SỞ KHOA HỌC VÀ CÔNG NGHỆ THÀNH PHỐ HỒ CHÍ MINH
TRUNG TÂM THÔNG TIN, THỐNG KÊ VÀ ỨNG DỤNG TIẾN BỘ KHOA HỌC CÔNG NGHỆ

CÔNG NGHỆ AN NINH MẠNG

XU HƯỚNG NGHIÊN CỨU TRÊN THẾ GIỚI VÀ MỘT SỐ GIẢI PHÁP ỨNG DỤNG TẠI VIỆT NAM

- Tháng 12/2025 -

MỤC LỤC

PHẦN MỞ ĐẦU

Trong bối cảnh cuộc Cách mạng công nghiệp lần thứ tư và tiến trình chuyển đổi số đang diễn ra mạnh mẽ trên phạm vi toàn cầu, không gian mạng đã trở thành môi trường hoạt động thiết yếu của các cơ quan nhà nước, doanh nghiệp và toàn xã hội. Các hệ thống công nghệ thông tin, dữ liệu số và hạ tầng mạng ngày càng giữ vai trò then chốt trong quản lý, điều hành, sản xuất – kinh doanh và cung cấp dịch vụ công.

Tuy nhiên, song hành với những lợi ích to lớn mà công nghệ số mang lại, các mối đe dọa về an ninh mạng cũng gia tăng nhanh chóng cả về số lượng, quy mô và mức độ tinh vi. Các hình thức tấn công mạng ngày nay không chỉ dừng lại ở việc xâm nhập trái phép hay đánh cắp dữ liệu, mà còn hướng tới phá hoại hệ thống, làm gián đoạn dịch vụ, gây thiệt hại nghiêm trọng về kinh tế, uy tín của tổ chức, doanh nghiệp, thậm chí ảnh hưởng đến an ninh quốc gia và trật tự an toàn xã hội.

Thực tiễn tại Việt Nam cho thấy, cùng với quá trình phát triển Chính phủ số, kinh tế số và xã hội số, nguy cơ mất an toàn, an ninh mạng ngày càng hiện hữu. Nhiều hệ thống thông tin quan trọng đang phải đối mặt với các nguy cơ như tấn công có chủ đích (APT), mã độc tống tiền, lộ lọt dữ liệu cá nhân và dữ liệu nhạy cảm. Trước những thách thức đó, Đảng và Nhà nước đã ban hành nhiều chủ trương, chính sách quan trọng nhằm tăng cường bảo đảm an toàn, an ninh mạng, tiêu biểu như Luật An ninh mạng, các chương trình, chiến lược quốc gia về chuyển đổi số và bảo đảm an toàn thông tin mạng.

Trong bối cảnh này, việc nghiên cứu, phân tích xu hướng công nghệ an ninh mạng trở thành yêu cầu cấp thiết, có ý nghĩa cả về lý luận và thực tiễn. Các công nghệ mới như trí tuệ nhân tạo, dữ liệu lớn, điện toán đám mây, Internet vạn vật… vừa mở ra nhiều cơ hội, đồng thời cũng đặt ra những thách thức mới đối với công tác bảo đảm an ninh mạng. Việc nắm bắt kịp thời các xu hướng công nghệ sẽ giúp các cơ quan, tổ chức chủ động hơn trong phòng ngừa, phát hiện và ứng phó với các nguy cơ, rủi ro trên không gian mạng.

Để giúp các nhà quản lý, nhà nghiên cứu và doanh nghiệp có thêm thông tin về các xu hướng phát triển công nghệ an ninh mạng trên thế giới và tình hình nghiên cứu, phát triển công nghệ an ninh mạng tại Việt Nam, Trung tâm Thông tin và Thống kê KH&CN TP.HCM tổ chức hội thảo "*Xu hướng công nghệ an ninh mạng*" và biên soạn tài liệu tổng quan *"Công nghệ an ninh mạng* - Xu hướng nghiên cứu trên thế giới và một số giải pháp ứng dụng tại Việt Nam". Tài liệu này gồm 3 phần:

- ***Phần 1: Hoạt động cấp bằng sáng chế toàn cầu về công nghệ an ninh mạng*** sẽ phân tích số liệu sáng chế quốc tế để thấy được xu hướng nghiên cứu công nghệ an ninh mạng thông qua các nội dung như: toàn cảnh về hoạt động công bố, bảo hộ sáng chế trên toàn thế giới tính đến thời điểm năm 2025; phân tích sáng chế theo quốc gia bảo hộ; phân tích các lĩnh vực nghiên cứu công nghệ an ninh mạng, các lĩnh vực công nghệ mới nổi (như Trí tuệ nhân tạo, Học máy, Blockchain, Bảo mật Zero-Trust, Bảo mật hậu lượng tử) đang được áp dụng trong các nghiên cứu về an ninh mạng. Các thông tin đáng chú ý khác như đánh giá về tỷ lệ sáng chế được bảo hộ ở phạm vi quốc tế trên tổng số sáng chế đã đăng ký, các tập đoàn công nghệ đang nắm giữ nhiều sáng chế,… cũng sẽ được giới thiệu.

- ***Phần 2: Các giải pháp an ninh mạng đã được nghiên cứu và ứng dụng tại Việt Nam*** sẽ điểm qua các sáng chế đã được đăng ký bảo hộ tại Việt Nam và khái quát một số giải pháp công nghệ của các chuyên gia trong nước, đã được trình bày tại Hội thảo. Đây là các giải pháp đã được các đơn vị nghiên cứu, trường đại học trong nước phát triển, như: Trường Đại học Bách Khoa, Trường Đại học Khoa học tự nhiên (Đại học Quốc gia TP.HCM), Học viện Công nghệ Bưu chính Viễn thông, Viện Ứng dụng Công nghệ mới.

- ***Phần 3: Kết luận*** sẽ khái quát lại xu hướng ứng dụng công nghệ an ninh mạng trên thế giới và tình hình nghiên cứu, ứng dụng công nghệ này tại Việt Nam.

Chúng tôi mong rằng tài liệu này sẽ cung cấp một bức tranh tổng quát về xu hướng công nghệ an ninh mạng trên thế giới và tại Việt Nam, giúp các nhà quản lý, nhà khoa học, nhà đầu tư, cũng như các doanh nghiệp công nghệ có thêm cơ hội hợp tác nghiên cứu, triển khai các giải pháp ứng dụng công nghệ mới, góp phần bảo vệ an toàn kết nối mạng, an toàn thông tin, đặc biệt khi xu hướng ứng dụng các công nghệ hiện đại, các thiết bị thông minh và hoạt động chuyển đổi số đang diễn ra mạnh mẽ trên tất cả các lĩnh vực kinh tế và đời sống xã hội.

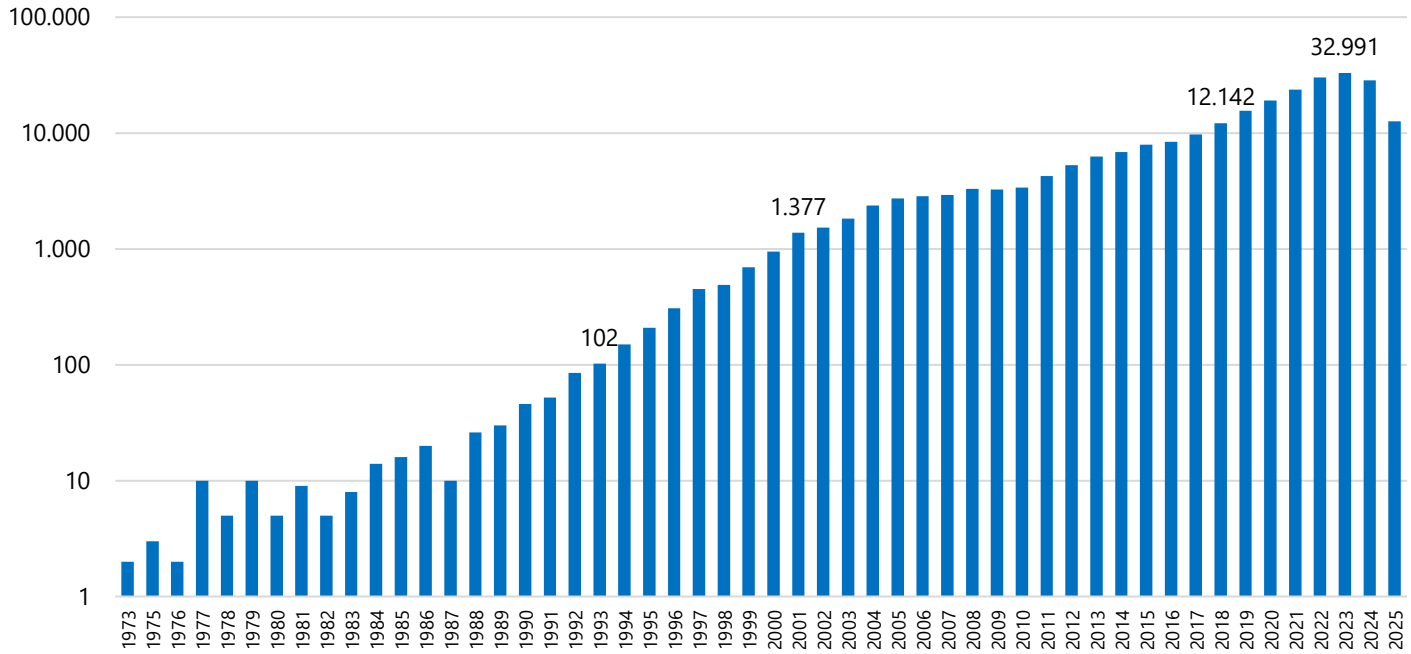
Trân trọng.

Ban Tổ chức

PHẦN 1 - HOẠT ĐỘNG CẤP BẰNG SÁNG CHẾ TOÀN CẦU VỀ CÔNG NGHỆ AN NINH MẠNG

1.1 Xu hướng cấp bằng sáng chế công nghệ an ninh mạng, theo năm công bố sớm nhất

Theo thống kê từ cơ sở dữ liệu (CSDL) sáng chế quốc tế WIPS Global đến tháng 10/2025, có 252.742 họ sáng chế (patent families) về công nghệ an ninh mạng đã được đăng ký bảo hộ trên toàn thế giới (Hình 1.1). Các sáng chế liên quan đến công nghệ an ninh mạng được ghi nhận đăng ký sớm nhất phần lớn thuộc sở hữu của Tập đoàn công nghệ International Business Machines Corporation (IBM, Mỹ), có thể kể đến như *"Hệ thống mã hóa khối sản phẩm để bảo mật dữ liệu"*, đây là sáng chế được bảo hộ trên phạm vi quốc tế với đơn đăng ký lần đầu vào ngày 24/02/1975 tại Mỹ, sau đó đăng ký bảo hộ tiếp ở 5 quốc gia (bao gồm: Ý, Anh, Pháp, Đức và Canada).



Hình 1.1. Xu hướng cấp bằng sáng chế công nghệ an ninh mạng, theo năm công bố sớm nhất (sử dụng thang đo Logarit)

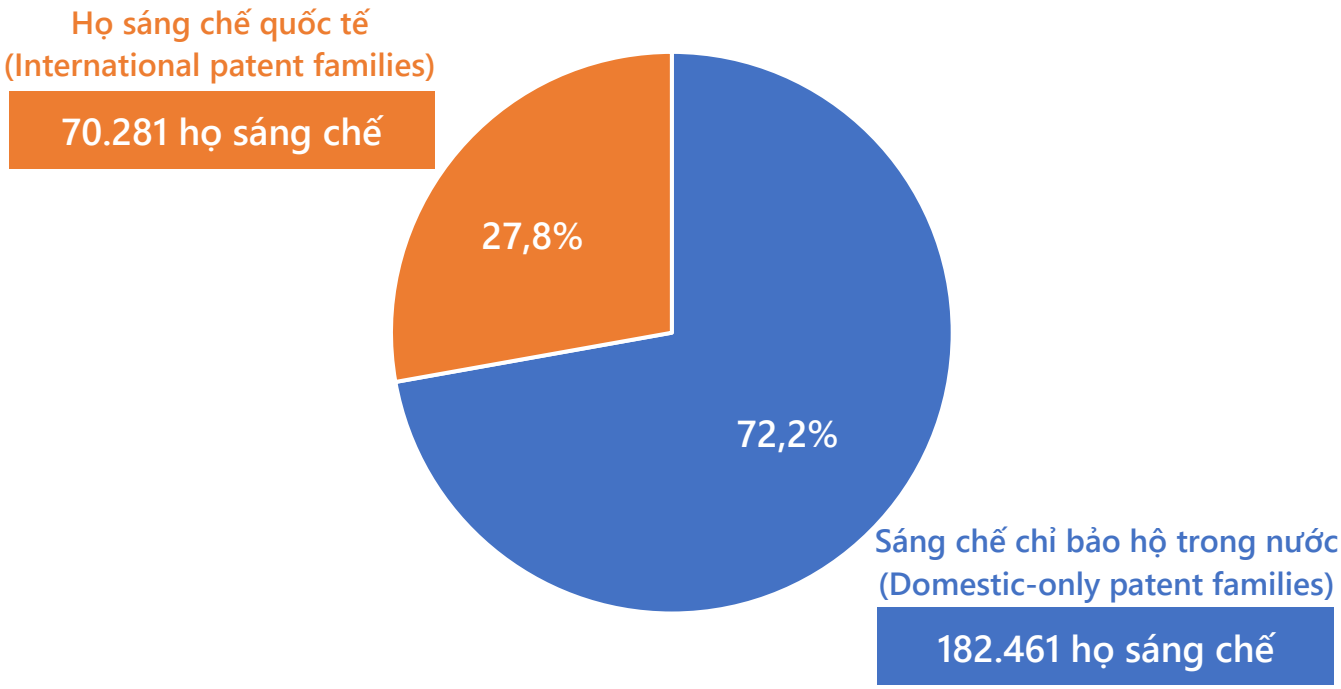
Số lượng sáng chế về công nghệ an ninh mạng đăng ký bảo hộ trên toàn thế giới vượt mốc 100 sáng chế/năm vào năm 1993, đến năm 2001 đã vượt mốc 1000 sáng chế/năm, đến năm 2018 là hơn 10.000 sáng chế/năm, và đạt mức cao nhất là 32.991 sáng chế vào năm 2023.

Tốc độ tăng trưởng kép hàng năm (Compound Annual Growth Rate - CAGR) của các sáng chế về công nghệ an ninh mạng trong vòng 20 năm qua (tương ứng với giai đoạn 2005 – 2024) là 13,2% và trong vòng 10 năm qua (tương ứng với giai đoạn 2015 – 2024) là 15,3%.

