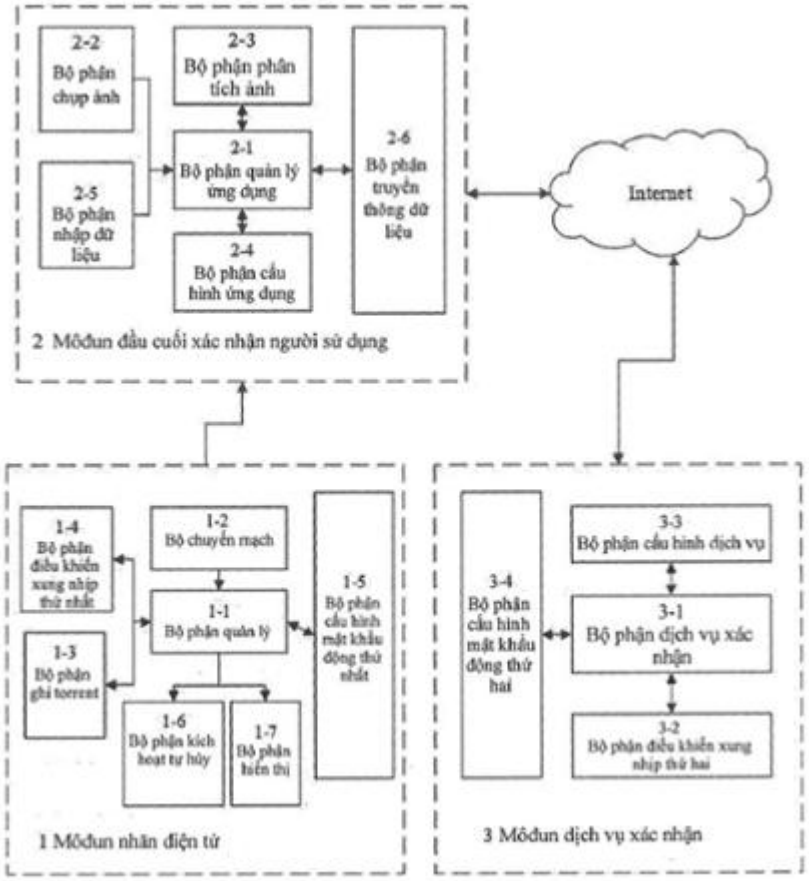
(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ
(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ
(11) **1-0032648**
(51)[7] **H04L 9/32**
(13) **B**

(21) 1-2016-02160
(22) 15/04/2015
(86) PCT/CN2015/076685 15/04/2015
(87) WO 2016/065861 06/05/2016
(30) 201410605962.X 31/10/2014 CN
(45) 25/07/2022 412
(43) 25/08/2017 353A
(73) HANGZHOU WOPUWULIAN SCIENCE & TECHNOLOGY CO., LTD. (CN)
Room 607, 6th Floor, No.6 Building, Jingchang Road No.768, Wuchang Street, Yuhang District Hangzhou, Zhejiang 311100, Republic of China
(72) FAN, Xiaodong (CN).
(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) PHƯƠNG PHÁP VÀ HỆ THỐNG XÁC NHẬN THEO THỜI GIAN THỰC TÍNH HỢP LỆ CỦA NHÃN BẢO MẬT MẬT KHẨU ĐỘNG ĐƯỢC ĐỒNG BỘ HÓA XUNG NHỊP

(57) Sáng chế đề cập đến hệ thống và phương pháp xác nhận theo thời gian thực tính hợp lệ của nhãn an ninh mật khẩu động được đồng bộ hóa xung nhịp, hệ thống này bao gồm, môđun nhãn điện tử, môđun thiết bị đầu cuối xác nhận người dùng, và mô đun cung cấp xác nhận. Môđun nhãn điện tử được sử dụng để tạo ra dữ liệu mật khẩu động và hiển thị. Môđun thiết bị đầu cuối xác nhận người dùng này chụp ảnh dữ liệu mật khẩu động được tạo ra bởi môđun nhãn điện tử và dữ liệu ảnh của số nhận dạng (ID) của môđun nhãn điện tử này. Sau khi xử lý phân tích, thu được dữ liệu văn bản, và sau đó dữ liệu văn bản này được gửi đến môđun cung cấp xác nhận qua internet. Sau khi nhận được dữ liệu văn bản này, môđun cung cấp xác nhận sẽ thu được kết quả là liệu thuật toán tạo ra dữ liệu mật khẩu động thứ nhất của môđun nhãn điện tử có nhất quán với thuật toán tạo ra dữ liệu mật khẩu động thứ hai của môđun cung cấp xác nhận này hay không. Kết quả này được trả lại cho môđun thiết bị đầu cuối xác nhận người dùng. Tính hợp lệ của môđun nhãn điện tử được xác định. Sáng chế nâng cao mức độ quản lý chuyên biệt và mức độ an toàn của hệ thống xác nhận theo thời gian thực tính hợp lệ của nhãn an ninh mật khẩu động được đồng bộ hóa xung nhịp.


2-2
Bộ phận chụp ảnh
2-3
Bộ phận phân tích ảnh
2-1
Bộ phận quản lý ứng dụng
2-4
Bộ phận cấu hình ứng dụng
2-5
Bộ phận nhập dữ liệu
2-6
Bộ phận truyền thông dữ liệu
Internet
2 Môđun đầu cuối xác nhận người sử dụng
1-4
Bộ phận điều khiển xung nhịp thứ nhất
1-2
Bộ chuyển mạch
1-1
Bộ phận quản lý
1-5
Bộ phận cấu hình mật khẩu động thứ nhất
1-3
Bộ phận ghi torrent
1-6
Bộ phận kích hoạt tự hủy
1-7
Bộ phận hiển thị
1 Môđun nhận điện tử
3-4
Bộ phận cấu hình mật khẩu động thứ hai
3-3
Bộ phận cấu hình dịch vụ
3-1
Bộ phận dịch vụ xác nhận
3-2
Bộ phận điều khiển xung nhịp thứ hai
3 Môđun dịch vụ xác nhận

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực bảo mật điện tử, cụ thể là đề cập đến hệ thống và phương pháp xác nhận theo thời gian thực tính hợp lệ của nhãn bảo mật mật khẩu động được đồng bộ hóa xung nhịp.

Tình trạng kỹ thuật của sáng chế

Với sự phát triển nhanh chóng của xã hội, khả năng tiêu dùng của con người luôn được nâng cao. Nhiều tội phạm bắt đầu thu được lợi nhuận rất lớn nhờ hàng giả. Điều này không chỉ gây ra nguy hiểm về kinh tế và thậm chí là về thể chất cho con người, mà còn gây ra các tác động xấu nghiêm trọng đối với sự phát triển của xã hội. Trong môi trường như vậy, lĩnh vực chống hàng giả càng ngày càng trở nên quan trọng. Tuy nhiên, nhãn bảo mật phổ biến thường theo các dạng laze, thẻ cào, mã vạch, mã chiều v.v.. Mỗi loại nhãn có tính thuận tiện riêng của nó, nhưng tất cả các loại nhãn này đều không thể thay đổi được, và có thể bị sao chép dễ dàng.

RFID (Radio Frequency Identification - nhận dạng tần số vô tuyến) và NFC (Near-Field Communication - truyền thông trường gần) là các dạng phổ biến được sử dụng trong lĩnh vực môđun nhãn điện tử. Các nhãn này đều yêu cầu các thiết bị đầu cuối xác nhận chuyên dụng để đọc, và dựa vào hệ thống chuyên nghiệp để xác nhận tính hợp lệ. Điều này không có lợi cho việc phổ biến đến người sử dụng, cũng như không sẵn có cho người sử dụng thực hiện xác nhận theo thời gian thực ở mọi lúc, mọi nơi.

Đầu ra của thẻ mật khẩu động là mật khẩu thay đổi theo thời gian mà chỉ có giá trị một lần. Nó có các tính năng chống giả mạo. Tuy nhiên, thẻ mật khẩu động kiểu xung nhịp thông thường được sử dụng chủ yếu trong ngân hàng trực tuyến đối với hệ thống xác nhận nhận dạng. Người sử dụng cần đăng nhập trang web trước,

và sau đó nhập dữ liệu mật khẩu động một cách thủ công vào máy chủ để xác nhận. Nếu điều này được áp dụng vào lĩnh vực bảo mật, thì hiển nhiên là sẽ bất tiện cho người sử dụng khi sử dụng, rồi sau đó sẽ dẫn đến việc nó không được ưa chuộng.

Bản chất kỹ thuật của sáng chế

Mục đích của một phương án của sáng chế là đề xuất hệ thống và phương pháp xác nhận theo thời gian thực tính hợp lệ của nhãn bảo mật mật khẩu động được đồng bộ hóa xung nhịp, nhằm giải quyết vấn đề sau đây trong lĩnh vực môđun nhãn điện tử, tức là, thiết bị đầu cuối xác nhận chuyên dụng được yêu cầu đọc và hệ thống chuyên nghiệp được dựa vào để xác minh tính hợp lệ, mà bất lợi cho việc phổ biến và bất tiện cho người sử dụng khi sử dụng mọi lúc mọi nơi.

Một phương án của sáng chế đề xuất phương pháp xác nhận theo thời gian thực tính hợp lệ của nhãn bảo mật mật khẩu động được đồng bộ hóa xung nhịp. Phương pháp xác nhận theo thời gian thực tính hợp lệ của nhãn bảo mật mật khẩu động được đồng bộ hóa xung nhịp bao gồm các bước sau.

Bước một, gán số ID (identification - định danh) duy nhất cho mỗi môđun nhãn điện tử, trong đó số ID được thể hiện là IDS1 và được bố trí trên bề mặt của môđun nhãn điện tử. Chu kỳ tích lũy xung nhịp đồng nhất được quy định trong môđun nhãn điện tử và môđun máy chủ xác nhận. Thông tin sản phẩm và thông tin có liên quan được ghi vào bộ phận cấu hình dịch vụ, trong đó thông tin sản phẩm và thông tin có liên quan được đại diện bởi số ID IDS1 của môđun nhãn điện tử. Tệp torrent để kết hợp môđun nhãn điện tử với môđun dịch vụ xác nhận được xác định, trong đó tệp torrent bao gồm dữ liệu xung nhịp DSS1, số ngẫu nhiên RandomD, và số ID IDS1 của môđun nhãn điện tử. Việc lưu trữ dữ liệu TDSH trong bộ phận cấu hình ứng dụng thể hiện rằng thiết bị tự hủy của môđun nhãn điện tử đã bị hỏng. Trường PSW, mà được sử dụng để thể hiện loại thuật toán tạo mật khẩu động được sử dụng bởi môđun nhãn điện tử mà số ID của nó là IDS1, được ghi vào bản ghi tương ứng với số ID IDS1 trong bộ phận cấu hình dịch vụ.

Bước hai, người sử dụng bật môđun nhãn điện tử thông qua bộ phận chuyển mạch. Bộ phận quản lý phát hiện xem liệu bộ phận kích khởi tự hủy có bị hỏng hay không. Nếu bộ phận kích khởi tự hủy bị hỏng, môđun nhãn điện tử xuất ra dữ liệu cụ thể TDSH qua bộ phận hiển thị, mà thể hiện rằng môđun nhãn điện tử đã ngừng làm việc. Nếu bộ phận kích khởi tự hủy làm việc bình thường, thì bộ phận quản lý của môđun nhãn điện tử khởi tạo dữ liệu xung nhịp ở DSS1 tại chu kỳ thay đổi xung nhịp thứ nhất theo chu kỳ thay đổi xung nhịp của bộ phận điều khiển xung nhịp. Bộ phận quản lý sử dụng dữ liệu xung nhịp DSS1, số ngẫu nhiên RandomD, số ID IDS1 của nhãn điện tử trong tệp torrent, làm các hệ số tính toán, để tạo ra dữ liệu mật khẩu động thứ nhất DKS1 thông qua thuật toán tạo mật khẩu động PSW1 của bộ phận cấu hình mật khẩu động thứ nhất, và hiển thị DKS1 trên bộ phận hiển thị; sau đó bộ phận quản lý tích lũy dữ liệu xung nhịp ban đầu DSS1 theo chu kỳ tích lũy xung nhịp định trước để thu được dữ liệu xung nhịp thứ hai DSS2, và lưu trữ DDS2 vào bộ nhớ cache.

Bước ba, bộ phận quản lý ứng dụng của môđun đầu cuối xác nhận người sử dụng điều khiển bộ phận chụp ảnh để thu thập dữ liệu ảnh TDT1 của môđun nhãn điện tử, trong đó dữ liệu ảnh IDT1 của môđun nhãn điện tử bao gồm dữ liệu mật khẩu động được hiển thị trên bộ phận hiển thị, và số ID IDS1 của môđun nhãn điện tử được bố trí trên bề mặt của môđun nhãn điện tử. Bộ phận quản lý ứng dụng của môđun đầu cuối xác nhận người sử dụng bố trí, phân đoạn, và phân tích dữ liệu ảnh IDT1 thông qua bộ phận phân tích ảnh để thu được dữ liệu mật khẩu động DZXS được hiển thị trên bộ phận hiển thị của môđun nhãn điện tử và số ID IDS1 của môđun nhãn điện tử. Sau đó, việc tìm kiếm được tiến hành trong bộ phận cấu hình ứng dụng. Nếu DZXS bằng TDSH, mà chỉ báo rằng thiết bị tự hủy của môđun nhãn điện tử bị hỏng, quy trình xác nhận kết thúc. Nếu DZXS không bằng TDSH, IDS1 được lưu trữ vào bộ phận cấu hình ứng dụng. IDS1 và DZXS được gửi đến môđun dịch vụ xác nhận thông qua bộ phận truyền thông dữ liệu được kết nối với internet.

