit dem Befehlstyp übereinstimmt; Hinzufügen des ersten Datenpakets zu einem Datenpaket-Informationssatz als Reaktion darauf, dass der Protokolltyp und der Befehlstyp korrekt sind; und

Erzeugen einer Filterregel gemäß dem Datenpaket-Informationssatz und Einsetzen der Filterregel in der programmierbaren Logikvorrichtung (200), wobei die programmierbare Logikvorrichtung (200) die sichere Datenübertragung gemäß der Filterregel durchführt.

2. System (10) nach Anspruch 1, wobei der Server (100) die Filterregel erzeugt, durch:

Erhalten einer Vielzahl von Datenpaketen aus dem Datenpaket-Informationssatz, die dem Protokolltyp und dem Befehlstyp entsprechen;

Erhalten einer Vielzahl von Merkmalswerten aus der Vielzahl von Datenpaketen, die jeweils der Vielzahl von Datenpaketen entsprechen, wobei die Vielzahl von Merkmalswerten mindestens einen ersten Merkmalswert und mindestens einen zweiten Merkmalswert umfasst;

Auswählen des mindestens einen ersten Merkmalswerts aus dem mindestens einen ersten Merkmalswert und dem mindestens einen zweiten Merkmalswert als ausgewählter Merkmalswert in Reaktion darauf, dass eine erste Zahl des mindestens einen ersten Merkmalswerts größer ist als eine zweite Zahl des mindestens einen zweiten Merkmalswerts; und

Generieren der Filterregel, die dem Protokolltyp und dem Befehlstyp entspricht, entsprechend dem ausgewählten Merkmalswert.

3. System (10) nach Anspruch 2, wobei der ausgewählte Merkmalswert mindestens eines der folgenden Merkmale umfasst: eine Internetprotokolladresse, eine Medienzugriffskontrolladresse und eine Portnummer des Übertragungskontrollprotokolls.

4. System (10) nach Anspruch 2 oder 3, wobei die Filterregel umfasst:

Verwerfen eines zweiten Datenpakets, das dem Protokolltyp und dem Befehlstyp entspricht, in Reaktion auf einen Merkmalswert des zweiten Datenpakets, der nicht mit dem ausgewählten Merkmalswert übereinstimmt.

5. System (10) nach Anspruch 4 ferner umfassend: ein erstes Gateway (300), das mit der programmier-

baren Logikvorrichtung (200) verbunden ist, wobei das erste Gateway (300) das zweite Datenpaket empfängt und das zweite Datenpaket an die programmierbare Logikvorrichtung (200) weiterleitet.

6. System (10) nach Anspruch 5, wobei das erste Gateway (300) mit dem Server (100) gekoppelt ist, wobei das erste Gateway (300) das erste Datenpaket empfängt und das erste Datenpaket an den Server (100) spiegelt.

7. System (10) nach Anspruch 5 oder 6, wobei das erste Gateway (300) das erste Datenpaket und das zweite Datenpaket von einem ersten Kommunikationsprotokoll in ein zweites Kommunikationsprotokoll umwandelt.

8. System (10) nach Anspruch 7 ferner umfassend:  
ein zweites Gateway (500), das mit der programmierbaren Logikvorrichtung (200) gekoppelt ist, wobei das zweite Gateway (500) ein Datenpaket von der programmierbaren Logikvorrichtung (200) über die sichere Datenübertragung empfängt und das Datenpaket von dem zweiten Kommunikationsprotokoll in das erste Kommunikationsprotokoll umwandelt.

9. System (10) nach einem der Ansprüche 4 bis 8, ferner umfassend:  
eine Diagnosevorrichtung (400), die mit der programmierbaren Logikvorrichtung (200) gekoppelt ist, wobei die Diagnosevorrichtung (400) das zweite Datenpaket empfängt, das von der programmierbaren Logikvorrichtung (200) verworfen wurde, und einen Bericht entsprechend dem zweiten Datenpaket erzeugt.

10. System (10) nach einem der vorhergehenden Ansprüche, wobei das maschinelle Lernmodell (121) ein faltbares neuronales Netz umfasst.

11. System (10) nach einem der vorhergehenden Ansprüche, wobei der Server (100) die Filterregel als Reaktion auf eine Anzahl von Datenpaketen in der Datenpaket-Informationsmenge erzeugt, die größer als ein Schwellenwert ist.

12. Verfahren zur sicheren Datenübertragung, das Folgendes umfasst:  
(S510) Koppeln einer programmierbaren Logikeinheit mit einem Server;  
(S520) Empfangen eines ersten Datenpakets durch den Server;  
(S530) Eingeben des ersten Datenpakets in ein maschinelles Lernmodell, um einen Protokolltyp und einen Befehlstyp des ersten Datenpakets durch den Server vorherzusagen;  
(S540) Überprüfen, ob der Protokolltyp und der Befehlstyp vom Server korrekt sind, durch:

Erhalten eines ersten Wertes von einem ersten Feld in dem ersten Datenpaket und Erhalten eines zweiten Wertes von einem zweiten Feld in dem ersten Datenpaket, wobei das erste Feld mit dem Protokolltyp verknüpft ist und das zweite Feld mit dem Befehlstyp verknüpft ist, der dem Protokolltyp entspricht;

Feststellen, dass der Protokolltyp korrekt ist, wenn sowohl der erste Wert als auch eine Datenlänge des ersten Datenpakets mit dem Protokolltyp übereinstimmen; und

Feststellen, dass der Befehlstyp korrekt ist, wenn der zweite Wert mit dem Befehlstyp übereinstimmt; (S550) Hinzufügen des ersten Datenpakets zu einem Datenpaket-Informationssatz als Reaktion darauf, dass der Protokolltyp und der Befehlstyp vom Server korrekt sind;

(S560) Erzeugen einer Filterregel gemäß dem Datenpaket-Informationssatz und Bereitstellen der Filterregel in der programmierbaren Logikvorrichtung durch den Server; und

(S570) Durchführen der sicheren Datenübertragung gemäß der Filterregel durch die programmierbare Logikvorrichtung.