1.2 Tỷ lệ sáng chế về công nghệ an ninh mạng được bảo hộ ở quy mô quốc tế, theo số lượng họ sáng chế đã công bố

Theo Tổ chức Sở hữu Trí tuệ Thế giới (World Intellectual Property Organization - WIPO), họ sáng chế quốc tế (International Patent Families - IPFs) là những sáng chế được đăng ký bảo hộ tại nhiều quốc gia/khu vực. Việc phân tích các IPFs sẽ giúp lọc ra những phát minh ít tác động hoặc mang tính cục bộ, để lại một tập dữ liệu phản ánh các khoản đầu tư đáng kể và tập trung vào tính khả thi về công nghệ và thương mại lâu dài, giúp cung cấp cái nhìn rõ ràng hơn về các xu hướng chính định hình sự đổi mới ở các lĩnh vực chiến lược.

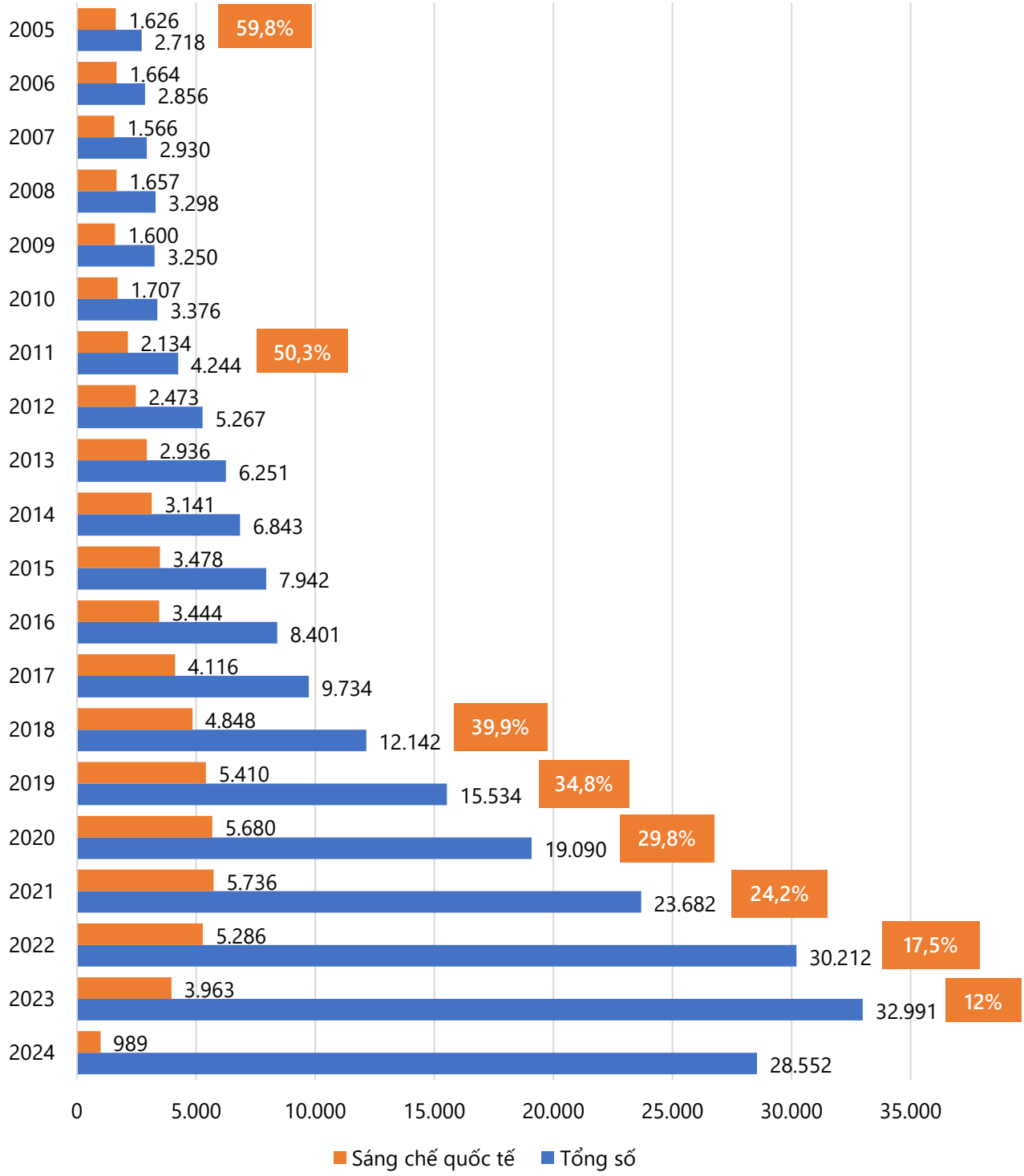
Số liệu phân tích cho thấy, có 70.281 họ sáng chế quốc tế trong hơn 252.000 họ sáng chế đăng ký bảo hộ trên toàn thế giới, chiếm tỷ lệ 27,8%. Còn lại 182.461 họ sáng chế (chiếm tỷ lệ 72,2%) chỉ được bảo hộ cục bộ trong nội bộ 1 quốc gia/khu vực nhất định (Hình 1.2).



Hình 1.2. Tỷ lệ sáng chế về công nghệ an ninh mạng quốc tế và trong nước theo số lượng họ sáng chế đã công bố, giai đoạn 1973-2025

Mặc dù tổng số sáng chế và sáng chế quốc tế tăng trưởng ổn định, nhưng tỷ lệ IPFs/Tổng số họ sáng chế đã giảm từ 59,8% năm 2005 xuống 29,8% năm 2020, và chỉ

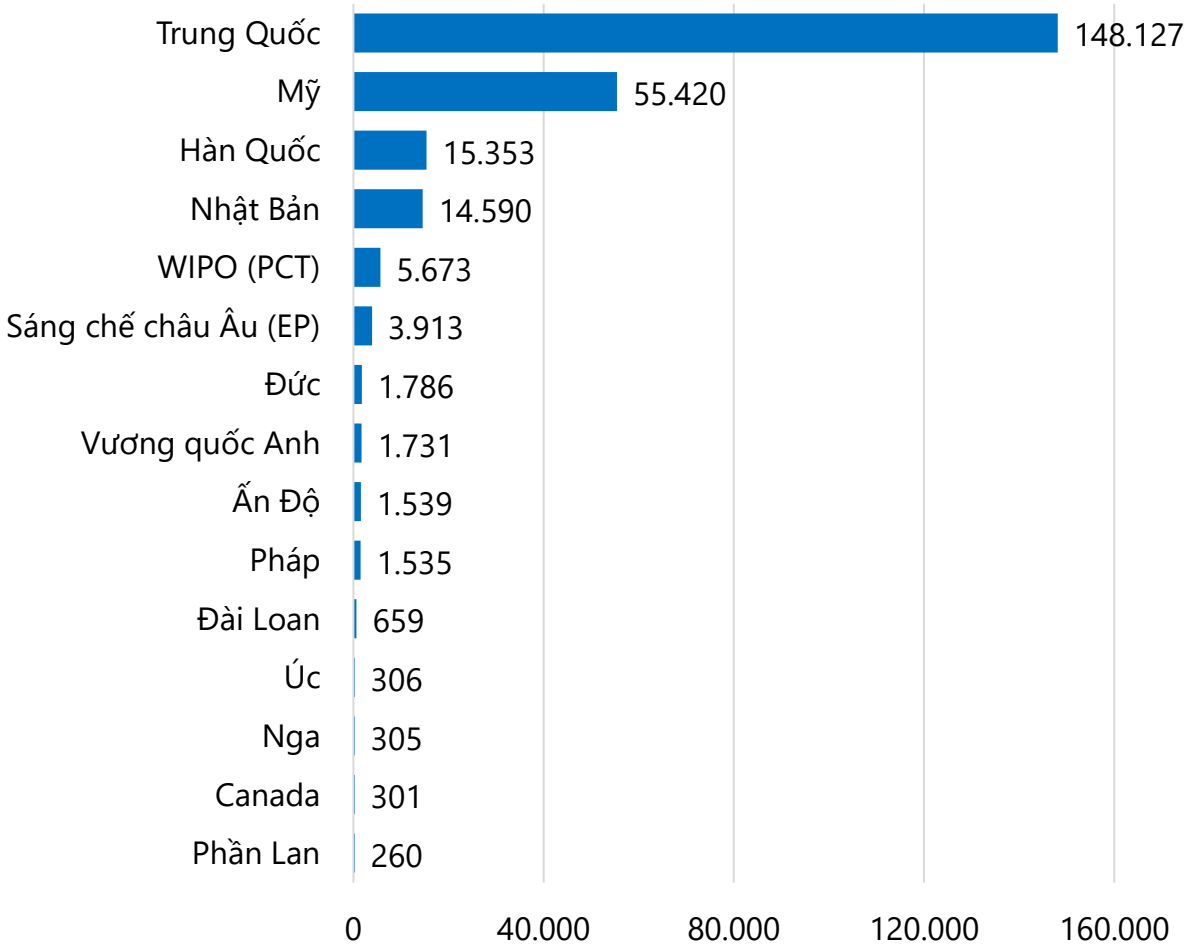
còn 12% năm 2023 (Hình 1.3), cho thấy các sáng chế thời gian gần đây tập trung đăng ký bảo hộ và đáp ứng nhu cầu trong nước, hơn là thúc đẩy những tiến bộ công nghệ trên phạm vi quốc tế.



Hình 1.3. Tỷ lệ IPFs so với tổng số họ sáng chế công nghệ an ninh mạng, giai đoạn 2005-2024

1.3 Sáng chế về công nghệ an ninh mạng theo nơi nộp đơn đăng ký bảo hộ

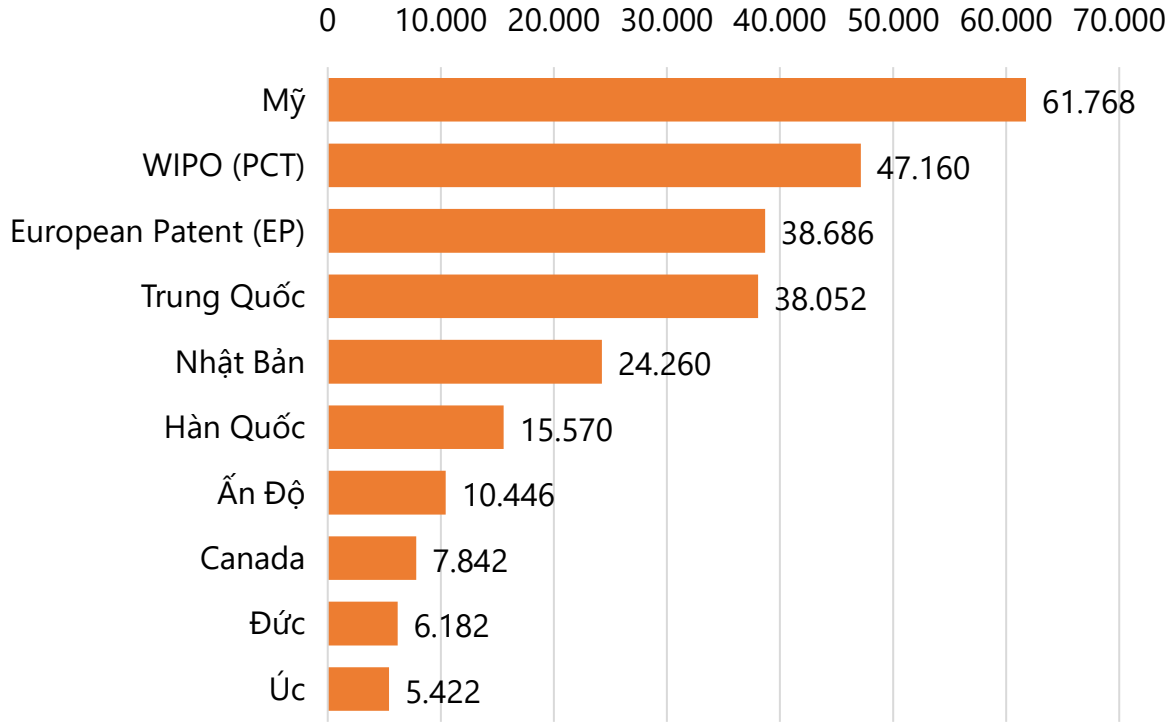
Sáng chế về công nghệ an ninh mạng đã được đăng ký bảo hộ tại 64 quốc gia, vùng lãnh thổ và 2 tổ chức quốc tế (Hình 1.4). Theo quốc gia/nơi nộp đơn bảo hộ lần đầu, 4 quốc gia dẫn đầu bao gồm: Trung Quốc đứng đầu với 148.127 họ sáng chế (chiếm tỷ lệ 58,7%), đứng thứ hai là Mỹ với 55.420 họ sáng chế (chiếm tỷ lệ 21,9%), đứng thứ ba là Hàn Quốc với 15.353 họ sáng chế (chiếm tỷ lệ 6,1%), đứng thứ 4 là Nhật Bản với 14.590 họ sáng chế (chiếm tỷ lệ 5,8%).



Hình 1.4. Sáng chế về công nghệ an ninh mạng theo nơi nộp đơn bảo hộ lần đầu, 1973-2025

Phân tích theo số lượng đăng ký bảo hộ tại các quốc gia/khu vực đối với 70.281 họ sáng chế quốc tế cho thấy, số lượng sáng chế đăng ký bảo hộ tại Mỹ dẫn đầu với 61.768 họ sáng chế (tần suất 87,9%) cho thấy đây là thị trường được nhắm mục tiêu chính trong chiến lược đăng ký bảo hộ sáng chế quốc tế, nơi có hệ thống bảo hộ và thực thi quyền sở hữu trí tuệ mạnh, môi trường thương mại hóa năng động và giá trị kinh tế cao. Bên cạnh đó, việc nộp đơn sáng chế quốc tế thông qua các tổ chức như

WIPO (theo Hiệp ước Hợp tác Sáng chế - Patent Cooperation Treaty - PCT) và Văn phòng Sáng chế châu Âu (European Patent Office - EPO) cũng được các chủ đơn chú trọng với tần suất lần lượt là 67,1% và 55%, nhằm mở rộng khả năng bảo hộ sáng chế tại các quốc gia thành viên của hai tổ chức này. Theo đó, các đơn đăng ký sáng chế nộp tại PCT có hiệu lực pháp lý tương đương với việc nộp đơn tại 158 quốc gia thành viên của PCT, việc cấp bằng sáng chế vẫn nằm dưới sự kiểm soát của các Văn phòng cấp bằng sáng chế quốc gia hoặc khu vực. Còn các đơn đăng ký sáng chế nộp tại EPO có hiệu lực pháp lý tại 44 quốc gia thành viên Liên minh Châu Âu mà chủ đơn đã chỉ định trong quá trình đăng ký.