Hơn nữa, việc bật môđun nhãn điện tử thông qua bộ phận chuyển mạch xảy

ra sau bước một. Sau đó, tệp torrent được ghi qua bộ phận ghi torrent, trong khi đó, tệp torrent được ghi vào bản ghi tương ứng với số ID IDS1 của bộ phận cấu hình dịch vụ của môđun dịch vụ xác nhận thông qua internet.

Hơn nữa, sau bước ba, môđun dịch vụ xác nhận nhận dữ liệu IDS1 và DZXS được gửi từ môđun đầu cuối xác nhận người sử dụng. Sau đó, bộ phận dịch vụ xác nhận tìm kiếm bản ghi tương ứng với IDS1 trong bộ phận cấu hình dịch vụ nhờ sử dụng IDS1, và trích xuất thuật toán tạo mật khẩu động PSW2 được chấp nhận bởi môđun nhãn điện tử, mà được thể hiện bởi dữ liệu xung nhịp DSS1, số ngẫu nhiên RandomD, và IDS1 mà được ghi từ đầu vào tệp torrent. Sau đó, bộ phận dịch vụ xác nhận thu được thời gian hệ thống RSS1 của môđun dịch vụ xác nhận hiện thời, trừ DSS1 từ RSS1 để thu được kết quả. Kết quả được chia cho chu kỳ tích lũy xung nhịp được xác định ban đầu để thu được RZSC mà là số lần môđun nhãn điện tử được tích lũy theo chu kỳ tích lũy xung nhịp. Cuối cùng, dữ liệu mật khẩu động RKS1 được tính toán nhờ sử dụng RandomD, DSS1, RZSC, và IDS1 làm các hệ số tính toán thông qua thuật toán tạo mật khẩu động PSW2 của bộ phận cấu hình mật khẩu động thứ hai.

Bộ phận dịch vụ xác nhận so sánh RKS1 tính toán được với DZXS. Nếu RKS1 bằng DZXS, kết quả chỉ báo rằng môđun nhãn điện tử này là hợp lệ được gửi đến môđun đầu cuối xác nhận người sử dụng thông qua internet. Nếu RKS1 không bằng DZXS, kết quả chỉ báo rằng môđun nhãn điện tử này là không hợp lệ được gửi đến môđun đầu cuối xác nhận người sử dụng thông qua internet.

Sau khi môđun đầu cuối xác nhận người sử dụng nhận kết quả được phản hồi từ môđun dịch vụ xác nhận, môđun đầu cuối xác nhận người sử dụng hiển thị kết quả, để hoàn thành quy trình xác nhận tính hợp lệ này đối với môđun nhãn điện tử.

Một mục đích khác theo một phương án của sáng chế là đề xuất hệ thống xác nhận theo thời gian thực tính hợp lệ của nhãn bảo mật mật khẩu động được

đồng bộ hóa xung nhịp, trong đó hệ thống xác nhận theo thời gian thực tính hợp lệ của nhãn bảo mật mật khẩu động đồng bộ hóa xung nhịp bao gồm: môđun nhãn điện tử, môđun đầu cuối xác nhận người sử dụng, và môđun dịch vụ xác nhận.

Môđun nhãn điện tử được sử dụng để tạo ra dữ liệu mật khẩu động và hiển thị. Môđun nhãn điện tử bao gồm bộ phận quản lý, bộ phận chuyển mạch, bộ phận ghi torrent, bộ phận điều khiển xung nhịp thứ nhất, bộ phận cấu hình mật khẩu động thứ nhất, bộ phận kích khởi tự hủy, và bộ phận hiển thị.

Môđun đầu cuối xác nhận người sử dụng được kết nối với môđun nhãn điện tử. Nó được sử dụng để chụp dữ liệu mật khẩu động được tạo ra bởi môđun nhãn điện tử và dữ liệu ảnh của số ID của môđun nhãn điện tử. Sau khi phân tích, dữ liệu dạng văn bản được thu nhận. Sau đó, dữ liệu dạng văn bản được gửi đến môđun dịch vụ xác nhận thông qua internet. Môđun đầu cuối xác nhận người sử dụng bao gồm: bộ phận quản lý ứng dụng, bộ phận chụp ảnh, bộ phận phân tích ảnh, bộ phận cấu hình ứng dụng, bộ phận nhập dữ liệu, và bộ phận truyền thông dữ liệu.

Môđun dịch vụ xác nhận được kết nối với môđun đầu cuối xác nhận người sử dụng. Sau khi nhận dữ liệu dạng văn bản, môđun dịch vụ xác nhận được sử dụng để, sau khi tính toán và xác nhận, thu được kết quả xem liệu thuật toán tạo mật khẩu động thứ nhất của môđun nhãn điện tử có phù hợp với thuật toán tạo mật khẩu động thứ hai của môđun dịch vụ xác nhận hay không. Kết quả được trả về cho môđun đầu cuối xác nhận người sử dụng, để xác định tính hợp lệ của môđun nhãn điện tử. Môđun dịch vụ xác nhận bao gồm bộ phận dịch vụ xác nhận, bộ phận điều khiển xung nhịp thứ hai, bộ phận cấu hình dịch vụ, và bộ phận cấu hình mật khẩu động thứ hai.

Hơn nữa, môđun nhãn điện tử còn bao gồm bộ phận quản lý, bộ phận chuyển mạch, bộ phận ghi torrent, bộ phận điều khiển xung nhịp thứ nhất, bộ phận cấu hình mật khẩu động thứ nhất, bộ phận kích khởi tự hủy, và bộ phận hiển thị.

Bộ phận quản lý được sử dụng để phát hiện xem liệu bộ phận kích khởi tự hủy có bị hỏng hay không; khởi tạo dữ liệu xung nhịp ở DSS1 trong suốt chu kỳ thay đổi xung nhịp thứ nhất theo chu kỳ thay đổi xung nhịp của bộ phận điều khiển xung nhịp thứ nhất; sử dụng dữ liệu xung nhịp DSS1, số ngẫu nhiên RandomD, số ID IDS1 của môđun nhãn điện tử làm các hệ số tính toán, trong đó dữ liệu xung nhịp DSS1, số ngẫu nhiên RandomD, số ID IDS1 được lưu trữ trong tệp torrent; tạo ra dữ liệu mật khẩu động DKS1 thông qua thuật toán tạo mật khẩu động PSW1 của bộ phận cấu hình mật khẩu động thứ nhất, và sau đó hiển thị dữ liệu mật khẩu động thứ nhất DKS1 trên bộ phận hiển thị; sau đó thu được DSS2 bằng cách tích lũy dữ liệu xung nhịp ban đầu DSS1 theo chu kỳ tích lũy xung nhịp định trước, và lữu trữ DDS2 trong bộ nhớ cache.

Bộ phận chuyển mạch được kết nối với bộ phận quản lý, và được sử dụng để bật môđun nhãn điện tử.

Bộ phận ghi torrent được kết nối với bộ phận quản lý, và được sử dụng để ghi tệp torrent.

Bộ phận điều khiển xung nhịp thứ nhất được kết nối với bộ phận quản lý, và được sử dụng để xuất ra chu kỳ thay đổi xung nhịp.

Bộ phận cấu hình mật khẩu động thứ nhất được kết nối với bộ phận quản lý, và được sử dụng để tạo ra dữ liệu mật khẩu động thứ nhất DKS1 thông qua thuật toán tạo mật khẩu động PSW1.

Bộ phận kích khởi tự hủy được kết nối với bộ phận quản lý, và được sử dụng để gửi tín hiệu phá hủy.

Bộ phận hiển thị được kết nối với bộ phận quản lý, và được sử dụng để hiển thị dữ liệu mật khẩu động DKS1.

Hơn nữa, thuật toán tạo mật khẩu động thứ nhất trong bộ phận cấu hình mật khẩu động thứ nhất sử dụng thuật toán mã hóa trạng thái (State Encryption

Algorithm).

Bộ phận quản lý truyền số ID riêng của môđun nhãn điện tử và dữ liệu xung nhịp hoặc số lần tạo ra mật khẩu động như là các hệ số tính toán đến bộ phận cấu hình mật khẩu động thứ nhất, để thu được dữ liệu mật khẩu động. Dữ liệu mật khẩu động có thể sử dụng các số, các chữ, tổ hợp của các số và các chữ, mã vạch, mã hai chiều, hoặc dạng biểu diễn mật khẩu bất kỳ.

Môđun nhãn điện tử truyền dữ liệu đến môđun đầu cuối xác nhận người sử dụng nhờ sử dụng màn hình hiển thị, NFC, RFID, hồng ngoại, hoặc phương pháp truyền thông bất kỳ.

Hơn nữa, phương pháp xác nhận dữ liệu mật khẩu động của môđun nhãn điện tử, kết cấu của môđun đầu cuối xác nhận người sử dụng và môđun dịch vụ xác nhận. Bộ phận phân tích ảnh của môđun đầu cuối xác nhận người sử dụng được bố trí trong môđun dịch vụ xác nhận. Môđun đầu cuối xác nhận người sử dụng chỉ chịu trách nhiệm chụp dữ liệu mật khẩu động mà được hiển thị trên môđun nhãn điện tử, và gửi dữ liệu ảnh thu thập được đến môđun dịch vụ xác nhận. Môđun dịch vụ xác nhận phân tích dữ liệu ảnh, và chuyển đổi định dạng dữ liệu và xác nhận dữ liệu ảnh được chuyển đổi.

Phương pháp xác nhận mật khẩu động của môđun nhãn điện tử, kết cấu của môđun đầu cuối xác nhận người sử dụng và môđun dịch vụ xác nhận. Khi mạng kém, bộ phận dịch vụ xác nhận, bộ phận cấu hình dịch vụ, và bộ phận cấu hình mật khẩu động thứ hai trong môđun dịch vụ xác nhận được bố trí trong môđun đầu cuối xác nhận người sử dụng. Sau khi thu thập dữ liệu mật khẩu động của môđun nhãn điện tử, môđun đầu cuối xác nhận người sử dụng hoàn thành dịch vụ xác nhận một cách trực tiếp trong chế độ ngoại tuyến.

Hơn nữa, môđun đầu cuối xác nhận người sử dụng bao gồm: bộ phận quản lý ứng dụng, bộ phận chụp ảnh, bộ phận phân tích ảnh, bộ phận cấu hình ứng dụng,

bộ phận nhập dữ liệu, và bộ phận truyền thông dữ liệu.

Bộ phận quản lý ứng dụng được sử dụng để điều khiển bộ phận chụp ảnh để chụp dữ liệu ảnh IDT1 của môđun nhãn điện tử; bộ phận phân tích ảnh bố trí, phân đoạn, và phân tích dữ liệu ảnh IDT1, để thu được dữ liệu mật khẩu động DZXS được hiển thị trên bộ phận hiển thị và số ID IDS1 của môđun nhãn điện tử có thể được thu nhận. Sau đó, việc tìm kiếm được tiến hành trong bộ phận cấu hình ứng dụng.

Bộ phận chụp ảnh được kết nối với bộ phận quản lý ứng dụng, và được sử dụng để thu thập dữ liệu ảnh IDT1 của môđun nhãn điện tử.

Bộ phận phân tích ảnh được kết nối với bộ phận quản lý ứng dụng, và được sử dụng để bố trí, phân đoạn và phân tích dữ liệu ảnh IDT1.

Bộ phận cấu hình ứng dụng được kết nối với bộ phận quản lý ứng dụng, và được sử dụng để tìm kiếm xem liệu dữ liệu mật khẩu động DZXS có phù hợp với số ID IDS1 của môđun nhãn điện tử hay không.

Bộ phận nhập dữ liệu được kết nối với bộ phận quản lý ứng dụng, và được sử dụng để nhập dữ liệu mật khẩu động DZXS để tìm kiếm.

Bộ phận truyền thông dữ liệu được kết nối với bộ phận quản lý ứng dụng, và được sử dụng để gửi IDS1 và DZXS đến môđun dịch vụ xác nhận thông qua internet.

Hơn nữa, môđun dịch vụ xác nhận bao gồm bộ phận dịch vụ xác nhận, bộ phận điều khiển xung nhịp thứ hai, bộ phận cấu hình dịch vụ, và bộ phận cấu hình mật khẩu động thứ hai.

Bộ phận dịch vụ xác nhận được sử dụng để trích xuất thuật toán tạo mật khẩu động PSW2 được chấp nhận bởi môđun nhãn điện tử, mà được thể hiện bởi dữ liệu xung nhịp DSS1, số ngẫu nhiên RandomD, và số ID IDS1 mà được ghi từ

đầu vào tệp torrent; thu nhận thời gian hệ thống RSS1 của môđun dịch vụ xác nhận hiện thời; tính toán dữ liệu mật khẩu động RKS1 thông qua thuật toán tạo mật khẩu động PSW2 của bộ phận cấu hình mật khẩu động thứ hai; so sánh RKS1 tính toán được với DZXS.

Bộ phận điều khiển xung nhịp thứ hai được kết nối với bộ phận dịch vụ xác nhận, và được sử dụng để cung cấp tín hiệu xung nhịp cho bộ phận dịch vụ xác nhận.

Bộ phận cấu hình dịch vụ được kết nối với bộ phận dịch vụ xác nhận, và được sử dụng để tìm kiếm bản ghi tương ứng với IDS1.

Bộ phận cấu hình mật khẩu động thứ hai được kết nối với bộ phận dịch vụ xác nhận, và được sử dụng để tính toán dữ liệu mật khẩu động RKS1 thông qua thuật toán tạo mật khẩu động PSW2.

Hơn nữa, bộ phận cấu hình dịch vụ là cơ sở dữ liệu mà có thể được đọc và được ghi bởi bộ phận dịch vụ xác nhận. Bộ phận cấu hình dịch vụ tạo cấu hình đặc tính của môđun nhãn điện tử nhờ sử dụng ID của môđun nhãn điện tử này, và lưu trữ thông tin sản phẩm được thể hiện bởi môđun nhãn điện tử và đặc tính của môđun nhãn điện tử trong cơ sở dữ liệu.

Nhiều thuật toán tạo mật khẩu động tương ứng với môđun nhãn điện tử được đặt trong bộ phận cấu hình mật khẩu động thứ hai của môđun dịch vụ xác nhận.

Sáng chế đề xuất hệ thống và phương pháp xác nhận theo thời gian thực tính hợp lệ của nhãn bảo mật mật khẩu động đồng bộ hóa xung nhịp, tạo cấu hình môđun nhãn điện tử, môđun đầu cuối xác nhận người sử dụng, và môđun dịch vụ xác nhận. Sáng chế khắc phục tính bất biến và tính sao chép của các nhãn hiện có. Kỹ thuật nhận dạng ảnh được sử dụng, cung cấp phương pháp xác nhận thuận tiện cho người sử dụng. Thiết bị tự hủy được chấp nhận, mà cho phép người sử dụng xác nhận trước khi hành vi mua xảy ra. Sự kết hợp của nhiều thuật toán mật khẩu

động được sử dụng, để nâng cao đáng kể độ an toàn của mật khẩu động. Các dữ liệu khác nhau ẩn trong môđun nhãn điện tử được sử dụng, cụ thể là sử dụng số ngẫu nhiên và dữ liệu xung nhịp làm các hệ số tính toán, sao cho mỗi môđun nhãn điện tử có mật khẩu khác nhau. Trong khi đó, dữ liệu mật khẩu được tạo ra bởi mỗi môđun nhãn điện tử chỉ có giá trị một lần, điều này nâng cao đáng kể độ an toàn của hệ thống. Sáng chế phù hợp với thuật toán tạo mật khẩu theo ID của môđun nhãn điện tử, điều này nâng cao đáng kể việc quản lý cá nhân hóa của hệ thống xác nhận theo thời gian thực tính hợp lệ của nhãn bảo mật mật khẩu động được đồng bộ hóa xung nhịp, và cũng làm tăng đáng kể độ an toàn của hệ thống xác nhận theo thời gian thực tính hợp lệ của nhãn bảo mật mật khẩu động được đồng bộ hóa xung nhịp.

Mô tả vắn tắt các hình vẽ

Fig.1 là sơ đồ giản lược của hệ thống xác nhận theo thời gian thực tính hợp lệ của nhãn bảo mật mật khẩu động được đồng bộ hóa xung nhịp được đề xuất bởi một phương án của sáng chế.

Fig.2 là lưu đồ của phương pháp xác nhận theo thời gian thực tính hợp lệ của nhãn bảo mật mật khẩu động được đồng bộ hóa xung nhịp được đề xuất bởi một phương án của sáng chế.

Fig.3 là hệ thống xác nhận theo thời gian thực tính hợp lệ của nhãn bảo mật mật khẩu động được đồng bộ hóa xung nhịp theo phương án thứ hai được đề xuất bởi một phương án của sáng chế.

Fig.4 là hệ thống xác nhận theo thời gian thực tính hợp lệ của nhãn bảo mật mật khẩu động được đồng bộ hóa xung nhịp theo phương án thứ ba được đề xuất bởi một phương án của sáng chế.

Trong đó: 1. Môđun nhãn điện tử; 1-1. Bộ phận quản lý; 1-2. Bộ phận chuyển mạch; 1-3. Bộ phận ghi torrent; 1-4. Bộ phận điều khiển xung nhịp thứ nhất;

1-5. Bộ phận cấu hình mật khẩu động thứ nhất; 1-6. Bộ phận kích khởi tự hủy; 1-7. Bộ phận hiển thị; 2. Môđun đầu cuối xác nhận người sử dụng; 2-1 Bộ phận quản lý ứng dụng; 2-2. Bộ phận chụp ảnh; 2-3. Bộ phận phân tích ảnh; 2-4. Bộ phận cấu hình ứng dụng; 2-5. Bộ phận nhập dữ liệu; 2-6. Bộ phận truyền thông dữ liệu; 3. Môđun dịch vụ xác nhận; 3-1. Bộ phận dịch vụ xác nhận; 3-2. Bộ phận điều khiển xung nhịp thứ hai; 3-3. Bộ phận cấu hình dịch vụ; 3-4. Bộ phận cấu hình mật khẩu động thứ hai.

Mô tả chi tiết sáng chế

Để làm sáng tỏ mục đích, giải pháp kỹ thuật, và các ưu điểm của sáng chế, phần mô tả chi tiết hơn nữa kết hợp với các phương án được thể hiện dưới đây. Cần hiểu rằng các phương án ở đây chỉ được sử dụng để minh họa sáng chế. Tuy nhiên, sáng chế không bị giới hạn ở đó.

Nguyên lý của sáng chế còn được mô tả kết hợp với các hình vẽ và các phương án cụ thể như sau.

Như được thể hiện trên Fig.1, hệ thống xác nhận theo thời gian thực tính hợp lệ của nhãn bảo mật mật khẩu động được đồng bộ hóa xung nhịp theo một phương án của sáng chế bao gồm: môđun nhãn điện tử 1, môđun đầu cuối xác nhận người sử dụng 2, và môđun dịch vụ xác nhận 3.

Môđun nhãn điện tử 1 được sử dụng để tạo ra dữ liệu mật khẩu động và hiển thị dữ liệu mật khẩu động.

Môđun đầu cuối xác nhận người sử dụng 2 được kết nối với môđun nhãn điện tử 1, và được sử dụng để chụp dữ liệu mật khẩu động được tạo ra bởi môđun nhãn điện tử 1 và dữ liệu ảnh của số ID của môđun nhãn điện tử; sau khi phân tích, dữ liệu dạng văn bản được thu nhận. Sau đó, dữ liệu dạng văn bản này được gửi đến môđun dịch vụ xác nhận 3 thông qua internet.

Môđun dịch vụ xác nhận 3 được kết nối với môđun đầu cuối xác nhận người

sử dụng 2. Sau khi nhận dữ liệu dạng văn bản, môđun dịch vụ xác nhận được sử dụng để, sau khi tính toán và xác nhận, thu nhận kết quả xem liệu thuật toán tạo ra dữ liệu mật khẩu động thứ nhất của môđun nhãn điện tử 1 có phù hợp với thuật toán tạo ra dữ liệu mật khẩu động thứ hai của môđun dịch vụ xác nhận 3 hay không, và trả kết quả này cho môđun đầu cuối xác nhận người sử dụng 2, để xác định tính hợp lệ của môđun nhãn điện tử 1.

Môđun nhãn điện tử 1 còn bao gồm bộ phận quản lý 1-1, bộ phận chuyển mạch 1-2, bộ phận ghi torrent 1-3, bộ phận điều khiển xung nhịp thứ nhất 1-4, bộ phận cấu hình mật khẩu động thứ nhất 1-5, bộ phận kích khởi tự hủy 1-6, và bộ phận hiển thị 1-7.

Bộ phận quản lý 1-1 được sử dụng để phát hiện liệu bộ phận kích khởi tự hủy 1-6 có bị hỏng hay không, khởi tạo dữ liệu xung nhịp ở DSS1 trong suốt chu kỳ thay đổi xung nhịp thứ nhất theo chu kỳ thay đổi xung nhịp của bộ phận điều khiển xung nhịp thứ nhất 1-4; tạo ra dữ liệu mật khẩu động DKS1 bởi thuật toán tạo mật khẩu động PSW1 của bộ phận cấu hình mật khẩu động thứ nhất 1-5 bằng cách sử dụng dữ liệu xung nhịp DSS1, số ngẫu nhiên RandomD, số ID IDS1 của môđun nhãn điện tử 1 trong dữ liệu torrent làm các hệ số tính toán; và hiển thị DKS1 trên bộ phận hiển thị 1-7; sau đó tích lũy dữ liệu xung nhịp ban đầu DSS1 theo chu kỳ tích lũy xung nhịp định trước để thu được DSS2, và lữu trữ DDS2 trong bộ nhớ cache.

Bộ phận chuyển mạch 1-2 được kết nối với bộ phận quản lý 1-1, và được sử dụng để bật môđun nhãn điện tử 1.

Bộ phận ghi torrent 1-3 được kết nối với bộ phận quản lý 1-1, và được sử dụng để ghi tệp torrent.

Bộ phận điều khiển xung nhịp thứ nhất 1-4 được kết nối với bộ phận quản lý 1-1, và được sử dụng để xuất ra chu kỳ thay đổi xung nhịp.

Bộ phận cấu hình mật khẩu động thứ nhất 1-5 được kết nối với bộ phận quản lý 1-1, và được sử dụng để tạo ra dữ liệu mật khẩu động DKS1 thông qua thuật toán tạo mật khẩu động PSW1.

Bộ phận kích khởi tự hủy 1-6 được kết nối với bộ phận quản lý 1-1, và được sử dụng để gửi tín hiệu phá hủy.

Bộ phận hiển thị 1-7 được kết nối với bộ phận quản lý 1-1, và được sử dụng để hiển thị dữ liệu mật khẩu động DKS1.

Môđun đầu cuối xác nhận người sử dụng 2 bao gồm: bộ phận quản lý ứng dụng 2-1, bộ phận chụp ảnh 2-2, bộ phận phân tích ảnh 2-3, bộ phận cấu hình ứng dụng 2-4, bộ phận nhập dữ liệu 2-5, và bộ phận truyền thông dữ liệu 2-6.

Bộ phận quản lý ứng dụng 2-1 được sử dụng để điều khiển bộ phận chụp ảnh 2-2 chụp dữ liệu ảnh IDT1 của môđun nhãn điện tử. Bộ phận phân tích ảnh 2-3 bố trí, phân đoạn, và phân tích dữ liệu ảnh IDT1, để thu được dữ liệu mật khẩu động DZXS được hiển thị trên bộ phận hiển thị 1-7 của môđun nhãn điện tử 1, và số ID IDS1 của nhãn điện tử; và sau đó tìm kiếm trong bộ phận cấu hình ứng dụng 2-4.

Bộ phận chụp ảnh 2-2 được kết nối với bộ phận quản lý ứng dụng 2-1, và được sử dụng để chụp dữ liệu ảnh IDT1 của môđun nhãn điện tử.

Bộ phận phân tích ảnh 2-3 được kết nối với bộ phận quản lý ứng dụng 2-1, và được sử dụng để bố trí, phân đoạn, và phân tích dữ liệu ảnh IDT1.

Bộ phận cấu hình ứng dụng 2-4 được kết nối với bộ phận quản lý ứng dụng 2-1, và được sử dụng để tìm kiếm xem liệu dữ liệu mật khẩu động DZXS có phù hợp với số ID IDS1 của môđun nhãn điện tử hay không. Bộ phận nhập dữ liệu 2-5 được kết nối với bộ phận quản lý ứng dụng 2-1, và được sử dụng để nhập dữ liệu mật khẩu động DZXS để tìm kiếm.

Bộ phận truyền thông dữ liệu 2-6 được kết nối với bộ phận quản lý ứng dụng 2-1, và được sử dụng để gửi IDS1 và DZXS đến môđun dịch vụ xác nhận 3 thông qua internet.

Môđun dịch vụ xác nhận 3 còn bao gồm bộ phận dịch vụ xác nhận 3-1, bộ phận điều khiển xung nhịp thứ hai 3-2, bộ phận cấu hình dịch vụ 3-3, và bộ phận cấu hình mật khẩu động thứ hai 3-4.

Bộ phận dịch vụ xác nhận 3-1 được sử dụng để trích xuất thuật toán tạo mật khẩu động PSW2 được chấp nhận bởi môđun nhãn điện tử, mà được thể hiện bởi dữ liệu xung nhịp DSS1, số ngẫu nhiên RandomD, và IDS1 mà được ghi từ đầu vào tệp torrent. Thời gian hệ thống RSS1 của môđun dịch vụ xác nhận hiện thời được thu nhận. Dữ liệu mật khẩu động RKS1 được tính toán thông qua thuật toán tạo mật khẩu động PSW2 của bộ phận cấu hình mật khẩu động thứ hai 3-4. Dữ liệu mật khẩu động đã tính RKS1 được so sánh với dữ liệu mật khẩu động DZXS.