Hình 1.5. Top 10 Quốc gia/khu vực đăng ký bảo hộ IPFs hàng đầu, giai đoạn 1973-2025

Mặc dù Trung Quốc dẫn đầu về số lượng đăng ký bảo hộ sáng chế trên toàn thế giới với 148.127 họ sáng chế, nhưng chỉ có 38.052 họ sáng chế quốc tế được đăng ký bảo hộ tại Trung Quốc. Điều này có thể cho thấy nhiều bằng sáng chế tại Trung Quốc vẫn tập trung và thiết kế phù hợp cho thị trường nội địa hơn là mở rộng phạm vi bảo hộ quốc tế.

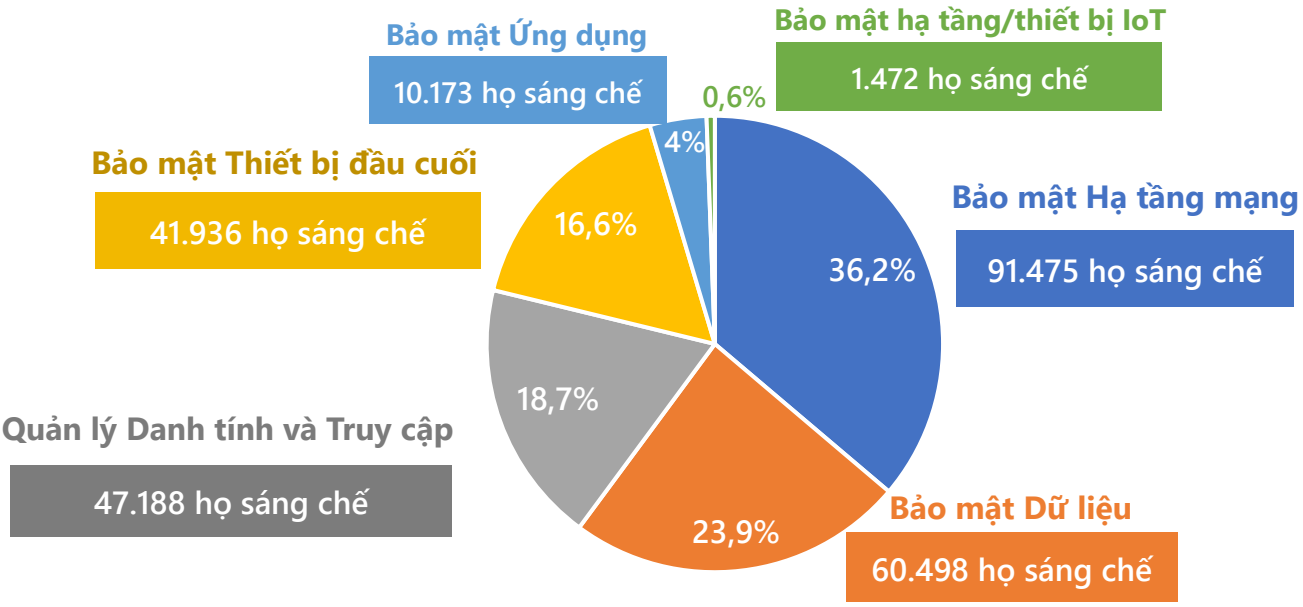
1.4 Sáng chế về công nghệ an ninh mạng chia theo các lĩnh vực

Dựa trên các ấn phẩm khoa học đã được công bố trên các tạp chí quốc tế, cũng như đối chiếu với bảng mã phân loại sáng chế quốc tế (IPC – International Patent Classification), có thể phân loại các sáng chế về công nghệ an ninh mạng theo 6 lĩnh vực nghiên cứu chính: *(1) Bảo mật Hạ tầng mạng (Network Security), (2) Bảo mật Dữ liệu (Data Security),*

(3) Bảo mật Thiết bị đầu cuối (Endpoint Security), (4) Bảo mật Ứng dụng (Application Security), (5) Quản lý Danh tính và Truy cập (Identity & Access Management), (6) Bảo mật hạ tầng/thiết bị IoT (IoT Security). Bên cạnh đó, theo các lĩnh vực công nghệ mới nổi trong thời gian gần đây, các lĩnh vực sau cũng được đưa vào phân tích, bao gồm: Trí tuệ nhân tạo và Học máy, Blockchain, Điện toán đám mây, Bảo mật Zero-Trust, Bảo mật lượng tử, Bảo mật hậu lượng tử.

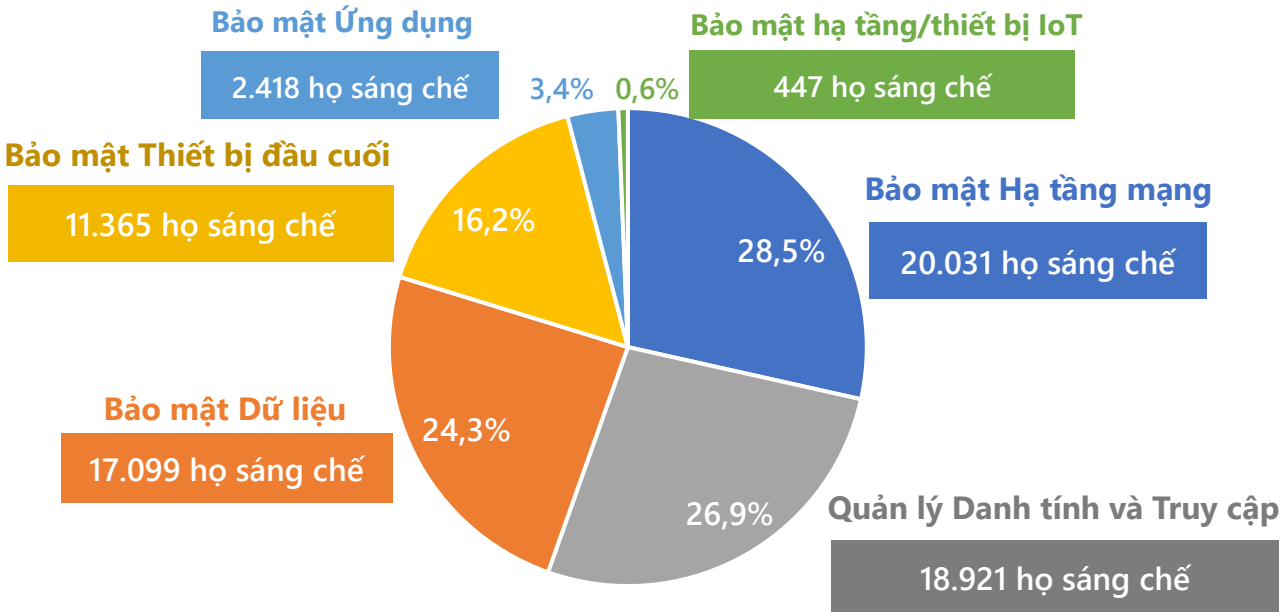
1.4.1 Tỷ lệ sáng chế trong các lĩnh vực an ninh mạng, theo tổng số họ sáng chế đã công bố

Dữ liệu từ WIPS cho thấy, Bảo mật Hạ tầng mạng có số lượng họ sáng chế đăng ký nhiều nhất với hơn 91.000 (chiếm tỷ lệ 36,2%), đứng thứ hai là Bảo mật Dữ liệu với hơn 60.000 họ sáng chế (chiếm tỷ lệ 23,9%), đứng thứ ba là Quản lý Danh tính và Truy cập với hơn 47.000 họ sáng chế (chiếm tỷ lệ 18,7%), đứng thứ 4 là Bảo mật Thiết bị đầu cuối với hơn 41.000 họ sáng chế (chiếm tỷ lệ 16,6%), thứ 5 là Bảo mật Ứng dụng với hơn 10.000 họ sáng chế (chiếm tỷ lệ 4%) và ít nhất là Bảo mật hạ tầng/thiết bị IoT với hơn 1.400 họ sáng chế (chiếm tỷ lệ 0,6%).



Hình 1.6. Tỷ lệ sáng chế trong các lĩnh vực an ninh mạng, theo tổng số họ sáng chế đã công bố, giai đoạn 1973-2025

Xem xét số lượng và tỷ lệ IPFs trong các lĩnh vực an ninh mạng, Bảo mật Hạ tầng mạng vẫn là lĩnh vực dẫn đầu với 20.031 họ sáng chế (chiếm tỷ lệ 28,5%), Quản lý Danh tính và Truy cập lên vị trí thứ 2 với 18.921 họ sáng chế (chiếm tỷ lệ 26,9%, Bảo mật Dữ liệu xuống vị trí thứ 3 với 17.099 họ sáng chế (chiếm tỷ lệ 24,3%), Bảo mật Thiết bị đầu cuối đứng thứ 4 với 11.365 họ sáng chế (chiếm tỷ lệ 16,2%).



Hình 1.6. Tỷ lệ sáng chế trong các lĩnh vực an ninh mạng, theo số lượng IPFs đã công bố, giai đoạn 1973-2025

Trong lĩnh vực *Bảo mật Hạ tầng mạng*, các sáng chế chủ yếu đề cập đến *Giao thức bảo mật mạng* (chiếm đến 87,3% trên tổng số họ sáng chế về Bảo mật Hạ tầng mạng). Một số lượng nhỏ sáng chế còn lại đề cập đến các phương pháp bảo mật như: Sử dụng khóa hoặc thuật toán; Phát hiện hoặc ngăn chặn xâm nhập mạng; Bảo mật đường truyền; và Kiểm tra khả năng bảo mật của mạng. Một số sáng chế có thể kể đến như: *"Phương pháp và hệ thống đồng bộ hóa khóa mã hóa/giải mã trong mạng truyền thông dữ liệu bằng cách sử dụng gói tin đánh dấu"*, giúp cải thiện khả năng đồng bộ hóa và bảo mật của mạng truyền thông dữ liệu bằng cách cho phép cập nhật động các khóa mã hóa/giải mã mà không làm gián đoạn các kết nối đang hoạt động, phát minh này được Tập đoàn IBM (Mỹ) đăng ký bảo hộ lần đầu tại Mỹ ngày 29/01/1996 (mã số US5805705A) và bảo hộ ở quy mô quốc tế tại 4 khu vực (bao gồm: EPO, Đức và Hàn Quốc); Sáng chế *"Phương pháp tiếp cận từ phía đầu để phân phối và quản lý khóa mã hóa an toàn cho các trung tâm dữ liệu đa địa điểm"* giúp cải thiện tính bảo mật và hiệu quả của việc phân phối và quản lý khóa trong các trung tâm dữ liệu đa địa điểm bằng cách giảm thiểu tài nguyên tính toán và lưu trữ, đồng thời cung cấp khả năng truy vết và khắc phục sự cố tốt hơn ở cấp độ gói dữ liệu, phát minh này được Tập đoàn Công nghệ Cisco (Mỹ) đăng ký bảo hộ lần đầu tại Mỹ ngày 22/10/2018 (mã số US10778662B2) và bảo hộ ở quy mô quốc tế tại 5 khu vực (bao gồm: WIPO (PCT), EPO, Canada, Ấn Độ và Trung Quốc).

Trong lĩnh vực *Bảo mật Dữ liệu*, các sáng chế chủ yếu đề cập đến vấn đề *Kiểm soát quyền truy cập dữ liệu* (chiếm 40,4% trên tổng số họ sáng chế về Bảo mật Dữ liệu). Các

sáng chế còn lại đề cập đến các phương pháp bảo mật như: Đảm bảo tính toàn vẹn của dữ liệu; Bảo vệ quyền riêng tư hoặc ẩn danh của người dùng; Bảo vệ quá trình tính toán hoặc xử lý dữ liệu. Các sáng chế trong lĩnh vực Bảo mật Dữ liệu xuất hiện từ rất sớm, có thể kể đến như: Sáng chế *"Cơ chế bảo mật phân cấp để gán động các cấp độ bảo mật cho các chương trình đối tượng"*, cung cấp một cơ chế bảo mật phân cấp cho phép linh hoạt trong việc cho phép một chương trình gọi các chương trình khác trong khi vẫn duy trì tính bảo mật dữ liệu, phát minh này được Tập đoàn IBM (Mỹ) đăng ký bảo hộ lần đầu tại Mỹ ngày 30/12/1976 (mã số US4104721A) và bảo hộ ở quy mô quốc tế tại 3 quốc gia (bao gồm: Anh, Đức và Pháp); Sáng chế mới được đăng ký bảo hộ trong thời gian gần đây như *"Hệ thống, phương pháp và thiết bị máy tính để xác thực tính toàn vẹn dữ liệu"*, bao gồm một hệ thống xác thực tính toàn vẹn dữ liệu với cơ sở dữ liệu người dùng và một thiết bị hộp đen để trả lời các truy vấn cục bộ mà không tiết lộ dữ liệu người dùng được lưu trữ, phát minh này được Công ty Elpis Technologies (Canada) đăng ký bảo hộ lần đầu tại Mỹ ngày 30/12/1976 (mã số US4104721A) và bảo hộ lần thứ hai tại Canada.

Trong lĩnh vực *Quản lý Danh tính và Truy cập*, các sáng chế chủ yếu đề cập đến vấn đề *Xác thực người dùng* (chiếm 57,2% trên tổng số họ sáng chế Quản lý Danh tính và Truy cập). Các sáng chế còn lại đề cập đến các phương pháp như: Xác thực chương trình hoặc thiết bị và Hạn chế truy cập, bảo mật truy cập để ngăn chặn truy cập trái phép. Có thể kể đến như: *"Hệ thống và phương pháp xác thực lẫn nhau kiểm tra tính xác thực của thiết bị trước khi truyền dữ liệu xác thực đến thiết bị"*, giúp cải thiện tính bảo mật của dữ liệu xác thực trên thẻ IC bằng cách đảm bảo rằng mã xác thực chỉ được truyền đến các thiết bị đầu cuối hợp pháp, ngăn chặn truy cập trái phép, phát minh này được Tập đoàn Toshiba (Nhật Bản) đăng ký bảo hộ lần đầu tại Nhật Bản ngày 05/10/1990 (mã số JP1990-266261) và bảo hộ ở quy mô quốc tế tại 3 khu vực khác (bao gồm: EPO, Đức và Mỹ); Sáng chế *"Phương pháp vận hành của thiết bị điện tử để khởi tạo mật khẩu BIOS và các thiết bị điện tử tương tự"*, giúp cải thiện tính bảo mật của việc quản lý mật khẩu BIOS bằng cách đảm bảo rằng chỉ các thiết bị đầu cuối người dùng đã được xác thực mới có thể khởi tạo hoặc khôi phục mật khẩu BIOS, phát minh này được Samsung Electronics (thuộc Tập đoàn Samsung - Hàn Quốc) đăng ký bảo hộ lần đầu tại Hàn Quốc ngày 06/04/2022 (mã số KR10-2022-0043053) và đăng ký bảo hộ ở quy mô quốc tế tại 2 khu vực (WIPO (PCT) và Mỹ).

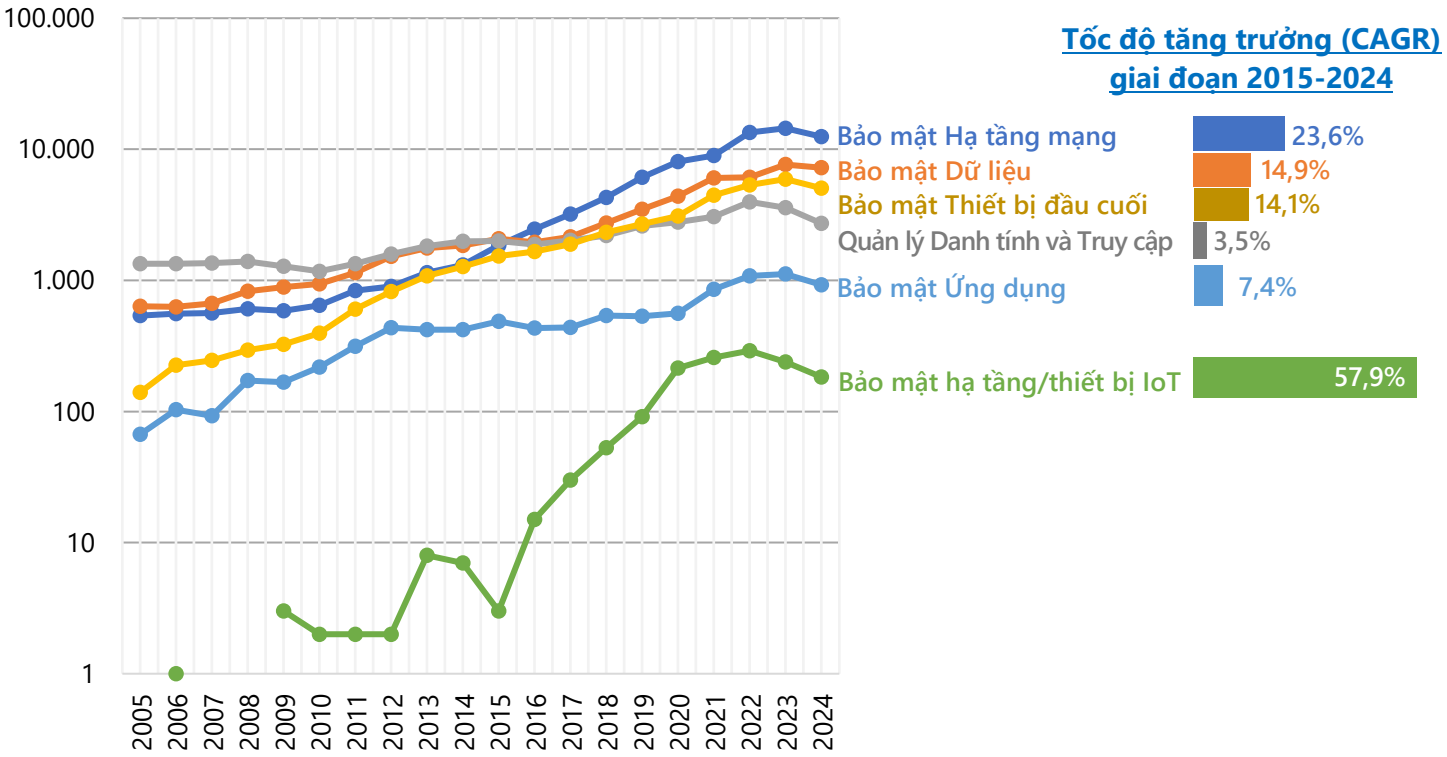
Trong lĩnh vực Bảo mật Thiết bị đầu cuối, các sáng chế chủ yếu đề cập đến vấn đề *Chứng nhận hoặc duy trì các nền tảng máy tính đáng tin cậy* (chiếm 68,8% trên tổng số

họ sáng chế về Quản lý Danh tính và Truy cập). Các sáng chế còn lại đề cập đến việc Giám sát người dùng, chương trình hoặc thiết bị và Bảo mật thiết bị di động và ứng dụng di động. Một số sáng chế nổi bật như: Sáng chế *"Quyền truy cập cấp ứng dụng vào vùng lưu trữ trên thiết bị máy tính"*, giúp cải thiện tính an toàn và bảo mật của việc thực thi ứng dụng trên các thiết bị không dây bằng cách hạn chế quyền truy cập vào các vùng lưu trữ dựa trên ứng dụng đang thực thi, phát minh này được Tập đoàn Qualcomm (Mỹ) đăng ký bảo hộ lần đầu tại Mỹ ngày 13/08/2001 (mã số US60/312177) và bảo hộ ở quy mô quốc tế tại 19 quốc gia, khu vực (bao gồm: WIPO (PCT), EPO, Anh, Úc, Canada, Trung Quốc, Ấn Độ, Nhật Bản, Hàn Quốc, NewZealand, Nga, Singapore,… và có đăng ký bảo hộ tại Việt Nam); *"Phương pháp và thiết bị cải thiện độ tin cậy của giao tiếp giữa máy bay và hệ thống điều khiển từ xa"*, liên quan đến việc cải thiện độ tin cậy của giao tiếp giữa máy bay và hệ thống điều khiển từ xa, đặc biệt là bằng cách đảm bảo an ninh của hệ thống điều khiển từ xa trước khi trao đổi dữ liệu, phát minh này được Airbus Operations SAS (thuộc tập đoàn Airbus - Pháp) đăng ký bảo hộ lần đầu tại Pháp ngày 23/01/2008 (mã số FR2926692B1) và bảo hộ lần thứ hai tại Mỹ.

Trong lĩnh vực Bảo mật Ứng dụng, các sáng chế chủ yếu đề cập đến các biện pháp chống phần mềm độc hại, chẳng hạn như: *"Phương pháp khắc phục các thao tác do chương trình và hệ thống của nó thực hiện"*, nhằm cải thiện việc phát hiện và khắc phục mã độc hại bằng cách cung cấp khả năng giám sát và phân tích hoạt động theo thời gian thực, cho phép phát hiện bao gồm các hành vi tiềm ẩn và các hoạt động độc hại mà quá trình mô phỏng không thể phát hiện, phát minh này được Sentinel Labs Israel (Israel) đăng ký bảo hộ lần đầu tại Mỹ ngày 11/08/2014 (mã số IL250521B) và đăng ký bảo hộ ở quy mô quốc tế tại 8 quốc gia/khu vực (bao gồm: WIPO (PCT), EPO, Anh, Úc, Canada, Nhật Bản, Singapore, Trung Quốc); *"Tạo chữ ký phần mềm độc hại tự động cho hệ thống phát hiện mối đe dọa"* được Tập đoàn IBM (Mỹ) đăng ký bảo hộ lần đầu tại Mỹ ngày 22/01/2019 (mã số US11308210B2) và bảo hộ tiếp tục lần thứ hai tại Trung Quốc; *"Phương pháp phát hiện phần mềm tống tiền, hệ thống liên quan và phương tiện lưu trữ"*, giúp cải thiện hiệu quả và độ chính xác của việc phát hiện phần mềm tống tiền bằng cách thực hiện phát hiện trạng thái mã hóa và hư hỏng tệp dựa trên các phần đặc điểm của tệp, phát minh này được Huawei Technologies (thuộc Tập đoàn Huawei - Trung Quốc) đăng ký bảo hộ lần đầu tại Trung Quốc ngày 29/03/2022 (mã số CN116933253A) và đăng ký bảo hộ ở quy mô quốc tế tại Mỹ và 2 tổ chức quốc tế là WIPO (PCT) và EPO.

Bảo mật Hạ tầng/thiết bị IoT có số lượng họ sáng chế ít nhất nhưng có tốc độ phát triển nhanh nhất, một số sáng chế có thể kể đến như: Sáng chế *"Bảo mật Internet vạn vật với tính toán đa bên (MPC)"*, giúp cải thiện tính bảo mật và quyền riêng tư của các liên lạc trong mạng IoT bằng cách cung cấp một giải pháp phi tập trung, gọn nhẹ và dễ sử dụng để trao đổi khóa và dữ liệu an toàn, phát minh này được Viện Kỹ thuật Hệ thống và Máy tính, Công nghệ và Khoa học (Bồ Đào Nha) đăng ký bảo hộ lần đầu tại Bồ Đào Nha ngày 16/05/2018 (mã số PT11074118) và bảo hộ ở quy mô quốc tế tại 5 quốc gia/khu vực (bao gồm: WIPO(PCT), EPO, Mỹ, Trung Quốc và Nhật Bản); Sáng chế *"Phương pháp điều khiển thiết bị IoT dựa trên quyền truy cập bằng nhận dạng vân tay"*, giúp thực hiện quyền truy cập bằng nhận dạng vân tay cho các thiết bị IoT, cho phép điều khiển an toàn và linh hoạt các thiết bị IoT Wi-Fi mà không cần kết nối có dây, phát minh này được Công ty Espressif Systems (Trung Quốc) đăng ký bảo hộ lần đầu tại Trung Quốc ngày 24/04/2017 (mã số CN106878025B) và bảo hộ ở quy mô quốc tế tại WIPO (PCT) và Mỹ.

Về xu hướng cấp bằng sáng chế cho các lĩnh vực an ninh mạng, có thể thấy Bảo mật hạ tầng/thiết bị IoT và Bảo mật Hạ tầng mạng có xu hướng phát triển nhanh nhất với tốc độ tăng trưởng vòng trong 10 năm gần đây (2015-2024) lần lượt là 57,9% và 23,6% (Hình 1.7).

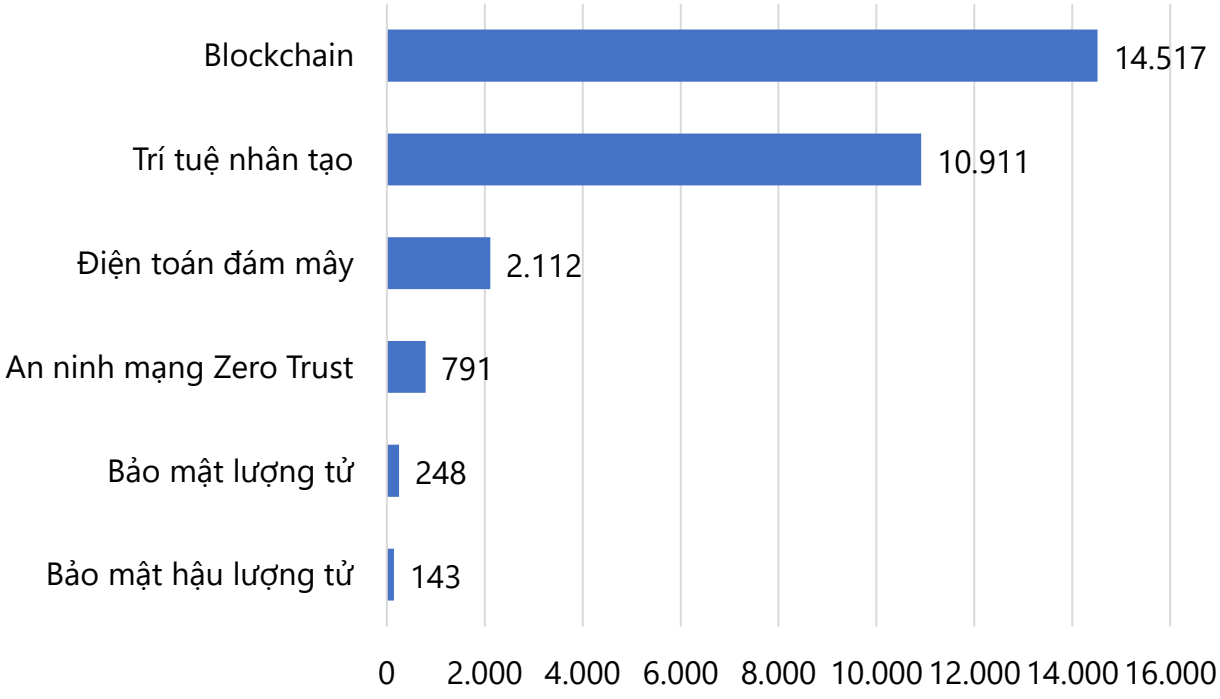


Hình 1.7. Xu hướng đăng ký sáng chế theo các lĩnh vực an ninh mạng và năm công bố sớm nhất, giai đoạn 2005-2024

Các công nghệ liên quan đến Bảo mật Dữ liệu và Bảo mật Thiết bị đầu cuối có mức tăng trưởng ổn định với tốc độ tăng trưởng trong giai đoạn 2015-2024 lần lượt là 14,9% và 14,1%. Công nghệ Bảo mật Ứng dụng, Quản lý Danh tính và Truy cập có tốc độ tăng trưởng khá chậm trong vòng 10 năm trở lại đây, lần lượt là 7,4% và 3,5%. Số lượng sáng chế trong lĩnh vực Bảo mật Hạ tầng mạng chỉ đứng thứ 3 vào năm 2005 nhưng đã liên tục tăng trưởng, đến năm 2016 đã vượt qua các lĩnh vực khác và dẫn đầu trong các lĩnh vực an ninh mạng được quan tâm nghiên cứu.