Bộ phận điều khiển xung nhịp thứ hai 3-2 được kết nối với bộ phận dịch vụ xác nhận 3-1, và được sử dụng để cung cấp tín hiệu xung nhịp cho bộ phận dịch vụ xác nhận 3-1.

Bộ phận cấu hình dịch vụ 3-3 được kết nối với bộ phận dịch vụ xác nhận 3-1, và được sử dụng để tìm kiếm bản ghi tương ứng với số ID IDS1.

Bộ phận cấu hình mật khẩu động thứ hai 3-4 được kết nối với bộ phận dịch vụ xác nhận 3-1, và được sử dụng để tính toán dữ liệu mật khẩu động RKS1 thông qua thuật toán tạo mật khẩu động PSW2.

Như được thể hiện trên Fig.2, một phương án về phương pháp xác nhận theo thời gian thực tính hợp lệ của nhãn bảo mật mật khẩu động được đồng bộ hóa xung nhịp, bao gồm các bước sau.

S201: gán số ID duy nhất cho mỗi môđun nhãn điện tử, trong đó số ID được thể hiện là IDS1, và được bố trí trên bề mặt của môđun nhãn điện tử. Chu kỳ tích

lũy xung nhịp đồng nhất được quy định trong môđun nhãn điện tử và môđun máy chủ xác nhận. Thông tin sản phẩm và thông tin có liên quan được ghi vào bộ phận cấu hình dịch vụ, trong đó thông tin sản phẩm và thông tin có liên quan được đại diện bởi số ID IDS1 của môđun nhãn điện tử. Tệp torrent để kết hợp môđun nhãn điện tử với môđun dịch vụ xác nhận được xác định, trong đó tệp torrent bao gồm dữ liệu xung nhịp DSS1, số ngẫu nhiên RandomD, và số ID IDS1 của môđun nhãn điện tử. Việc lưu trữ dữ liệu TDSH trong bộ phận cấu hình ứng dụng thể hiện rằng thiết bị tự hủy của môđun nhãn điện tử đã bị hỏng. Trường PSW, mà được sử dụng để đại diện cho loại thuật toán tạo mật khẩu động được sử dụng bởi môđun nhãn điện tử mà số ID của nó là IDS1, được ghi vào bản ghi tương ứng với số ID IDS1 trong bộ phận cấu hình dịch vụ.

S202: môđun nhãn điện tử được bật thông qua bộ phận chuyển mạch. Sau đó, tệp torrent được ghi thông qua bộ phận ghi torrent, trong khi đó, tệp torrent được ghi vào bản ghi tương ứng với IDS1 trong bộ phận cấu hình dịch vụ của môđun dịch vụ xác nhận thông qua internet.

S203: môđun nhãn điện tử được bật thông qua bộ phận chuyển mạch. Bộ phận quản lý phát hiện xem liệu bộ phận kích khởi tự hủy có bị hỏng hay không. Nếu bộ phận kích khởi tự hủy bị hỏng, môđun nhãn điện tử xuất ra dữ liệu cụ thể TDSH qua bộ phận hiển thị, thể hiện rằng môđun nhãn điện tử đã ngừng làm việc. Nếu bộ phận kích khởi tự hủy làm việc bình thường, bộ phận quản lý của môđun nhãn điện tử khởi tạo dữ liệu xung nhịp ở DSS1 tại chu kỳ thay đổi xung nhịp thứ nhất theo chu kỳ thay đổi xung nhịp của bộ phận điều khiển xung nhịp. Bộ phận quản lý sử dụng dữ liệu xung nhịp DSS1, số ngẫu nhiên RandomD, số ID IDS1 của nhãn điện tử trong tệp torrent, làm các hệ số tính toán, để tạo ra dữ liệu mật khẩu động DKS1 bởi thuật toán tạo mật khẩu động PSW1 của bộ phận cấu hình mật khẩu động thứ nhất. Sau đó, dữ liệu mật khẩu động thứ nhất DKS1 được hiển thị trên bộ phận hiển thị. Sau đó, bộ phận quản lý tích lũy dữ liệu xung nhịp ban đầu DSS1 để thu được DSS2 theo chu kỳ tích lũy xung nhịp định trước. Sau đó, DDS2

được lưu trữ trong bộ nhớ cache.

S204: bộ phận quản lý ứng dụng của môđun đầu cuối xác nhận người sử dụng điều khiển bộ phận chụp ảnh để chụp dữ liệu ảnh TDT1 của môđun nhãn điện tử, trong đó dữ liệu ảnh IDT1 của môđun nhãn điện tử bao gồm dữ liệu mật khẩu động được hiển thị trên bộ phận hiển thị, và số ID IDS1 của môđun nhãn điện tử được bố trí trên bề mặt của môđun nhãn điện tử. Bộ phận quản lý ứng dụng của môđun đầu cuối xác nhận người sử dụng bố trí, phân đoạn, và phân tích dữ liệu ảnh IDT1 qua bộ phận phân tích ảnh để thu được dữ liệu mật khẩu động DZXS được hiển thị trên bộ phận hiển thị của môđun nhãn điện tử và số ID IDS1 của môđun nhãn điện tử. Sau đó việc tìm kiếm được tiến hành trong bộ phận cấu hình ứng dụng. Nếu DZXS bằng TDSH, mà chỉ báo rằng thiết bị tự hủy của môđun nhãn điện tử bị hỏng, quy trình xác nhận kết thúc. Nếu DZXS không bằng TDSH, IDS1 được lưu trữ vào bộ phận cấu hình ứng dụng. IDS1 và DZXS được gửi đến môđun dịch vụ xác nhận thông qua bộ phận truyền thông dữ liệu được kết nối với internet.

S205: môđun dịch vụ xác nhận nhận dữ liệu IDS1 và DZXS được gửi từ môđun đầu cuối xác nhận người sử dụng. Sau đó, bộ phận dịch vụ xác nhận tìm kiếm bản ghi tương ứng với IDS1 trong bộ phận cấu hình dịch vụ sử dụng IDS1, và trích xuất thuật toán tạo mật khẩu động PSW2 được chấp nhận bởi môđun nhãn điện tử được đại diện bởi dữ liệu xung nhịp DSS1, số ngẫu nhiên RandomD, và IDS1 mà được ghi từ đầu vào tệp torrent. Sau đó, bộ phận dịch vụ xác nhận thu được thời gian hệ thống RSS1 của môđun dịch vụ xác nhận hiện thời, và trừ DSS1 từ RSS1 để thu được kết quả. Kết quả được chia cho chu kỳ tích lũy xung nhịp xác định ban đầu để thu được RZSC mà là số lần môđun nhãn điện tử được tích lũy theo chu kỳ tích lũy xung nhịp. Cuối cùng, dữ liệu mật khẩu động RKS1 được tính toán nhờ sử dụng RandomD, DSS1, RZSC, và IDS1 làm các hệ số tính toán thông qua thuật toán tạo mật khẩu động PSW2 của bộ phận cấu hình mật khẩu động thứ hai.

S206: bộ phận dịch vụ xác nhận so sánh RKS1 tính toán được với DZXS. Nếu RKS1 bằng DZXS, kết quả chỉ báo rằng môđun nhãn điện tử này là hợp lệ được gửi đến môđun đầu cuối xác nhận người sử dụng thông qua internet. Nếu RKS1 không bằng DZXS, kết quả chỉ báo rằng môđun nhãn điện tử này là không hợp lệ được gửi đến môđun đầu cuối xác nhận người sử dụng thông qua internet.

S207: sau khi môđun đầu cuối xác nhận người sử dụng nhận kết quả được phản hồi từ môđun dịch vụ xác nhận, môđun đầu cuối xác nhận người sử dụng hiển thị kết quả, để hoàn thành quy trình xác nhận tính hợp lệ này đối với môđun nhãn điện tử.

Hơn nữa, bộ phận cấu hình dịch vụ là cơ sở dữ liệu mà có thể được đọc và được ghi bởi bộ phận dịch vụ xác nhận. Bộ phận cấu hình dịch vụ tạo cấu hình đặc tính của môđun nhãn điện tử nhờ sử dụng ID của môđun nhãn điện tử, và lưu trữ thông tin sản phẩm được thể hiện bởi môđun nhãn điện tử và đặc tính của môđun nhãn điện tử trong cơ sở dữ liệu.

Hơn nữa, thuật toán tạo mật khẩu động trong bộ phận cấu hình mật khẩu động có thể là thuật toán mã hóa trạng thái (State Encryption Algorithm), thuật toán mã hóa thủ công, hoặc thuật toán tạo mật khẩu động bất kỳ. Hơn nữa, thuật toán mật khẩu động có thể là một thuật toán, hoặc sự kết hợp của nhiều thuật toán. Sáng chế nhấn mạnh rằng thuật toán tạo mật khẩu động của bộ phận cấu hình mật khẩu động thứ nhất của môđun nhãn điện tử và của bộ phận cấu hình mật khẩu động thứ hai của môđun dịch vụ xác nhận là giống nhau.

Hơn nữa, bộ phận quản lý của môđun nhãn điện tử truyền số ID riêng của môđun nhãn điện tử và dữ liệu xung nhịp hoặc số lần tạo ra mật khẩu động làm các hệ số tính toán đến bộ phận cấu hình mật khẩu động thứ nhất, để thu được dữ liệu mật khẩu động. Do mỗi môđun nhãn điện tử được cấp một số ID duy nhất, và dữ liệu xung nhịp hoặc số lần tạo ra mật khẩu động liên tục thay đổi, nên dữ liệu mật khẩu động được tạo ra bởi mỗi môđun nhãn điện tử là khác nhau và có giá trị một

lần. Dữ liệu mật khẩu động có thể là các số, các chữ, tổ hợp của các số và các chữ, mã vạch, mã hai chiều và loại dạng biểu diễn mật khẩu bất kỳ.

Hơn nữa, dữ liệu mật khẩu động được hiển thị bởi bộ phận hiển thị của môđun nhãn điện tử. Môđun đầu cuối xác nhận người sử dụng điều khiển bộ phận chụp ảnh để thu thập dữ liệu. Môđun nhãn điện tử có thể sử dụng phương pháp truyền thông, như NFC, RFID, và v.v., để truyền dữ liệu đến môđun xác nhận người sử dụng.

Hơn nữa, phương pháp dùng cho môđun đầu cuối xác nhận người sử dụng để thu thập dữ liệu mật khẩu động của môđun nhãn điện tử, và bộ phận hiển thị của môđun nhãn điện tử hiển thị dữ liệu mật khẩu động. Môđun đầu cuối xác nhận người sử dụng điều khiển bộ phận chụp ảnh để chụp dữ liệu ảnh của dữ liệu mật khẩu động của môđun nhãn điện tử, và chuyển đổi chúng thành dữ liệu dạng văn bản. Thiết bị đầu cuối xác nhận người sử dụng có thể sử dụng phương pháp truyền thông như NFC, RFID, hồng ngoại v.v., để thu thập dữ liệu mật khẩu động của môđun nhãn điện tử, hoặc nhập thủ công dữ liệu mật khẩu động được hiển thị trên bộ phận hiển thị của môđun nhãn điện tử vào môđun đầu cuối xác nhận người sử dụng qua bộ phận nhập dữ liệu qua màn hình chạm, các nút, v.v..

Hơn nữa, phương pháp xác nhận dữ liệu mật khẩu động của môđun nhãn điện tử, và kết cấu của môđun đầu cuối xác nhận người sử dụng và môđun dịch vụ xác nhận. Dựa trên điều kiện giảm khối lượng tính toán của môđun đầu cuối xác nhận người sử dụng và tiết kiệm tài nguyên phần cứng, bộ phận phân tích ảnh của môđun đầu cuối xác nhận người sử dụng có thể được bố trí trong môđun dịch vụ xác nhận. Môđun đầu cuối xác nhận người sử dụng chỉ chịu trách nhiệm thu thập dữ liệu mật khẩu động được hiển thị trên môđun nhãn điện tử, và gửi dữ liệu ảnh đến môđun dịch vụ xác nhận. Môđun dịch vụ xác nhận phân tích dữ liệu ảnh, chuyển đổi định dạng dữ liệu, và xác nhận dữ liệu.

Hơn nữa, phương pháp xác nhận dữ liệu mật khẩu động của môđun nhãn

điện tử, kết cấu của môđun đầu cuối xác nhận người sử dụng và môđun dịch vụ xác nhận. Khi mạng đang ở trạng thái kém, bộ phận dịch vụ xác nhận, bộ phận cấu hình dịch vụ, và bộ phận cấu hình mật khẩu động thứ hai trong môđun dịch vụ xác nhận có thể được bố trí trong môđun đầu cuối xác nhận người sử dụng. Sau khi môđun đầu cuối xác nhận người sử dụng thu thập dữ liệu mật khẩu động của môđun nhãn điện tử, dịch vụ xác nhận được hoàn tất trực tiếp trong chế độ ngoại tuyến.

Hơn nữa, trong môđun dịch vụ xác nhận, nhiều thuật toán tạo mật khẩu động tương ứng với môđun nhãn điện tử có thể được thay thế trong bộ phận cấu hình mật khẩu động thứ hai của môđun dịch vụ xác nhận.

Các phương án cụ thể của sáng chế:

Phương án 1: dựa trên kết cấu được thể hiện trên Fig.1, thiết bị được sử dụng theo sáng chế bao gồm ba phần, tức là, môđun nhãn điện tử 1, môđun đầu cuối xác nhận người sử dụng 2, và môđun dịch vụ xác nhận 3. Phương pháp xác nhận theo thời gian thực tính hợp lệ đối với mật khẩu động bao gồm các bước sau.

Bước A: số ID duy nhất được gán đối với mỗi môđun nhãn điện tử 1, trong đó số ID được thể hiện là IDS1 và được bố trí trên bề mặt của môđun nhãn điện tử 1. Chu kỳ tích lũy xung nhịp đồng nhất được quy định trong môđun nhãn điện tử 1 và môđun máy chủ xác nhận 3. Thông tin sản phẩm và thông tin có liên quan được ghi vào bộ phận cấu hình dịch vụ 3-3, trong đó thông tin sản phẩm và thông tin có liên quan được đại diện bởi số ID IDS1 của môđun nhãn điện tử 1. Tệp torrent để kết hợp môđun nhãn điện tử 1 với môđun dịch vụ xác nhận 3 được xác định, trong đó tệp torrent bao gồm dữ liệu xung nhịp DSS1, số ngẫu nhiên RandomD, và số ID IDS1 của môđun nhãn điện tử 1. Việc lưu trữ dữ liệu TDSH trong bộ phận cấu hình ứng dụng 2-4 thể hiện rằng thiết bị tự hủy đã bị hỏng. Trường PSW, mà được sử dụng để đại diện cho loại thuật toán tạo mật khẩu động được sử dụng bởi môđun nhãn điện tử mà số ID của nó là IDS1, được ghi vào bản ghi tương ứng với số ID IDS1 của bộ phận cấu hình dịch vụ 3-3.

Bước B: Môđun nhãn điện tử 1 được bật thông qua bộ phận chuyển mạch 1-2. Sau đó, tệp torrent được ghi thông qua bộ phận ghi torrent 1-3, trong khi đó, tệp torrent được ghi vào bản ghi tương ứng với IDS1 trong bộ phận cấu hình dịch vụ 3-3 của môđun dịch vụ xác nhận 3 thông qua internet.

Bước C: người sử dụng bật môđun nhãn điện tử 1 thông qua bộ phận chuyển mạch 1-2. Bộ phận quản lý 1-1 phát hiện xem liệu bộ phận kích khởi tự hủy 1-6 có bị hỏng hay không. Nếu bộ phận kích khởi tự hủy 1-6 bị hỏng, môđun nhãn điện tử 1 xuất ra dữ liệu cụ thể TDSH qua bộ phận xuất tín hiệu thể hiện rằng môđun nhãn điện tử 1 đã ngừng làm việc. Nếu bộ phận kích khởi tự hủy 1-6 làm việc bình thường, bộ phận quản lý 1-1 của môđun nhãn điện tử 1 khởi tạo dữ liệu xung nhịp ở DSS1 trong chu kỳ thay đổi xung nhịp thứ nhất theo chu kỳ thay đổi xung nhịp của bộ phận điều khiển xung nhịp thứ nhất 1-4. Bộ phận quản lý 1-1 sử dụng dữ liệu xung nhịp DSS1, số ngẫu nhiên RandomD, số ID IDS1 của nhãn điện tử trong dữ liệu torrent làm các hệ số tính toán, để tạo ra dữ liệu mật khẩu động thứ nhất DKS1 bởi thuật toán tạo mật khẩu động PSW1 của bộ phận cấu hình mật khẩu động thứ nhất 1-5. Dữ liệu mật khẩu động thứ nhất DKS1 được hiển thị trên bộ phận hiển thị 1-7. Sau đó, bộ phận quản lý 1-1 tích lũy dữ liệu xung nhịp ban đầu DSS1 theo chu kỳ tích lũy xung nhịp định trước để thu được DSS2. DDS2 được lưu trữ trong bộ nhớ cache.

Bước D: bộ phận quản lý ứng dụng 2-1 của môđun đầu cuối xác nhận người sử dụng 2 điều khiển bộ phận chụp ảnh 2-2 chụp dữ liệu ảnh TDT1 của môđun nhãn điện tử 1, trong đó dữ liệu ảnh IDT1 của môđun nhãn điện tử 1 bao gồm dữ liệu mật khẩu động được hiển thị trên bộ phận hiển thị 1-7 và số ID IDS1 của môđun nhãn điện tử 1 mà được bố trí trên bề mặt của môđun nhãn điện tử 1. Bộ phận quản lý ứng dụng 2-1 của môđun đầu cuối xác nhận người sử dụng 2 bố trí, phân đoạn, và phân tích dữ liệu ảnh IDT1 qua bộ phận phân tích ảnh 2-3 để thu được dữ liệu mật khẩu động thứ hai DZXS được hiển thị trên bộ phận hiển thị 1-7 của môđun nhãn điện tử 1 và số ID IDS1 trong môđun nhãn điện tử 1. Sau đó, việc

tìm kiếm được tiến hành trong bộ phận cấu hình ứng dụng 2-4. Nếu DZXS bằng TDSH, mà chỉ báo rằng thiết bị tự hủy của môđun nhãn điện tử bị hỏng, quy trình xác nhận được kết thúc. Nếu DZXS không bằng TDSH, số ID IDS1 được lưu trữ vào bộ phận cấu hình ứng dụng 2-4. Sau đó, IDS1 và DZXS được gửi đến môđun dịch vụ xác nhận 3 qua bộ phận truyền thông dữ liệu được kết nối với internet.

Bước E: sau khi môđun dịch vụ xác nhận 3 nhận dữ liệu IDS1 và DZXS được gửi từ môđun đầu cuối xác nhận người sử dụng 2, bộ phận dịch vụ xác nhận 3-1 tìm kiếm bản ghi tương ứng với IDS1 trong bộ phận cấu hình dịch vụ 3-3, và trích xuất thuật toán tạo mật khẩu động PSW2 được chấp nhận bởi môđun nhãn điện tử 1 được đại diện bởi dữ liệu xung nhịp DSS1, số ngẫu nhiên RandomD, và IDS1 mà được ghi từ đầu vào tệp torrent. Sau đó, bộ phận dịch vụ xác nhận 3-1 nhận thời gian hệ thống RSS1 của môđun dịch vụ xác nhận hiện thời 3, và trừ DSS1 từ RSS1 để thu được kết quả. Kết quả được chia cho chu kỳ tích lũy xung nhịp xác định ban đầu để thu được RZSC mà là số lần môđun nhãn điện tử được tích lũy theo chu kỳ tích lũy xung nhịp. Cuối cùng, dữ liệu mật khẩu động RKS1 được tính toán nhờ sử dụng RandomD, DSS1, RZSC, và IDS1 làm các hệ số tính toán, thông qua thuật toán tạo mật khẩu động PSW2 của bộ phận cấu hình mật khẩu động thứ hai 3-4.

Bước F: bộ phận dịch vụ xác nhận 3 so sánh RKS1 tính toán được với DZXS. Nếu RKS1 bằng DZXS, thì kết quả chỉ báo rằng môđun nhãn điện tử này 1 là hợp lệ được gửi đến môđun đầu cuối xác nhận người sử dụng 2 thông qua internet. Nếu RKS1 không bằng DZXS, thì kết quả chỉ báo rằng môđun nhãn điện tử này 1 là không hợp lệ được gửi đến môđun đầu cuối xác nhận người sử dụng 2 thông qua internet.

Bước H: sau khi môđun đầu cuối xác nhận người sử dụng 2 nhận kết quả được phản hồi từ môđun dịch vụ xác nhận 3, môđun đầu cuối xác nhận người sử dụng hiển thị kết quả, để hoàn thành quy trình xác nhận tính hợp lệ này đối với

môđun nhãn điện tử 1.

Phương án 2: dựa trên kết cấu được thể hiện trên Fig.1, khi mạng không ổn định hoặc không có mạng, bộ phận dịch vụ xác nhận 3-1, bộ phận cấu hình dịch vụ 3-3, bộ phận cấu hình mật khẩu động thứ hai 3-4, và bộ phận điều khiển xung nhịp 3-2 trong môđun dịch vụ xác nhận có thể được bố trí trong môđun đầu cuối xác nhận người sử dụng 2. Sau khi môđun đầu cuối xác nhận người sử dụng 2 thu thập dữ liệu mật khẩu động của môđun nhãn điện tử 1, môđun đầu cuối xác nhận người sử dụng 2 hoàn thành dịch vụ xác nhận một cách trực tiếp ở chế độ ngoại tuyến.

Kết hợp với kết cấu được thể hiện trên Fig.3, một cải biến của sáng chế bao gồm hai phần: môđun nhãn điện tử 1 và môđun đầu cuối xác nhận người sử dụng 2. Môđun nhãn điện tử 1 được sử dụng để tạo ra dữ liệu mật khẩu động và hiển thị. Môđun đầu cuối xác nhận người sử dụng 2 thu thập dữ liệu ảnh của dữ liệu mật khẩu động của môđun nhãn điện tử 1. Sau khi xử lý phân tích, dữ liệu mật khẩu dạng văn bản được thu nhận. Sau khi xác nhận, kết quả của việc liệu thuật toán tạo mật khẩu động thứ nhất của môđun nhãn điện tử 1 có phù hợp với thuật toán tạo mật khẩu động thứ hai của môđun đầu cuối xác nhận người sử dụng 2 hay không được thu nhận, sao cho tính hợp lệ của môđun nhãn điện tử được xác định.

Phương án 3: dựa trên kết cấu được thể hiện trên Fig.1, khi mạng ổn định và điều được yêu cầu đối với người sử dụng là giảm lượng tính toán cục bộ của môđun đầu cuối xác nhận người sử dụng, bộ phận phân tích ảnh 2-3 của đầu cuối xác nhận người sử dụng 2 có thể được bố trí trong môđun dịch vụ xác nhận 3. Đầu cuối xác nhận người sử dụng 2 chỉ chịu trách nhiệm thu thập dữ liệu được hiển thị trên môđun nhãn điện tử 1, và gửi dữ liệu ở định dạng ảnh đến môđun dịch vụ xác nhận 3 thông qua internet. Môđun dịch vụ xác nhận 3 phân tích ảnh và cung cấp dịch vụ xác nhận.

Kết hợp với kết cấu được thể hiện trên Fig.4, một cải biến của sáng chế bao gồm ba phần: môđun nhãn điện tử 1, môđun đầu cuối xác nhận người sử dụng 2, và

môđun dịch vụ xác nhận 3. Môđun nhãn điện tử 1 được sử dụng để tạo ra dữ liệu mật khẩu động và hiển thị. Môđun đầu cuối xác nhận người sử dụng 2 thu thập dữ liệu mật khẩu động được tạo ra bởi môđun nhãn điện tử và dữ liệu ảnh của số ID của môđun nhãn điện tử, và gửi dữ liệu ảnh đến môđun dịch vụ xác nhận 3 thông qua internet. Môđun dịch vụ xác nhận 3 nhận dữ liệu ảnh được gửi từ môđun đầu cuối xác nhận người sử dụng 2. Sau khi xử lý phân tích, dữ liệu dạng văn bản được thu nhận. Việc xác nhận được tiến hành. Sau khi xác nhận, môđun dịch vụ xác nhận 3 thu được kết quả xem liệu thuật toán tạo mật khẩu động thứ nhất của môđun nhãn điện tử 1 có phù hợp với thuật toán tạo mật khẩu động thứ hai của môđun dịch vụ xác nhận 3 hay không. Kết quả được trả về cho môđun đầu cuối xác nhận người sử dụng 2 thông qua internet, để xác định tính hợp lệ của môđun nhãn điện tử 1.

Các phương án được mô tả trên đây chỉ là các phương án cụ thể của sáng chế. Tuy nhiên, sáng chế không bị giới hạn ở đó. Sự cải biến, tương đương, và cải tiến về mục đích và nguyên lý của sáng chế sẽ được hiểu là nằm trong phạm vi bảo hộ của sáng chế.