1.4.2 Phân tích sáng chế công nghệ an ninh mạng theo một số công nghệ mới nổi trong thời gian gần đây

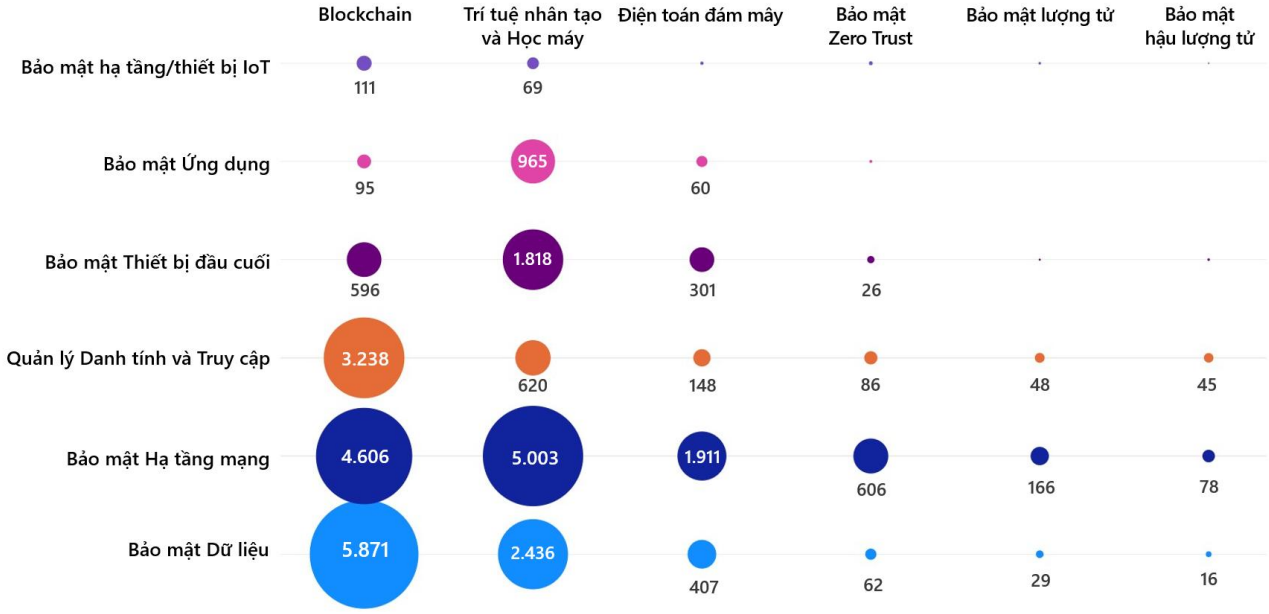
Phân tích theo các từ khóa liên quan đến 6 lĩnh vực công nghệ mới nổi, chỉ có 28.722 họ sáng chế đề cập cụ thể. Trong đó, sáng chế về an ninh mạng đề cập nhiều nhất đến công nghệ Blockchain; đứng thứ hai là công nghệ Trí tuệ nhân tạo (AI) và ứng dụng các thuật toán Học máy (Machine Learning), Học sâu (Deep Learning), công nghệ Điện toán đám mây đứng thứ ba; các công nghệ Bảo mật Zero-Trust, Bảo mật lượng tử, Bảo mật hậu lượng tử hiện chỉ có một số lượng nhỏ sáng chế nhắc đến (Hình 1.8).



Hình 1.8. Một số công nghệ mới nổi được sử dụng trong sáng chế về an ninh mạng

Phân tích theo các lĩnh vực an ninh mạng và công nghệ mới nổi cho thấy, công nghệ Blockchain được sử dụng nhiều trong các sáng chế về Bảo mật dữ liệu, Bảo mật hạ

tầng mạng và Xác thực danh tính và truy cập (Hình 1.9). Công nghệ AI và Học máy được sử dụng nhiều trong các sáng chế về Bảo mật hạ tầng mạng, Bảo mật dữ liệu và Bảo mật Thiết bị đầu cuối. Công nghệ Điện toán đám mây được sử dụng chủ yếu trong Bảo mật Hạ tầng mạng, tương tự với An ninh mạng Zero Trust, Bảo mật lượng tử và Bảo mật hậu lượng tử.



Hình 1.9. Số lượng họ sáng chế công nghệ an ninh mạng theo một số công nghệ mới nổi

Một số sáng chế ứng dụng công nghệ Blockchain trong an ninh mạng như: *"Phương pháp, thiết bị và hệ thống xử lý và xác minh dữ liệu dịch vụ"*, sử dụng blockchain để lưu trữ bản sao dữ liệu trong cơ sở dữ liệu dịch vụ thông thường, đảm bảo cơ sở dữ liệu thông thường có khả năng hoạt động hiệu quả cao và hiệu quả giám sát dữ liệu dịch vụ được đảm bảo, phát minh này được Tập đoàn Alibaba (Trung Quốc) đăng ký bảo hộ lần đầu tại Trung Quốc ngày 06/12/2016 (mã số CN107016542A) và đăng ký bảo hộ ở quy mô quốc tế tại 13 quốc gia/khu vực khác (bao gồm: WIPO (PCT), EPO, Mỹ, Nhật Bản, Hàn Quốc, Ấn Độ, Việt Nam, ...).

Đối với sáng chế ứng dụng công nghệ Trí tuệ nhân tạo trong an ninh mạng, có thể kể đến như: *"Thiết bị phát hiện mã độc hại loại tránh cho hệ thống ảo hóa dựa trên trí tuệ nhân tạo sử dụng các tính năng tích hợp"*, nhằm cải thiện hiệu quả của nhiều sản phẩm bảo mật dựa trên hệ thống ảo hóa trong việc ngăn chặn tác hại xã hội do các biến thể của mã độc hại và mã độc tống tiền gây ra, phát minh này được Công ty SecureLink (Hàn Quốc) đăng ký bảo hộ lần đầu tại Hàn Quốc ngày 12/11/2021 (mã số KR10-2517057B1) và đăng ký bảo hộ ở quy mô quốc tế tại WIPO (PCT) và Mỹ;

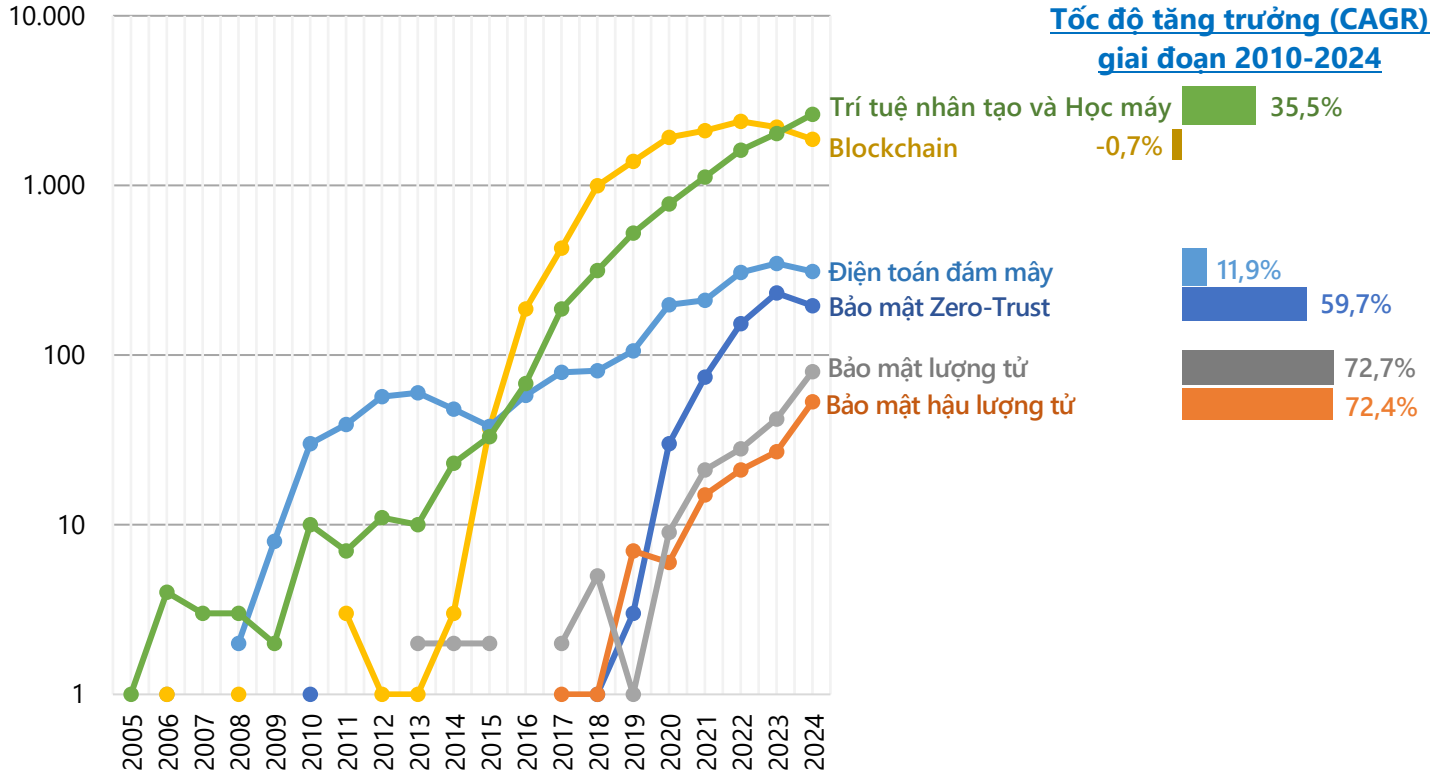
Ứng dụng trong Điện toán đám mây, có các sáng chế như: *"Quản lý khóa bảo mật"*, nhằm cải thiện việc lưu trữ và truy cập dữ liệu an toàn trong hệ thống điện toán đám mây bằng cách cung cấp kiến trúc quản lý khóa bảo mật và kiến trúc N-clave, phát minh này được Tập đoàn Microsoft (Mỹ) đăng ký bảo hộ lần đầu tại Mỹ ngày 14/11/2016 (mã số US10439803B2) và bảo hộ ở quy mô quốc tế tại 22 quốc gia/khu vực (bao gồm: WIPO (PCT), EPO, Úc, Anh, Hàn Quốc, Nhật Bản, Canada, Trung Quốc,…).

Trong Bảo mật Zero-Trust, có các sáng chế như: *"Hệ thống và phương pháp mạng dựa trên DNS không tin cậy"*, liên quan đến mạng dựa trên hệ thống tên miền không tin cậy (zero trust domain name system - ZTDNS) và có thể được áp dụng để bảo mật giao tiếp giữa các thiết bị và tài nguyên máy tính, phát minh này được Tập đoàn Microsoft (Mỹ) đăng ký bảo hộ lần đầu tại Mỹ ngày 01/11/2023 (mã số US2025-0141841A1) và đăng ký bảo hộ ở quy mô quốc tế tại WIPO (PCT).

Một số sáng chế ứng dụng công nghệ Bảo mật lượng tử trong an ninh mạng có thể kể đến như: Sáng chế *"Phương pháp và hệ thống bảo mật chữ ký số"*, cung cấp một phương pháp tạo chữ ký số, xác thực chữ ký số chống lượng tử bằng cách xác thực khóa riêng để xác thực nguồn dữ liệu, và một hệ thống chữ ký số chống lượng tử, phát minh này được Công ty PQCee Private (Singapore) đăng ký bảo hộ lần đầu tại Singapore ngày 05/11/2021 (mã số SG10202112269TA0) và đăng ký bảo hộ ở quy mô quốc tế tại 13 khu vực (bao gồm: WIPO (PCT), EPO, Mỹ, Nhật Bản, Hàn Quốc, Úc, Anh, Canada, Ấn Độ, Trung Quốc, Việt Nam, Indonesia, Mexico).

Một số sáng chế ứng dụng công nghệ Bảo mật hậu lượng tử trong an ninh mạng có thể kể đến như: Sáng chế *"Hệ thống và phương pháp truyền thông an toàn"*, nhằm cải thiện tính bảo mật truyền thông giữa các hệ thống Công nghệ Vận hành (OT) và/hoặc Công nghệ Thông tin (IT) sử dụng Mã hóa Hậu lượng tử (Post-Quantum Encryption - PQE), được Công ty Crowley Government Services (Mỹ) đăng ký bảo hộ lần đầu tại Mỹ ngày 24/03/2023 (mã số US63/454424) và đăng ký bảo hộ ở quy mô quốc tế tại WIPO (PCT).

Về tốc độ tăng trưởng của các sáng chế ứng dụng các công nghệ mới nổi, phân tích cho thấy Bảo mật lượng tử, Bảo mật hậu lượng tử và Bảo mật Zero-Trust có tốc độ tăng rất nhanh trong giai đoạn 5 năm gần đây (2020-2025), lần lượt là 72,7%, 72,4% và 59,7% (Hình 1.10).

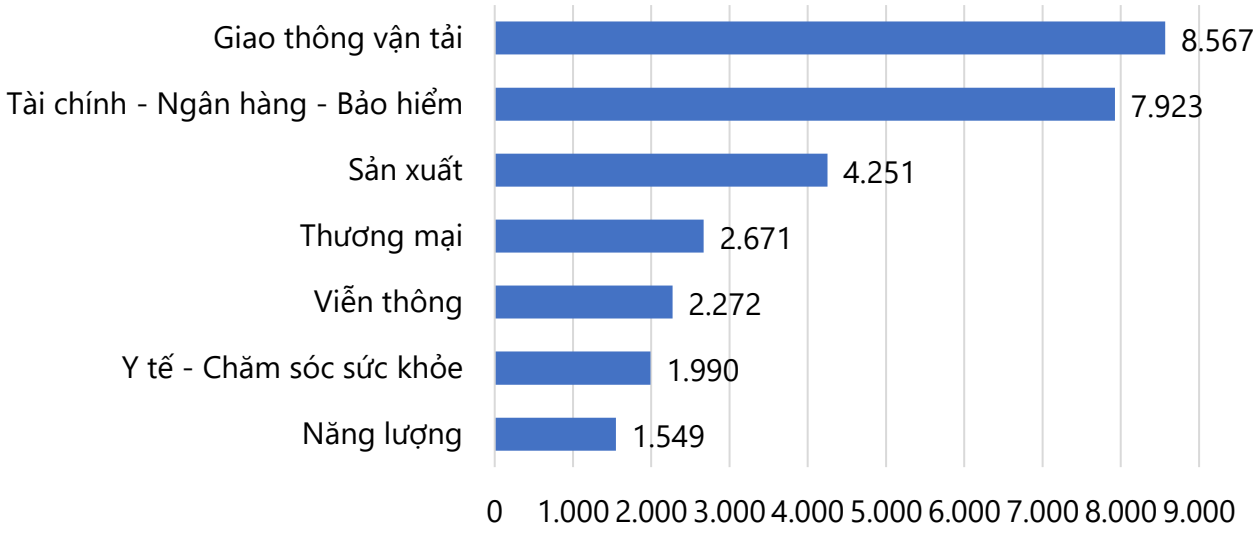


Hình 1.10. Xu hướng đăng ký sáng chế theo lĩnh vực công nghệ mới nổi và năm công bố sớm nhất, giai đoạn 2005-2024

Công nghệ Trí tuệ nhân tạo và Học máy cho thấy sự tăng trưởng ổn định và liên tục với tốc độ tăng trưởng giai đoạn 2020-2024 là 35,5%. Công nghệ điện toán đám mây tăng trưởng ổn định nhưng với tốc độ chậm hơn (11,9%). Còn công nghệ blockchain mặc dù tăng trưởng rất nhanh từ giai đoạn 2014 nhưng đến năm 2020 bắt đầu chững lại.