YÊU CẦU BẢO HỘ

1. Phương pháp xác nhận theo thời gian thực tính hợp lệ của nhãn bảo mật mật khẩu động được đồng bộ hóa xung nhịp, trong đó phương pháp xác nhận theo thời gian thực tính hợp lệ của nhãn bảo mật mật khẩu động được đồng bộ hóa xung nhịp bao gồm các bước sau:

gán số ID duy nhất cho môđun nhãn điện tử, trong đó số ID được thể hiện là IDS1 và được bố trí trên bề mặt của môđun nhãn điện tử; thiết lập chu kỳ tích lũy xung nhịp đồng nhất trong môđun nhãn điện tử và môđun máy chủ xác nhận; ghi thông tin sản phẩm và thông tin có liên quan vào bộ phận cấu hình dịch vụ, trong đó thông tin sản phẩm và thông tin có liên quan được đại diện bởi IDS1 của môđun nhãn điện tử; xác định tệp torrent để kết hợp môđun nhãn điện tử với môđun dịch vụ xác nhận, trong đó tệp torrent bao gồm: dữ liệu xung nhịp DSS1, số ngẫu nhiên RandomD, và số ID IDS1 của môđun nhãn điện tử; trong đó việc lưu trữ dữ liệu TDSH trong bộ phận cấu hình ứng dụng thể hiện rằng thiết bị tự hủy của môđun nhãn điện tử đã bị hỏng; ghi trường PSW, mà được sử dụng để thể hiện loại thuật toán tạo mật khẩu động được sử dụng bởi môđun nhãn điện tử mà số ID của nó là IDS1, vào bản ghi tương ứng với số ID IDS1 trong bộ phận cấu hình dịch vụ;

bật môđun nhãn điện tử bởi người sử dụng thông qua bộ phận chuyển mạch, phát hiện, bởi bộ phận quản lý, xem liệu bộ phận kích khởi tự hủy có bị hỏng hay không; nếu bộ phận kích khởi tự hủy bị hỏng, xuất ra, bởi môđun nhãn điện tử, dữ liệu cụ thể TDSH qua bộ phận hiển thị thể hiện rằng môđun nhãn điện tử đã ngừng làm việc; nếu bộ phận kích khởi tự hủy làm việc bình thường, sử dụng bộ phận quản lý của môđun nhãn điện tử để khởi tạo dữ liệu xung nhịp cho DSS1 trong chu kỳ xung nhịp thứ nhất theo chu kỳ xung nhịp của bộ phận điều khiển xung nhịp; tạo ra, bởi bộ phận quản lý, dữ liệu mật khẩu động DKS1 bởi thuật toán tạo mật khẩu động PSW1 của bộ phận cấu hình mật khẩu động thứ nhất, sử dụng dữ liệu xung nhịp DSS1, số ngẫu nhiên RandomD, số ID IDS1 của nhãn điện tử trong tệp torrent làm các hệ số tính toán, và hiển thị DKS1 trên bộ phận hiển thị; sau đó tích lũy, bởi bộ phận quản lý, dữ liệu xung nhịp ban đầu DSS1 và chu kỳ tích lũy xung nhịp

định trước để thu được dữ liệu xung nhịp thứ hai DSS2, và lưu trữ DDS2 vào bộ nhớ cache;

chụp, bởi bộ phận chụp ảnh được điều khiển bởi bộ phận quản lý ứng dụng của môđun đầu cuối xác nhận người sử dụng, dữ liệu ảnh TDT1 của môđun nhãn điện tử, trong đó dữ liệu ảnh IDT1 của môđun nhãn điện tử bao gồm dữ liệu mật khẩu động được hiển thị trên bộ phận hiển thị và số ID IDS1 của môđun nhãn điện tử được bố trí trên bề mặt của môđun nhãn điện tử; bố trí, phân đoạn, và phân tích, bởi bộ phận quản lý ứng dụng của môđun đầu cuối xác nhận người sử dụng qua bộ phận phân tích ảnh, dữ liệu ảnh IDT1 để thu được dữ liệu mật khẩu động DZXS được hiển thị trên bộ phận hiển thị của môđun nhãn điện tử và số ID IDS1 của môđun nhãn điện tử; và sau đó tìm kiếm trong bộ phận cấu hình ứng dụng; kết thúc quy trình xác nhận, nếu DZXS bằng TDSH, mà chỉ báo rằng thiết bị tự hủy của môđun nhãn điện tử bị hỏng; lưu trữ số ID IDS1 vào bộ phận cấu hình ứng dụng, nếu DZXS không bằng TDSH; và sau đó gửi IDS1 và DZXS đến môđun dịch vụ xác nhận qua bộ phận truyền thông dữ liệu được kết nối với Internet.

2. Phương pháp xác nhận theo thời gian thực tính hợp lệ của nhãn bảo mật mật khẩu động được đồng bộ hóa xung nhịp theo điểm 1, trong đó sau khi bật môđun nhãn điện tử qua bộ phận chuyển mạch; và ghi tệp torrent thông qua bộ phận ghi torrent, trong khi đồng thời ghi tệp torrent vào bản ghi tương ứng với IDS1 trong bộ phận cấu hình dịch vụ của môđun dịch vụ xác nhận thông qua internet.

3. Phương pháp xác nhận theo thời gian thực tính hợp lệ của nhãn bảo mật mật khẩu động được đồng bộ hóa xung nhịp theo điểm 1, trong đó sau khi gửi IDS1 và DZXS đến môđun dịch vụ xác nhận, nhận, bởi môđun dịch vụ xác nhận, dữ liệu IDS1 và DZXS được gửi từ môđun đầu cuối xác nhận người sử dụng, và sau đó tìm kiếm, bởi bộ phận dịch vụ xác nhận, bản ghi tương ứng với IDS1 trong bộ phận cấu hình dịch vụ sử dụng IDS1, và trích xuất thuật toán tạo mật khẩu động PSW2 được chấp nhận bởi môđun nhãn điện tử được đại diện bởi dữ liệu xung nhịp DSS1, số ngẫu nhiên RandomD, và IDS1 mà được ghi từ đầu vào tệp torrent; sau đó thu được, bởi bộ phận dịch vụ xác nhận, thời gian hệ thống RSS1 của môđun dịch vụ

xác nhận hiện thời, và trừ DSS1 từ RSS1 để thu được kết quả, chia kết quả cho chu kỳ tích lũy xung nhịp xác định ban đầu để thu được RZSC mà là số lần môđun nhãn điện tử được tích lũy theo chu kỳ tích lũy xung nhịp; cuối cùng, tính toán dữ liệu mật khẩu động RKS1 nhờ sử dụng RandomD, DSS1, RZSC, và IDS1 làm các hệ số tính toán;

so sánh, bởi bộ phận dịch vụ xác nhận, RKS1 tính toán được với DZXS; gửi kết quả chỉ báo rằng môđun nhãn điện tử này là hợp lệ đến môđun đầu cuối xác nhận người sử dụng thông qua internet, nếu RKS1 bằng DZXS; gửi kết quả chỉ báo rằng môđun nhãn điện tử này là không hợp lệ thông qua internet, nếu RKS1 không bằng DZXS;

hiển thị kết quả, sau khi môđun đầu cuối xác nhận người sử dụng nhận kết quả được phản hồi từ môđun dịch vụ xác nhận, để hoàn thành quy trình xác nhận tính hợp lệ này đối với môđun nhãn điện tử.

4. Hệ thống xác nhận theo thời gian thực tính hợp lệ của nhãn bảo mật mật khẩu động được đồng bộ hóa xung nhịp bao gồm:

môđun nhãn điện tử, được sử dụng để tạo ra dữ liệu mật khẩu động và hiển thị, môđun nhãn điện tử có số ID IDS1;

môđun đầu cuối xác nhận người sử dụng, được kết nối với môđun nhãn điện tử, và được sử dụng để chụp dữ liệu mật khẩu động được tạo ra bởi môđun nhãn điện tử và dữ liệu ảnh của số ID của môđun nhãn điện tử; sau khi phân tích, dữ liệu ảnh được chuyển đổi sang dữ liệu dạng văn bản; sau đó gửi dữ liệu dạng văn bản đến môđun dịch vụ xác nhận thông qua internet; trong đó môđun đầu cuối xác nhận người sử dụng bao gồm: bộ phận quản lý ứng dụng, bộ phận chụp ảnh, bộ phận phân tích ảnh, bộ phận cấu hình ứng dụng, bộ phận nhập dữ liệu, và bộ phận truyền thông dữ liệu; và

môđun dịch vụ xác nhận, được kết nối với môđun đầu cuối xác nhận người sử dụng, và được sử dụng để thu nhận kết quả xem liệu thuật toán tạo mật khẩu động thứ nhất của môđun nhãn điện tử có phù hợp với thuật toán tạo mật khẩu động thứ

hai của môđun dịch vụ xác nhận hay không, sau khi tính toán và xác nhận hợp lệ, và sau khi nhận dữ liệu dạng văn bản; và trả kết quả này cho môđun đầu cuối xác nhận người sử dụng, để xác định tính hợp lệ của môđun nhãn điện tử; trong đó môđun dịch vụ xác nhận bao gồm: bộ phận dịch vụ xác nhận, bộ phận điều khiển xung nhịp thứ hai, bộ phận cấu hình dịch vụ, và bộ phận cấu hình mật khẩu động thứ hai;

trong đó môđun nhãn điện tử còn bao gồm:

bộ phận quản lý, được sử dụng để phát hiện xem liệu bộ phận kích khởi tự hủy có bị hỏng hay không; khởi tạo dữ liệu xung nhịp ở DSS1 trong suốt chu kỳ xung nhịp thứ nhất theo chu kỳ thay đổi xung nhịp của bộ phận điều khiển xung nhịp thứ nhất; sử dụng dữ liệu xung nhịp DSS1, số ngẫu nhiên RandomD, số ID IDS1 của môđun nhãn điện tử làm các hệ số tính toán, trong đó dữ liệu xung nhịp DSS1, số ngẫu nhiên RandomD, số ID IDS1 được lưu trữ trong tệp torrent; tạo ra dữ liệu mật khẩu động DKS1 thông qua thuật toán tạo mật khẩu động PSW1 của bộ phận cấu hình mật khẩu động thứ nhất, và sau đó hiển thị DKS1 trên bộ phận hiển thị; sau đó thu được dữ liệu xung nhịp thứ hai DSS2 bằng cách tích lũy dữ liệu xung nhịp ban đầu DSS1 theo chu kỳ tích lũy xung nhịp định trước, và lưu trữ DDS2 trong bộ nhớ cache;

bộ phận chuyển mạch, được kết nối với bộ phận quản lý, và được sử dụng để bật môđun nhãn điện tử;

bộ phận ghi torrent, được kết nối với bộ phận quản lý, và được sử dụng để ghi tệp torrent;

bộ phận điều khiển xung nhịp thứ nhất, được kết nối với bộ phận quản lý, và được sử dụng để xuất ra chu kỳ xung nhịp;

bộ phận cấu hình mật khẩu động thứ nhất, được kết nối với bộ phận quản lý, và được sử dụng để tạo ra dữ liệu mật khẩu động DKS1 thông qua thuật toán tạo mật khẩu động PSW1;

bộ phận kích khởi tự hủy, được kết nối với bộ phận quản lý, và được sử dụng

để gửi tín hiệu phá hủy; và

bộ phận hiển thị, được kết nối với bộ phận quản lý, và được sử dụng để hiển thị dữ liệu mật khẩu động DKS1.

5. Hệ thống xác nhận theo thời gian thực tính hợp lệ của nhãn bảo mật mật khẩu động được đồng bộ hóa xung nhịp theo điểm 4, trong đó thuật toán tạo mật khẩu động trong bộ phận cấu hình mật khẩu động thứ nhất sử dụng thuật toán mã hóa trạng thái (State Encryption Algorithm);

trong đó bộ phận quản lý truyền số ID riêng của môđun nhãn điện tử và dữ liệu xung nhịp hoặc số lần tạo ra mật khẩu động như là các hệ số tính toán đến bộ phận cấu hình mật khẩu động thứ nhất, để thu được dữ liệu mật khẩu động; trong đó dữ liệu mật khẩu động được chọn từ nhóm bao gồm: số, chữ, tổ hợp của số và chữ, mã vạch, mã hai chiều, hoặc dạng biểu diễn mật khẩu bất kỳ;

trong đó môđun nhãn điện tử truyền dữ liệu đến môđun đầu cuối xác nhận người sử dụng nhờ sử dụng màn hình hiển thị, NFC, RFID, hoặc hồng ngoại.

6. Hệ thống xác nhận theo thời gian thực tính hợp lệ của nhãn bảo mật mật khẩu động được đồng bộ hóa xung nhịp theo điểm 4, trong đó môđun đầu cuối xác nhận người dùng còn bao gồm:

bộ phận quản lý ứng dụng, được sử dụng để điều khiển bộ phận chụp ảnh để chụp dữ liệu ảnh IDT1 của môđun nhãn điện tử; bố trí, phân đoạn, và phân tích dữ liệu ảnh IDT1 bởi bộ phận phân tích ảnh, thu nhận dữ liệu mật khẩu động DZXS được hiển thị trên bộ phận hiển thị và số ID IDS1 của môđun nhãn điện tử; và sau đó tìm kiếm trong bộ phận cấu hình ứng dụng;

bộ phận chụp ảnh, được kết nối với bộ phận quản lý ứng dụng, và được sử dụng để thu thập dữ liệu ảnh IDT1 của môđun nhãn điện tử;

bộ phận phân tích ảnh, được kết nối với bộ phận quản lý ứng dụng, và được sử dụng để bố trí, phân đoạn, và phân tích dữ liệu ảnh IDT1;

bộ phận cấu hình ứng dụng, được kết nối với bộ phận quản lý ứng dụng, và

được sử dụng để lưu trữ dữ liệu TDSH thể hiện rằng thiết bị tự hủy của môđun nhãn điện tử bị hỏng, và cơ sở dữ liệu nhỏ lưu trữ tạm thời dữ liệu mật khẩu động DZXS;

bộ phận nhập dữ liệu, được kết nối với bộ phận quản lý ứng dụng, và được sử dụng để nhập dữ liệu mật khẩu động thứ hai DZXS để tìm kiếm; và

bộ phận truyền thông dữ liệu, được kết nối với bộ phận quản lý ứng dụng, và được sử dụng để gửi IDS1 và DZXS đến môđun dịch vụ xác nhận thông qua internet.