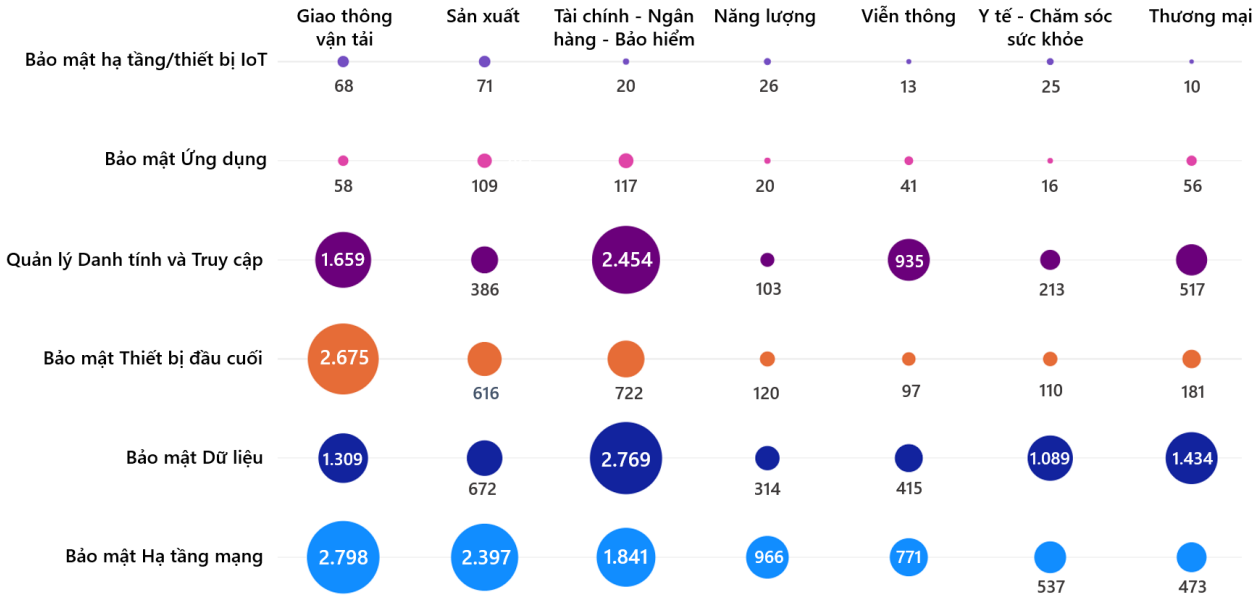
1.4.3 Phân tích sáng chế công nghệ an ninh mạng theo các ngành/lĩnh vực công nghiệp ứng dụng

Phân tích theo các từ khóa liên quan đến 7 ngành công nghiệp, chỉ có 29.223 họ sáng chế đề cập cụ thể. Trong đó, sáng chế về an ninh mạng được ứng dụng nhiều nhất trong ngành Giao thông vận tải; ứng dụng nhiều thứ hai là trong các ngành Tài chính - Ngân hàng - Bảo hiểm; ứng dụng nhiều thứ ba là trong ngành Sản xuất, các ngành được ứng dụng nhiều tiếp theo lần lượt là Thương mại, Viễn thông, Y tế - Chăm sóc sức khỏe và Năng lượng (Hình 1.11).



Hình 1.11. Số lượng họ sáng chế về an ninh mạng được ứng dụng trong các ngành công nghiệp

Phân tích theo các lĩnh vực an ninh mạng và các ngành công nghiệp, ngành Giao thông vận tải với phần với các sáng chế tập trung vào Bảo mật Hạ tầng mạng, Bảo mật Thiết bị đầu cuối, Xác thực danh tính và Bảo mật dữ liệu (Hình 1.12). Ngành Tài chính - Ngân hàng - Bảo hiểm với các sáng chế tập trung vào Bảo mật dữ liệu, Xác thực danh tính và Bảo mật Hạ tầng mạng. Ngành Sản xuất và Năng lượng với các sáng chế tập trung vào Bảo mật Hạ tầng mạng. Ngành Thương mại và Y tế-Chăm sóc sức khỏe với các sáng chế tập trung vào Bảo mật Dữ liệu. Ngành viễn thông với các sáng chế tập trung vào Xác thực danh tính và Bảo mật Hạ tầng mạng.



Hình 1.12. Số lượng họ sáng chế công nghệ an ninh mạng theo các ngành/lĩnh vực công nghiệp ứng dụng

Ngành Giao thông vận tải với các phương tiện tự hành, hoặc được lắp đặt các thiết bị điện tử thông minh dễ trở thành mục tiêu của tấn công mạng. Một số sáng chế về an ninh mạng ứng dụng trong ngành Giao thông vận tải có thể kể đến như: Sáng chế *"Thiết bị kiểm soát truy cập và phương pháp kiểm soát truy cập"*, nhằm giải quyết vấn đề hạn chế truy cập vào API của xe từ bên ngoài xe một cách phù hợp, ngăn ngừa rò rỉ thông tin cá nhân và điều khiển xe trái phép, phát minh này được Tập đoàn Denso (Nhật Bản) đăng ký bảo hộ lần đầu tại Nhật Bản ngày 29/09/2022 (mã số JP2022-156690) và đăng ký bảo hộ ở quy mô quốc tế tại 4 quốc gia/khu vực (bao gồm: WIPO (PCT), Mỹ, Đức và Trung Quốc).

Ngành Tài chính-Ngân hàng-Bảo hiểm với các thách thức trong quản lý danh tính và bảo mật dữ liệu giao dịch và khách hàng. Một số sáng chế về an ninh mạng ứng dụng trong ngành Tài chính-Ngân hàng-Bảo hiểm như: *"Thẻ giao dịch động được bảo vệ bằng xác thực đa yếu tố"*, nhằm cải thiện tính bảo mật của các giao dịch tài chính bằng cách sử dụng xác thực đa yếu tố, phát minh này được Công ty Capital One Services (thuộc Tập đoàn tài chính Capital One - Mỹ) đăng ký bảo hộ lần đầu tại Mỹ ngày 28/12/2016 (mã số US10535068B2) và đăng ký bảo hộ ở quy mô quốc tế tại EPO và Canada.

Ngành Sản xuất ngày nay với các hệ thống robotics, thiết bị công nghiệp thông minh cần phải đảm bảo an toàn kết nối mạng để cho quá trình sản xuất không bị gián đoạn và mất kiểm soát. Một số sáng chế về an ninh mạng ứng dụng trong ngành Sản xuất như: *"Phương pháp thiết lập kết nối an toàn với thiết bị công nghiệp"*, nhằm tạo ra một mạng riêng ảo (VPN), thiết lập kết nối an toàn với thiết bị công nghiệp và có thể được áp dụng cho nhiều môi trường công nghiệp khác nhau như môi trường Công nghiệp 4.0 hoặc môi trường Internet vạn vật công nghiệp (IIoT), phát minh này được Công ty Schneider Electric Industries SAS (thuộc tập đoàn Schneider Electric - Pháp) đăng ký bảo hộ quốc tế lần đầu trên phạm vi toàn Châu Âu ngày 22/03/2024 tại EPO (mã số EP4622175A1) và các lần tiếp theo tại Mỹ và Trung Quốc.

Ngành Năng lượng đối mặt với các thách thức trong đảm bảo an toàn mạng lưới chống lại các cuộc tấn công mạng (như ransomware) có thể gây tê liệt hệ thống. Một số sáng chế về an ninh mạng ứng dụng trong ngành Năng lượng như: *"Phương pháp và hệ thống phòng thủ chủ động đối với các mối đe dọa chưa biết"*, nhằm thực hiện dự đoán mối đe dọa trên dữ liệu mạng thu được từ mạng thông tin điện lực trong thời gian thực, qua đó hình thành một hệ thống bảo vệ an ninh tinh vi và tự thích ứng hơn, cải thiện khả năng giám sát và cảnh báo sớm các sự kiện an ninh hệ thống, và

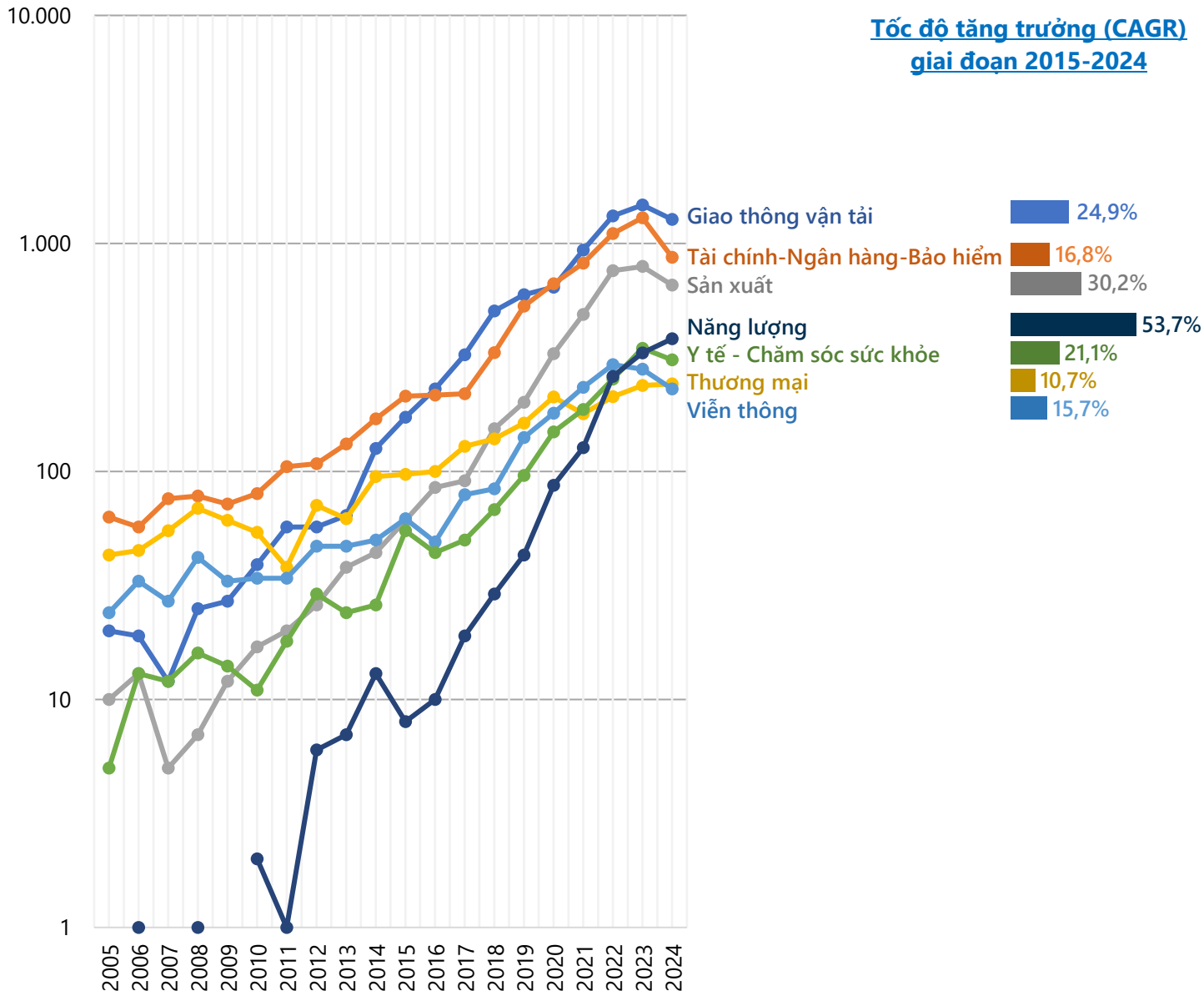
nâng cao mức độ phòng thủ tổng thể của mạng lưới điện, phát minh này được phối hợp nghiên cứu và đăng ký bảo hộ lần đầu bởi 3 đơn vị (Công ty TNHH Điện lực Giang Tô, Công ty TNHH Công nghệ thông tin và Truyền thông NARI và Đại học Khoa học và Công nghệ Nam Kinh), bảo hộ lần đầu tại Trung Quốc ngày 16/08/2023 (mã số CN116760636A) và đăng ký bảo hộ ở quy mô quốc tế tại WIPO (PCT) và Mỹ.

Ngành Y tế - Chăm sóc sức khỏe với các hệ thống y tế và hồ sơ sức khỏe điện tử đặt ra yêu cầu lớn về bảo mật dữ liệu và hạ tầng mạng. Một số sáng chế về an ninh mạng ứng dụng trong ngành Y tế - Chăm sóc sức khỏe như: Sáng chế *"Truyền thông an toàn trong hệ thống giám sát y tế"*, nhằm giải quyết thách thức bảo vệ dữ liệu nhạy cảm khỏi bị chặn và giả mạo khi sử dụng các thiết bị y tế công suất thấp với khả năng tính toán giảm cho các quy trình mã hóa hoặc giải mã, phát minh này được Công ty Abbott Diabetes Care thuộc Tập đoàn Abbott Laboratories - Mỹ) đăng ký bảo hộ lần đầu tại Mỹ ngày 31/08/2020 (mã số US12126995B2) và đăng ký bảo hộ ở quy mô quốc tế tại 6 quốc gia/khu vực (bao gồm: WIPO (PCT), EPO, Úc, Canada, Trung Quốc và Nhật Bản).

Ngành Thương mại, đặc biệt là thương mại điện tử cũng đối mặt các nguy cơ lừa đảo, mã độc, tấn công DDoS, đến các lỗ hổng bảo mật chuỗi cung ứng, đe dọa dữ liệu khách hàng và doanh nghiệp. Một số sáng chế về an ninh mạng ứng dụng trong ngành Thương mại như: Sáng chế *"Nền tảng mã hóa"*, nhằm giải quyết những hạn chế của các quy trình thương mại điện tử truyền thống bằng cách cung cấp một tập hợp các khả năng để lưu trữ, giao dịch, chuyển giao, trao đổi và xử lý một tập hợp các liên kết được mã hóa an toàn, phát minh này được Công ty Verona Pharma (thuộc Tập đoàn Merck - Mỹ) đăng ký bảo hộ lần đầu tại Mỹ ngày 02/11/2018 (mã số US11334875B2) và đăng ký bảo hộ ở quy mô quốc tế tại 11 quốc gia/khu vực (bao gồm: WIPO (PCT), EPO, Úc, Canada, Trung Quốc, Ý, Ấn Độ, Nhật Bản,...).

Ngành Viễn thông đang đối mặt với nhiều thách thức về quản lý truy cập và bảo mật hạ tầng mạng. Một số sáng chế về an ninh mạng ứng dụng trong ngành Viễn thông như: *"Phương pháp nội hóa các chức năng bảo mật trong mạng lõi 5G được thực hiện bởi SDAF (Chức năng Phân tích Dữ liệu Bảo mật)"*, nhằm giải quyết sự thiếu hụt chức năng mạng cho các chức năng bảo mật trung gian trong mạng lõi 5G SBA (Service-Based Architecture) và sự thiếu vắng phương pháp nhúng các chức năng bảo mật vào mạng lõi, được Quỹ Hợp tác Học viện Công nghiệp Đại học Kookmin (Hàn Quốc) đăng ký bảo hộ lần đầu tại Hàn Quốc ngày 06/12/2023 (mã số KR10-2025-0086263A) và đăng ký bảo hộ ở quy mô quốc tế tại WIPO thông qua PCT.

Về tốc độ tăng trưởng của sáng chế công nghệ an ninh mạng trong các ngành công nghiệp trong 10 năm qua (giai đoạn 2015-2024), phân tích cho thấy hầu hết các ngành đều tăng trưởng dương hai con số (Hình 1.13). Trong đó, ngành Năng lượng tăng trưởng rất nhanh, với tốc độ tăng trưởng là 53,7%, đứng thứ 2 là ngành Sản xuất với tốc độ tăng trưởng là 30,2%, đứng thứ 3 là ngành Giao thông vận tải với tốc độ tăng trưởng là 24,9%, thứ 4 là ngành y tế-chăm sóc sức khỏe với tốc độ tăng trưởng là 21,1%. Các ngành còn lại (Tài chính-Ngân hàng-Bảo hiểm; Viễn Thông và Thương mại) với mức tăng trưởng chậm hơn, lần lượt là 16,8%, 15,7% và 10,7%.

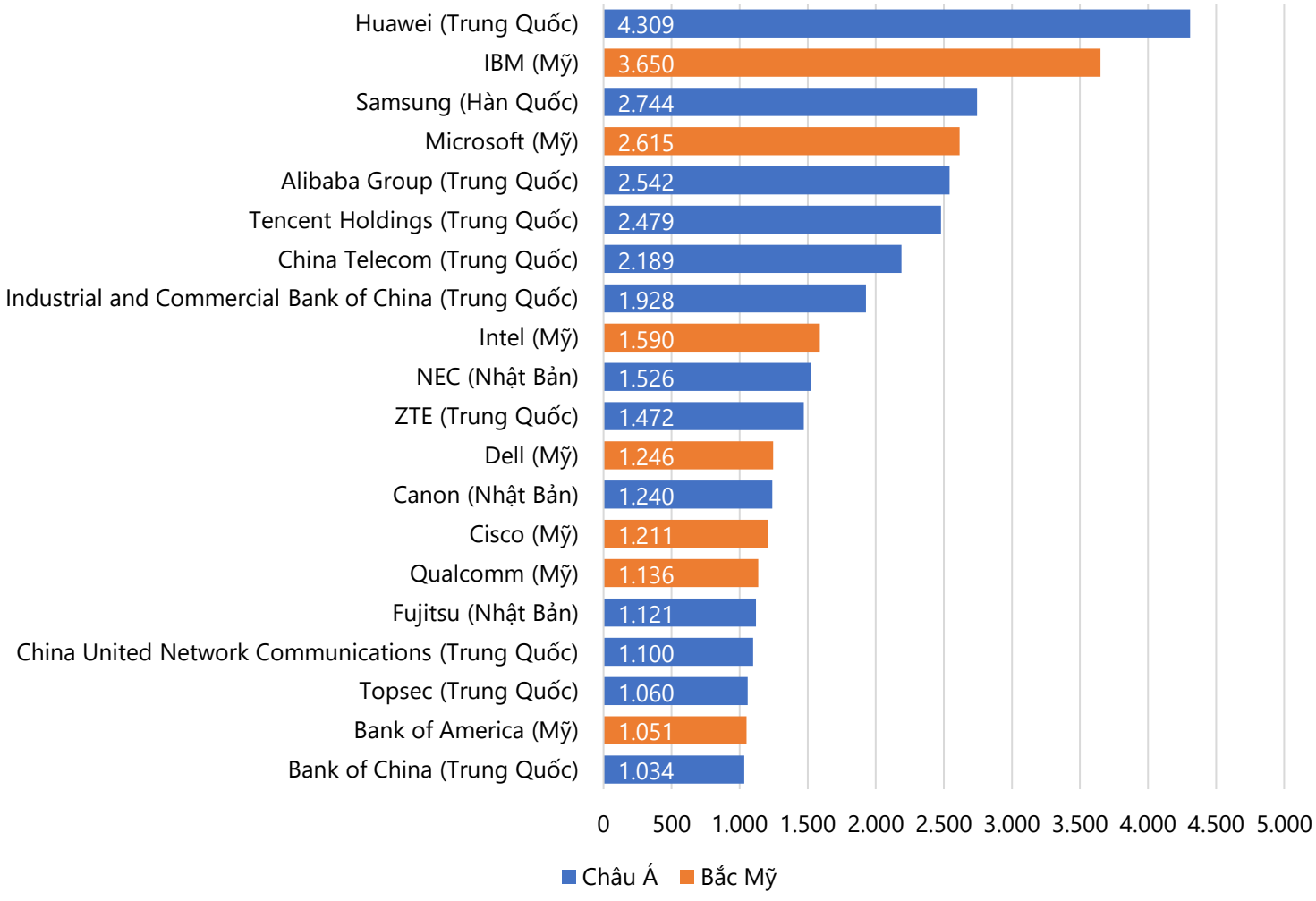


Hình 1.13. Xu hướng đăng ký sáng chế theo ngành công nghiệp được ứng dụng và năm công bố sớm nhất, giai đoạn 2005-2024

1.5 Các tổ chức dẫn đầu về sở hữu sáng chế công nghệ an ninh mạng

1.5.1 Các tổ chức dẫn đầu về sở hữu sáng chế công nghệ an ninh mạng trên thế giới, theo tổng số họ sáng chế được công bố

Tập đoàn Huawei (Trung Quốc) là đơn vị dẫn đầu sở hữu các sáng chế về công nghệ an ninh mạng, với 4.309 họ sáng chế (không bao gồm các sáng chế đồng chủ đơn với các tổ chức khác), đứng thứ 2 là Tập Đoàn IBM (Mỹ) với 3.650 họ sáng chế, đứng thứ 3 là Tập đoàn Samsung (Hàn Quốc) với 2.744 họ sáng chế, đứng thứ 4 là Tập đoàn Microsoft (Mỹ) với 2.615 họ sáng chế, đứng thứ 5 là Tập đoàn Alibaba (Trung Quốc) với 2.542 họ sáng chế.

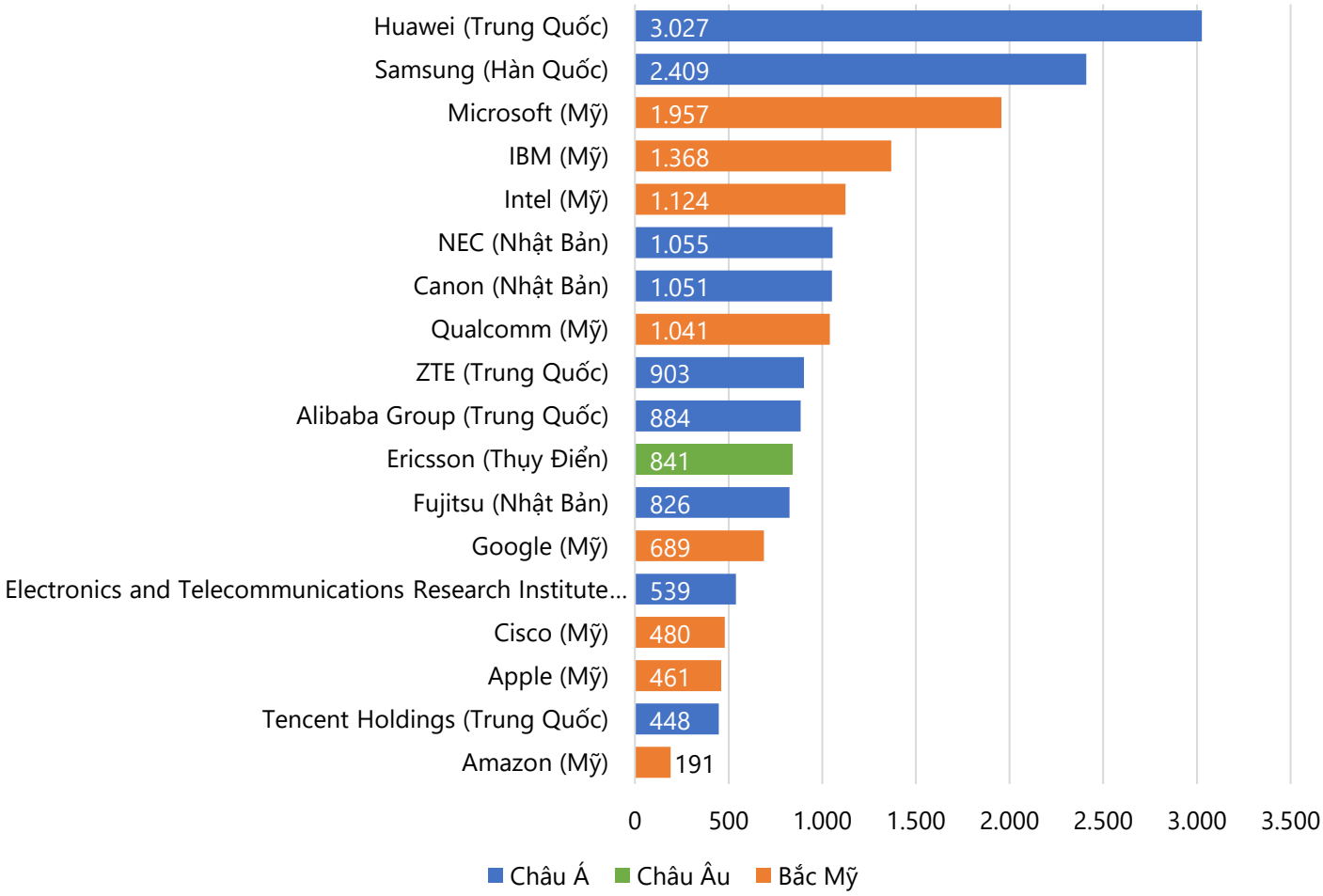


Hình 1.14. Top 20 tổ chức dẫn đầu về sở hữu sáng chế công nghệ an ninh mạng trên thế giới, theo tổng số họ sáng chế được công bố trong giai đoạn 1973-2025

Có thể thấy, trong 20 tổ chức dẫn đầu sở hữu sáng chế công nghệ an ninh mạng, chủ yếu là các tập đoàn công nghệ của Trung Quốc (9) và Mỹ (7), Nhật Bản (3) và Hàn Quốc (1).

1.5.2 Các tổ chức dẫn đầu về sở hữu sáng chế công nghệ an ninh mạng trên thế giới, theo số họ sáng chế quốc tế (IPFs) được công bố

Tập đoàn Huawei (Trung Quốc) tiếp tục dẫn đầu sở hữu sáng chế quốc tế với 3.027 IPFs; Tập đoàn Samsung (Hàn Quốc) vươn lên vị trí thứ hai với 2.409 IPFs; Tập đoàn Microsoft (Mỹ) vươn lên vị trí thứ 3 với 1.957 IPFs; còn Tập đoàn IBM (Mỹ) xuống vị trí thứ 4 với 1.368 IPFs. Có thể thấy trong các tổ chức sở hữu nhiều IPFs, xuất hiện 1 đại diện của Châu Âu, Tập đoàn Ericsson (Thụy Điển), còn lại các tập đoàn công nghệ của Châu Á vẫn tiếp chiếm ưu thế lớn so với các khu vực khác.



Hình 1.15. Top 18 tổ chức dẫn đầu về sở hữu sáng chế công nghệ an ninh mạng trên thế giới, theo số họ sáng chế quốc tế (IPFs) được công bố trong giai đoạn 1973-2025

PHẦN 2 - CÁC GIẢI PHÁP AN NINH MẠNG ĐÃ ĐƯỢC NGHIÊN CỨU VÀ ỨNG DỤNG TẠI VIỆT NAM

2.1 Sáng chế về công nghệ an ninh mạng được đăng ký bảo hộ tại Việt Nam

Từ nguồn cơ sở dữ liệu của Cục Sở hữu Trí tuệ, tính đến tháng 10/2025, có 131 sáng chế, giải pháp hữu ích đề cập đến công nghệ an ninh mạng đã được công bố bảo hộ tại Việt Nam từ năm 1999 đến nay. Trong đó, 32 sáng chế, giải pháp hữu ích có chủ đơn là các viện nghiên cứu, trường đại học, cơ quan quản lý nhà nước và doanh nghiệp Việt Nam, còn lại là các chủ đơn đến từ Trung Quốc (33), Mỹ (31), Phần Lan (10), Anh (7), Singapore (3), ... Các chủ đơn đăng ký sáng chế nổi bật có thể kể đến: Tập đoàn Qualcomm (Mỹ) với 22 sáng chế, giải pháp hữu ích; Tập đoàn Huawei (Trung Quốc) với 17 sáng chế, giải pháp hữu ích; Tập đoàn Nokia (Phần Lan) với 10 sáng chế, giải pháp hữu ích. Ngoài các tập đoàn nước ngoài, các tổ chức KH&CN trong nước như Viện Công nghệ thông tin (ĐHQG Hà Nội) và Trường Đại học Bách khoa (ĐHQG TP.HCM), và các doanh nghiệp trong nước như Viettel, BKAV, VinAI,... cũng có những sáng chế được bảo hộ. Các sáng chế, giải pháp hữu ích về công nghệ an ninh mạng đăng ký bảo hộ tại Việt Nam chủ yếu đề cập đến Bảo mật Hạ tầng mạng (63 sáng chế, giải pháp hữu ích, chiếm tỷ lệ 48,1%) và Quản lý Danh tính và Truy cập (42 sáng chế, giải pháp hữu ích, chiếm tỷ lệ 32,1%).

Một số đơn sáng chế có tác giả/chủ đơn là các tổ chức/nhà khoa học Việt Nam có thể điểm qua như sau:

2.1.1 Bảo mật Hạ tầng mạng

- **Hệ thống thông tin thủy âm số sử dụng công nghệ đa truy cập phân chia theo mã (CDMA) và phương pháp bù dịch tần Doppler kết hợp khôi phục dữ liệu trong miền thời gian cho hệ thống này**

Số đơn: VN 1-2025-01702

Ngày công bố đơn: 25/06/2025

Chủ đơn: Đại học Bách khoa Hà Nội

Tác giả: Nguyễn Quốc Khương, Nguyễn Văn Đức

Tóm tắt: Sáng chế đề cập tới việc thiết kế một hệ thống thông tin không dây dưới nước sử dụng công nghệ CDMA. Sáng chế giải quyết hai vấn đề quan trọng trong thông tin. Thứ nhất là vấn đề bù dịch tần Doppler do có sự chuyển động tương đối giữa bên phát và bên thu. Để bù dịch tần sáng chế thực hiện hai bước. Bước thứ nhất là thực hiệu bù thô thông qua việc tính gần đúng độ dịch tần Doppler và lấy mẫu lại tín hiệu. Tiếp đó độ dư lệch tần sẽ được hiệu chỉnh tinh thông qua kỹ thuật xoay pha chòm sao của tín hiệu thu được. Vấn đề thứ hai là đề xuất một thuật toán ước lượng kênh trong miền thời gian mà không cần sử dụng tín hiệu dẫn đường cho hệ thống CDMA. Hệ thống truyền thông không dây dưới nước CDMA nhờ vậy có độ bảo mật cao và tính chống nhiễu tốt hơn hệ thống thông thường.