7. Hệ thống xác nhận theo thời gian thực tính hợp lệ của nhãn bảo mật mật khẩu động được đồng bộ hóa xung nhịp theo điểm 4, trong đó môđun dịch vụ xác nhận còn bao gồm:

bộ phận dịch vụ xác nhận, được sử dụng để trích xuất thuật toán tạo mật khẩu động PSW2 được chấp nhận bởi môđun nhãn điện tử, mà được thể hiện bởi dữ liệu xung nhịp DSS1, số ngẫu nhiên RandomD, và IDS1 mà được ghi từ đầu vào tệp torrent; thu nhận thời gian hệ thống RSS1 của môđun dịch vụ xác nhận hiện thời; tính toán dữ liệu mật khẩu động RKS1 thông qua thuật toán tạo mật khẩu động PSW2 của bộ phận cấu hình mật khẩu động thứ hai; so sánh RKS1 tính toán được với DZXS;

bộ phận điều khiển xung nhịp thứ hai, được kết nối với bộ phận dịch vụ xác nhận, và được sử dụng để cung cấp tín hiệu xung nhịp cho bộ phận dịch vụ xác nhận;

bộ phận cấu hình dịch vụ, được kết nối với bộ phận dịch vụ xác nhận, và được sử dụng làm cơ sở dữ liệu để lưu trữ các đặc tính khác nhau của IDS1;

bộ phận cấu hình mật khẩu động thứ hai, được kết nối với bộ phận dịch vụ xác nhận, và được sử dụng để tính toán dữ liệu mật khẩu động RKS1 thông qua thuật toán tạo mật khẩu động PSW2.

8. Hệ thống xác nhận theo thời gian thực tính hợp lệ của nhãn bảo mật mật khẩu động được đồng bộ hóa xung nhịp theo điểm 7, trong đó bộ phận cấu hình dịch vụ

là cơ sở dữ liệu mà được tạo cấu hình để được đọc và ghi bởi bộ phận dịch vụ xác nhận; bộ phận cấu hình dịch vụ tạo cấu hình đặc tính của môđun nhãn điện tử nhờ sử dụng ID của môđun nhãn điện tử, và lưu trữ thông tin sản phẩm được thể hiện bởi môđun nhãn điện tử và đặc tính của môđun nhãn điện tử trong cơ sở dữ liệu;

trong đó nhiều thuật toán tạo mật khẩu động tương ứng với môđun nhãn điện tử được đặt trong bộ phận cấu hình mật khẩu động thứ hai của môđun dịch vụ xác nhận.

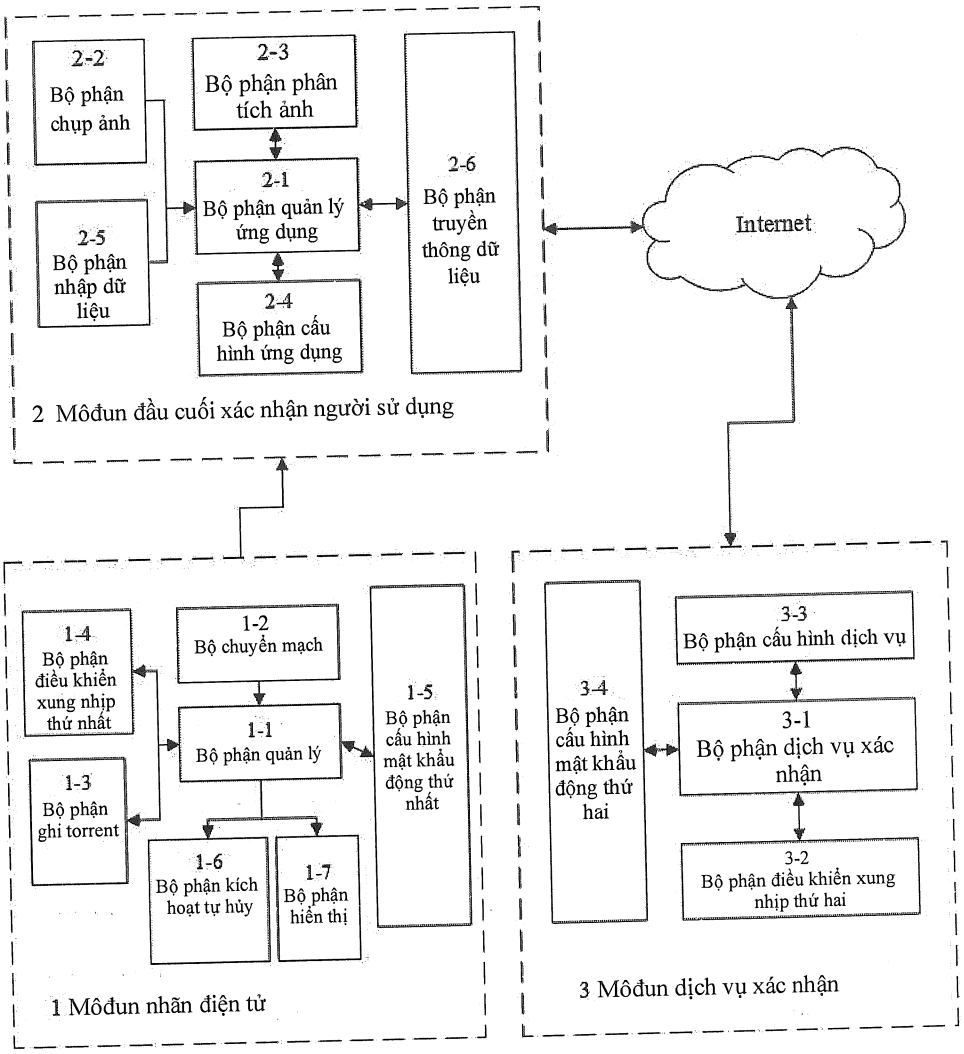

2-2
Bộ phận chụp ảnh
2-3
Bộ phận phân tích ảnh
2-1
Bộ phận quản lý ứng dụng
2-5
Bộ phận nhập dữ liệu
2-4
Bộ phận cấu hình ứng dụng
2-6
Bộ phận truyền thông dữ liệu
Internet
2 Môđun đầu cuối xác nhận người sử dụng
1-4
Bộ phận điều khiển xung nhịp thứ nhất
1-2
Bộ chuyển mạch
1-1
Bộ phận quản lý
1-3
Bộ phận ghi torrent
1-6
Bộ phận kích hoạt tự hủy
1-7
Bộ phận hiển thị
1-5
Bộ phận cấu hình mật khẩu động thứ nhất
1 Môđun nhãn điện tử
3-4
Bộ phận cấu hình mật khẩu động thứ hai
3-3
Bộ phận cấu hình dịch vụ
3-1
Bộ phận dịch vụ xác nhận
3-2
Bộ phận điều khiển xung nhịp thứ hai
3 Môđun dịch vụ xác nhận

Fig.1

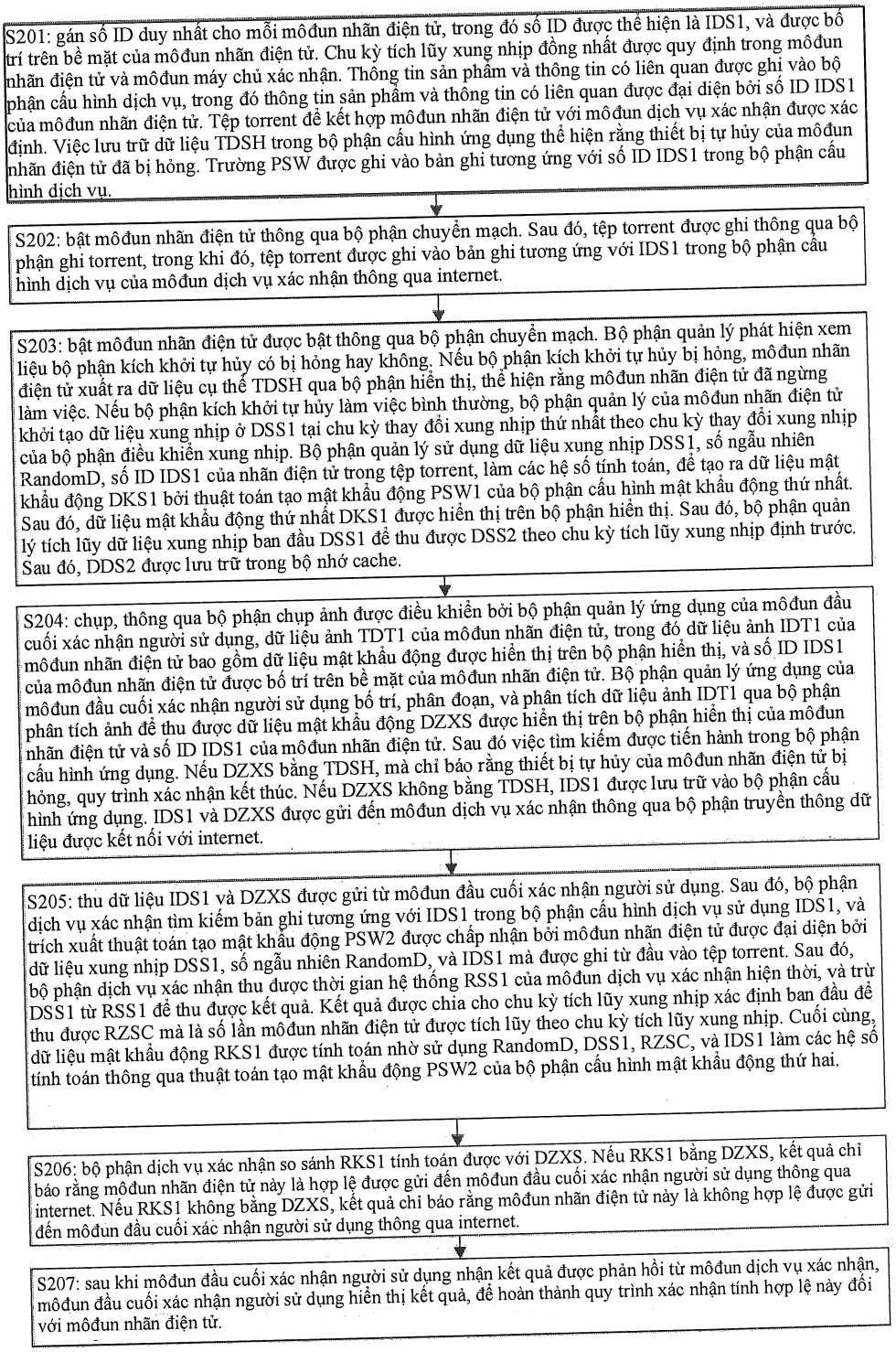

S201: gán số ID duy nhất cho mỗi môđun nhãn điện tử, trong đó số ID được thể hiện là IDS1, và được bố trí trên bề mặt của môđun nhãn điện tử. Chu kỳ tích lũy xung nhịp đồng nhất được quy định trong môđun nhãn điện tử và môđun máy chủ xác nhận. Thông tin sản phẩm và thông tin có liên quan được ghi vào bộ phận cấu hình dịch vụ, trong đó thông tin sản phẩm và thông tin có liên quan được đại diện bởi số ID IDS1 của môđun nhãn điện tử. Tệp torrent để kết hợp môđun nhãn điện tử với môđun dịch vụ xác nhận được xác định. Việc lưu trữ dữ liệu TDSH trong bộ phận cấu hình ứng dụng thể hiện rằng thiết bị tự hủy của môđun nhãn điện tử đã bị hỏng. Trường PSW được ghi vào bản ghi tương ứng với số ID IDS1 trong bộ phận cấu hình dịch vụ.
S202: bật môđun nhãn điện tử thông qua bộ phận chuyển mạch. Sau đó, tệp torrent được ghi thông qua bộ phận ghi torrent, trong khi đó, tệp torrent được ghi vào bản ghi tương ứng với IDS1 trong bộ phận cấu hình dịch vụ của môđun dịch vụ xác nhận thông qua internet.
S203: bật môđun nhãn điện tử được bật thông qua bộ phận chuyển mạch. Bộ phận quản lý phát hiện xem liệu bộ phận kích khởi tự hủy có bị hỏng hay không. Nếu bộ phận kích khởi tự hủy bị hỏng, môđun nhãn điện tử xuất ra dữ liệu cụ thể TDSH qua bộ phận hiển thị, thể hiện rằng môđun nhãn điện tử đã ngừng làm việc. Nếu bộ phận kích khởi tự hủy làm việc bình thường, bộ phận quản lý của môđun nhãn điện tử khởi tạo dữ liệu xung nhịp ở DSS1 tại chu kỳ thay đổi xung nhịp thứ nhất theo chu kỳ thay đổi xung nhịp của bộ phận điều khiển xung nhịp. Bộ phận quản lý sử dụng dữ liệu xung nhịp DSS1, số ngẫu nhiên RandomD, số ID IDS1 của nhãn điện tử trong tệp torrent, làm các hệ số tính toán, để tạo ra dữ liệu mật khẩu động DKS1 bởi thuật toán tạo mật khẩu động PSW1 của bộ phận cấu hình mật khẩu động thứ nhất. Sau đó, dữ liệu mật khẩu động thứ nhất DKS1 được hiển thị trên bộ phận hiển thị. Sau đó, bộ phận quản lý tích lũy dữ liệu xung nhịp ban đầu DSS1 để thu được DSS2 theo chu kỳ tích lũy xung nhịp định trước. Sau đó, DDS2 được lưu trữ trong bộ nhớ cache.
S204: chụp, thông qua bộ phận chụp ảnh được điều khiển bởi bộ phận quản lý ứng dụng của môđun đầu cuối xác nhận người sử dụng, dữ liệu ảnh TDT1 của môđun nhãn điện tử, trong đó dữ liệu ảnh IDT1 của môđun nhãn điện tử bao gồm dữ liệu mật khẩu động được hiển thị trên bộ phận hiển thị, và số ID IDS1 của môđun nhãn điện tử được bố trí trên bề mặt của môđun nhãn điện tử. Bộ phận quản lý ứng dụng của môđun đầu cuối xác nhận người sử dụng bố trí, phân đoạn, và phân tích dữ liệu ảnh IDT1 qua bộ phận phân tích ảnh để thu được dữ liệu mật khẩu động DZXS được hiển thị trên bộ phận hiển thị của môđun nhãn điện tử và số ID IDS1 của môđun nhãn điện tử. Sau đó việc tìm kiếm được tiến hành trong bộ phận cấu hình ứng dụng. Nếu DZXS bằng TDSH, mà chỉ báo rằng thiết bị tự hủy của môđun nhãn điện tử bị hỏng, quy trình xác nhận kết thúc. Nếu DZXS không bằng TDSH, IDS1 được lưu trữ vào bộ phận cấu hình ứng dụng. IDS1 và DZXS được gửi đến môđun dịch vụ xác nhận thông qua bộ phận truyền thông dữ liệu được kết nối với internet.
S205: thu dữ liệu IDS1 và DZXS được gửi từ môđun đầu cuối xác nhận người sử dụng. Sau đó, bộ phận dịch vụ xác nhận tìm kiếm bản ghi tương ứng với IDS1 trong bộ phận cấu hình dịch vụ sử dụng IDS1, và trích xuất thuật toán tạo mật khẩu động PSW2 được chấp nhận bởi môđun nhãn điện tử được đại diện bởi dữ liệu xung nhịp DSS1, số ngẫu nhiên RandomD, và IDS1 mà được ghi từ đầu vào tệp torrent. Sau đó, bộ phận dịch vụ xác nhận thu được thời gian hệ thống RSS1 của môđun dịch vụ xác nhận hiện thời, và trừ DSS1 từ RSS1 để thu được kết quả. Kết quả được chia cho chu kỳ tích lũy xung nhịp xác định ban đầu để thu được RZSC mà là số lần môđun nhãn điện tử được tích lũy theo chu kỳ tích lũy xung nhịp. Cuối cùng, dữ liệu mật khẩu động RKS1 được tính toán nhờ sử dụng RandomD, DSS1, RZSC, và IDS1 làm các hệ số tính toán thông qua thuật toán tạo mật khẩu động PSW2 của bộ phận cấu hình mật khẩu động thứ hai.
S206: bộ phận dịch vụ xác nhận so sánh RKS1 tính toán được với DZXS. Nếu RKS1 bằng DZXS, kết quả chỉ báo rằng môđun nhãn điện tử này là hợp lệ được gửi đến môđun đầu cuối xác nhận người sử dụng thông qua internet. Nếu RKS1 không bằng DZXS, kết quả chỉ báo rằng môđun nhãn điện tử này là không hợp lệ được gửi đến môđun đầu cuối xác nhận người sử dụng thông qua internet.
S207: sau khi môđun đầu cuối xác nhận người sử dụng nhận kết quả được phản hồi từ môđun dịch vụ xác nhận, môđun đầu cuối xác nhận người sử dụng hiển thị kết quả, để hoàn thành quy trình xác nhận tính hợp lệ này đối với môđun nhãn điện tử.

Fig.2

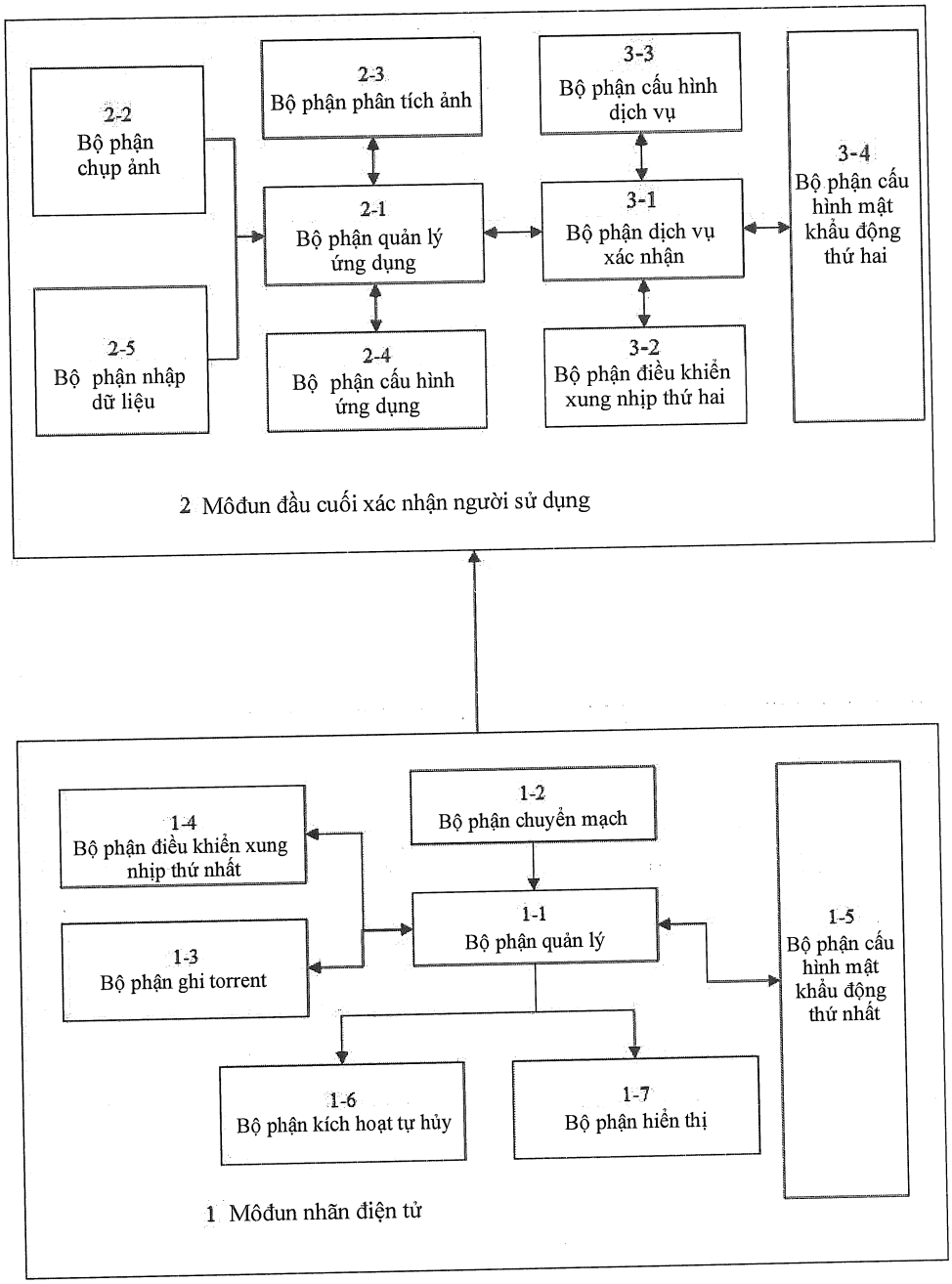

2-2
Bộ phận
chụp ảnh
2-3
Bộ phận phân tích ảnh
3-3
Bộ phận cấu hình
dịch vụ
3-4
Bộ phận cấu
hình mật
khẩu động
thứ hai
2-1
Bộ phận quản lý
ứng dụng
3-1
Bộ phận dịch vụ
xác nhận
2-5
Bộ phận nhập
dữ liệu
2-4
Bộ phận cấu hình
ứng dụng
3-2
Bộ phận điều khiển
xung nhịp thứ hai
2 Môđun đầu cuối xác nhận người sử dụng
1-4
Bộ phận điều khiển xung
nhịp thứ nhất
1-2
Bộ phận chuyển mạch
1-5
Bộ phận cấu
hình mật
khẩu động
thứ nhất
1-1
Bộ phận quản lý
1-3
Bộ phận ghi torrent
1-6
Bộ phận kích hoạt tự hủy
1-7
Bộ phận hiển thị
1 Môđun nhãn điện tử

Fig.3

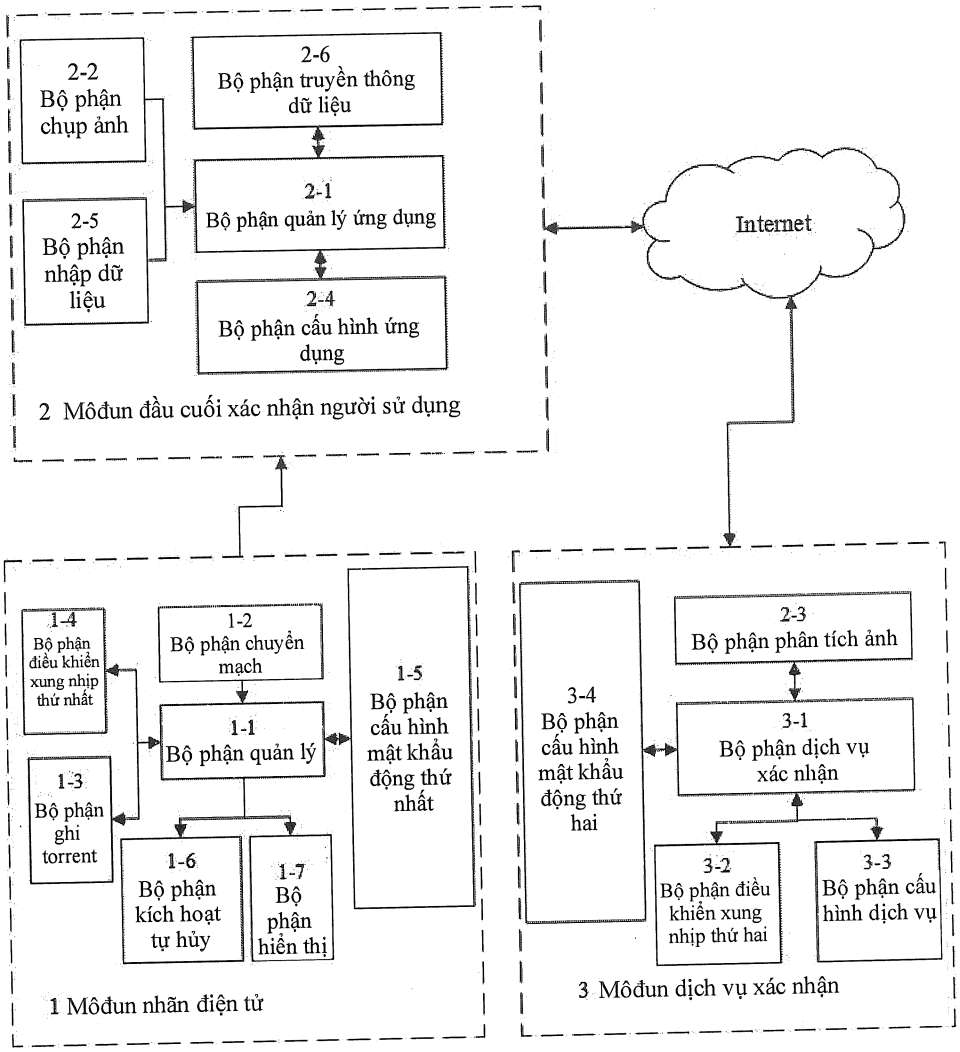

2-2
Bộ phận chụp ảnh
2-6
Bộ phận truyền thông dữ liệu
2-1
Bộ phận quản lý ứng dụng
2-5
Bộ phận nhập dữ liệu
2-4
Bộ phận cấu hình ứng dụng
2 Môđun đầu cuối xác nhận người sử dụng
Internet
1-4
Bộ phận điều khiển xung nhịp thứ nhất
1-2
Bộ phận chuyển mạch
1-5
Bộ phận cấu hình mật khẩu động thứ nhất
1-1
Bộ phận quản lý
1-3
Bộ phận ghi torrent
1-6
Bộ phận kích hoạt tự hủy
1-7
Bộ phận hiển thị
1 Môđun nhãn điện tử
3-4
Bộ phận cấu hình mật khẩu động thứ hai
2-3
Bộ phận phân tích ảnh
3-1
Bộ phận dịch vụ xác nhận
3-2
Bộ phận điều khiển xung nhịp thứ hai
3-3
Bộ phận cấu hình dịch vụ
3 Môđun dịch vụ xác nhận

Fig.4