- **Phương pháp xác thực, phân quyền và bảo mật kết nối giữa các dịch vụ nhỏ trong hệ thống kiến trúc dịch vụ phân tán tầm trung**

Số đơn: VN 1-2024-09792

Ngày công bố đơn: 26/05/2025

Chủ đơn: Tập đoàn Công nghiệp - Viễn thông Quân Đội (Viettel)

Tác giả: Nguyễn Văn Cương, Võ Hoài Nam, Vũ Huy Hùng

Tóm tắt: Sáng chế đề xuất phương pháp xác thực, phân quyền và bảo mật trong hệ thống kiến trúc dịch vụ nhỏ phân tán tầm trung nhằm mục đích tăng cường bảo mật cho hệ thống, giảm thiểu tối đa ảnh hưởng trước sự tấn công trái phép từ bên trong cũng như bên ngoài mạng lưới dịch vụ, giảm tác động tiêu cực tới hệ thống trong trường hợp thông tin tài khoản người dùng bị đánh cắp hoặc làm giả mạo nhằm truy cập trái phép. Phương pháp được thực hiện qua các bước: xây dựng bộ luật ánh xạ kết nối từ người dùng tới các dịch vụ trong hệ thống, thông qua dịch vụ máy chủ web (web server); xây dựng bộ luật kiểm soát luồng truy cập, mã hóa giao tiếp giữa người dùng với hệ thống, và giữa các dịch vụ với nhau; phân phối và thực thi bộ luật kiểm soát truy cập, mã hóa giao tiếp trong hệ thống.

- **Hệ thống lõi bảo mật lớp IP (IPSec CORE) bằng giải thuật mã hóa nâng cao kết hợp bộ đếm trường Galois (AES-GCM) sử dụng hai máy trạng thái độc lập kết hợp phương pháp mở rộng bản mã đa luồng, được thiết kế ở cấp độ chuyển thanh ghi (RTL)**

Số đơn: VN 1-2023-07853

Ngày công bố đơn: 25/01/2024

Chủ đơn: Trường Đại học Bách khoa - Đại học Quốc gia TP.HCM

Tác giả: PGS.TS. Hoàng Trang

Tóm tắt: Sáng chế đề cập đến hệ thống lõi bảo mật lớp IP (IPSec CORE) bằng giải thuật mã hóa nâng cao kết hợp bộ đếm trường Galois (AES-GCM) sử dụng hai máy trạng thái độc lập kết hợp phương pháp mở rộng bản mã đa luồng, được thiết kế ở cấp độ chuyển thanh ghi (RTL). Hệ thống lõi IPSec này có chức năng mã hóa xác thực và giải mã xác thực dựa trên nền tảng mã hóa nâng cao kết hợp bộ đếm trường Galois hay còn gọi là AES-GCM 128 bít, có khả năng cung cấp kết nối bảo mật làm phần lõi cho các thiết bị định tuyến (router), trên nền tảng lớp mạng trong mô hình OSI với tốc độ cao. Lõi IP mềm này có thể tương thích với hầu hết các thiết bị phần cứng FPGA và có thể kết hợp với các nền tảng khác thông qua giao tiếp miniPCIe hoặc các chuẩn giao tiếp phổ biến để tạo thành một hệ thống mã hóa xác thực và giải mã xác thực hoàn chỉnh. Lõi bảo mật lớp IP mã hóa và giải mã thực hiện trên nền tảng mã hóa nâng cao AES đảm nhiệm tác vụ mã hóa và giải mã gói tin. Phần bộ đếm Galois giúp xác thực dữ liệu. Phương pháp mở rộng bản mã đa luồng giúp lõi bảo mật lớp IP đạt thông lượng cao, đồng thời tối ưu được lượng tài nguyên khi sử dụng trên mảng cổng logic khả trình bằng trường (FPGA) hoặc mạch tích hợp chuyên dụng (ASIC) sau này. Thông qua các chuẩn giao tiếp tạo thành hệ thống hoàn chỉnh, đáp ứng được yêu cầu của một phần lõi cho chức năng mã hóa, giải mã, xác thực hiện nay.

- **Quy trình thiết kế phần cứng bảo mật cân bằng giữa chi phí thực thi và mức độ bảo mật**

Số đơn: VN 1-2023-06893

Ngày công bố đơn: 25/01/2024

Chủ đơn: Viện Công nghệ thông tin - Đại học Quốc gia Hà Nội

Tác giả: Trần Xuân Tú, Đào Mạnh Hiệp, Bùi Duy Hiếu

Tóm tắt: Sáng chế mô tả quy trình thiết kế phần cứng hệ thống bảo mật đảm bảo hiệp thương giữa chi phí thực thi phần cứng và mức độ bảo mật của hệ thống. Quy trình thiết kế gồm 8 bước: (301) xây dựng đặc tả thiết kế; (302) ước lượng và đánh giá tiền thiết kế phần cứng; (303) thiết kế phần cứng dưới dạng chuyển dịch thanh ghi (RTL); (304) mô phỏng và kiểm chứng chức năng thiết kế; (305) tổng hợp phần cứng; (306) mô phỏng và kiểm chứng thiết kế hậu tổng hợp; (307) ước lượng, bóc tách và đánh giá lưu vết công suất; và (308) tích hợp để sản xuất vi mạch. Trong đó, bước (302) bao gồm 6 công đoạn nhằm ước lượng và đánh giá các lựa chọn thiết kế, cụ

thể: (401) lựa chọn thuật toán, kiến trúc; (402) ước lượng giả lưu vết công suất của các khối cơ sở; (403) tổng hợp giả lưu vết của hệ thống; (404) đánh giá bảo mật của giả lưu vết; (405) ước lượng chi phí thực thi phần cứng của hệ thống; (406) đánh giá chi phí thực thi của hệ thống.

- **Phương pháp phát hiện bất thường trong mạng**

Số bằng: VN1-0049501-000

Ngày cấp bằng: 02/07/2025

Chủ bằng & Tác giả: PGS.TS. Đỗ Xuân Chợ.

Tóm tắt: Sáng chế đề cập đến phương pháp phát hiện bất thường trong mạng bao gồm: phân tích, bởi công cụ mạng IDS (Intrusion Detection System - Hệ thống Phát hiện Xâm nhập), lưu lượng mạng để lưu lại nhật ký lưu lượng mạng mà chứa các thành phần chứa các dấu hiệu trong lưu lượng mạng có liên quan đến HTTP (Hyper Text Transfer Protocol), DNS (Domain Name System), TLS (Transport Layer Security), và tệp tin; so khớp các dấu hiệu trong lưu lượng mạng đã nêu với tập dấu hiệu bất thường hoặc kiểm tra các dấu hiệu trong lưu lượng mạng đã nêu bằng tập luật phát hiện tấn công dựa trên dữ liệu tổng hợp về các cuộc tấn công mạng đã biết trước đó. Nếu kết quả là có bất thường trong mạng thì có thể phát hiện được rất nhanh chóng và đơn giản. Trái lại, nếu kết quả là không có bất thường trong mạng thì tiếp tục thực hiện việc phát hiện bất thường bằng cách trích xuất các đặc trưng có trong nhật ký liên quan đến HTTP, nhật ký liên quan đến DNS, nhật ký liên quan đến TLS, và nhật ký liên quan đến tệp tin của lưu lượng mạng, và tập hợp toàn bộ các đặc trưng được xác định trước này thành một vec tơ đặc trưng của lưu lượng mạng làm đầu vào cho mô hình rừng ngẫu nhiên (Random Forest) đã được huấn luyện và kiểm thử, để phát hiện xem liệu có bất thường trong mạng hay không. Nhờ tiếp tục thực hiện việc phát hiện bất thường bằng mô hình máy học, sáng chế được cho là tăng khả năng phát hiện các bất thường trong mạng mà chưa được biết trước một cách đáng kể.

- **Phương pháp ngăn chặn tấn công từ chối dịch vụ kiểu TCP SYN**

Số bằng: VN1-0039924-000

Ngày cấp bằng: 24/04/2024

Chủ bằng: Đại học Bách Khoa Hà Nội

Tác giả: Nguyễn Hữu Thanh, Nguyễn Minh Hiếu, Lê Công Tuấn, Đinh Khắc Tuyến, Nguyễn Danh Nghĩa

Tóm tắt: Sáng chế đề cập đến phương pháp ngăn chặn tấn công từ chối dịch vụ TCP SYN, được thực hiện tại máy chủ và/hoặc các nút mạng trung gian để chống tấn công ngập lụt. Phương pháp này được xây dựng trên cơ sở bộ lọc Bloom để xác định xem liệu bản tin TCP SYN, là bản tin với cờ SYN để yêu cầu thiết lập kết nối theo cơ chế bắt tay 3 bước theo giao thức TCP (Transmission Control Protocol) được gửi từ thực thể mạng có yêu cầu kết nối tới máy chủ, là bản tin được gửi lần đầu hay bản tin được gửi lần tiếp theo. Trong trường hợp bản tin SYN được gửi từ cuộc tấn công mạng, thông thường sẽ không có bản tin SYN tiếp theo của luồng thông tin tương ứng được gửi lại. Do đó trong giải pháp này nếu bản tin SYN được gửi lần đầu tiên bản tin này sẽ được loại bỏ, nhờ đó ngăn chặn được cuộc tấn công mạng. Trái lại, nếu bản tin SYN được gửi từ người dùng thật, bản tin SYN tiếp theo của luồng thông tin tương ứng sẽ được gửi lại, nhờ đó giúp người dùng này có thể kết nối và truy cập tới máy chủ. So với các phương pháp ngăn chặn tấn công TCP SYN trước đây, tài nguyên cần thiết trên các thiết bị bảo mật trong phương pháp sử dụng bộ lọc Bloom nhỏ hơn một cách đáng kể, từ đó tăng độ tin cậy và khả năng chống chịu của hệ thống với các cuộc tấn công, do đó có thể được sử dụng để ngăn chặn các cuộc tấn công TCP SYN quy mô lớn.

- **Thiết bị kết nối có bảo mật dữ liệu trên đường truyền**

Số đơn: VN 2-2020-00305

Ngày công bố đơn: 25/01/2022

Chủ đơn: Viện Công nghệ thông tin - Viện Hàn lâm Khoa học và Công nghệ Việt Nam

Tác giả: Đặng Thành Trung, Vương Huy Hoàng, Phạm Ngọc Minh, Vũ Thị Quyên, Đặng Mạnh Chính

Tóm tắt: Giải pháp hữu ích đề cập đến thiết bị kết nối có bảo mật dữ liệu đường truyền và tích hợp các chuẩn truyền thông, như chuẩn truyền thông công nghiệp, chuẩn truyền thông không dây, ..., và có thể được áp dụng trong hệ thống IoT. Theo giải pháp hữu ích, các thông số từ mạng cảm biến, thiết bị công nghiệp được truyền qua mạng RS232, RS485 bằng giao thức Modbus tới thiết bị kết nối. Tại đây, dữ liệu được mã hóa bằng thuật toán trao đổi khóa Diffie - Hellman kết hợp với thuật toán RC4. Thuật toán này được tích hợp trên bộ vi xử lý tốc độ cao trong thiết bị kết nối giúp đảm bảo an toàn và tăng tính tin cậy của hệ thống. Sau đó dữ liệu mã hóa sẽ được truyền đến máy chủ (Server) qua chuẩn kết nối Ethernet, Wifi, 3G, 4G - LTE. Nhờ thiết bị này mà người sử dụng có thể giám sát và điều khiển từ xa qua kết nối Internet đáp ứng xu thế phát triển của IoT trong thời đại công nghiệp hiện nay.

- **Phương pháp mã hoá, giải mã trên đường truyền từ máy chủ đến thiết bị cổng kết nối Internet vạn vật (IoTs - Internet of Things)**

Số đơn: VN 1-2020-05601

Ngày công bố đơn: 25/01/2021

Chủ đơn: Sở Khoa học và Công nghệ TP.HCM

Tác giả: Nguyễn Hiếu Minh, Trịnh Xuân Thắng, Ngô Võ Kế Thành, Nguyễn Tuấn Khoa

Tóm tắt: Sáng chế đề cập đến phương pháp mã hoá, giải mã trên đường truyền từ máy chủ (server) đến thiết bị cổng kết nối (gateway) internet vạn vật (IOTs-internet ofthings) bao gồm các bước sau: i) Thiết lập kết nối giữa mô đun bảo mật với thiết bị cổng kết nối và máy chủ; ii) Xác nhận cho phép truyền nhận dữ liệu giữa máy chủ, thiết bị cổng kết nối, và thiết bị đầu cuối thông qua giao thức trao đổi khóa IKEv2 trong mô đun bảo mật; iii) Thực hiện mã hóa dữ liệu gói tin trước khi truyền đi hoặc tiến hành giải mã dữ liệu gói tin trước khi sử dụng thông qua giao thức ESP (Encapsulaton Secutity Payload) trong mô đun bảo mật.

- **Lõi IP (Intellectual Property core) thực hiện giải mã mật mã dùng hệ mật mã khóa công khai RSA (Rivest - Shamir - Adleman) và hệ mật mã dòng ZUC (ZuChongzi) trong truyền dữ liệu video**

Số đơn: VN 2-2014-00293

Ngày công bố đơn: 25/05/2016

Chủ đơn: Trường Đại học Khoa học Tự nhiên - Đại học Quốc gia TP.HCM - Sở Khoa học và Công nghệ TP.HCM

Tác giả: Nguyễn Đình Thúc, Nguyễn Văn Toàn, Nguyễn Đức Phúc, Huỳnh Hữu Thuận

Tóm tắt: Sáng chế đề cập đến thiết kế lõi IP thực hiện giải mã mật mã sử dụng hệ mật mã RSA và hệ mật mã dòng ZUC nhằm cung cấp giải pháp bảo mật cao cũng như tốc độ giải mã cao của tín hiệu video được mã hóa. Kiến trúc lõi IP này bao gồm 3 phần: bộ xử lí giải mã hệ mật mã dòng ZUC, bộ xử lí giải mã hệ mật mã khóa công khai RSA, và bộ điều khiển chung CONTROL UNIT. Bộ giải mã RSA đảm nhiệm việc thiết lập khóa (giải mã khóa bí mật và báo hiệu) cho bộ xử lí hệ mật mã dòng ZUC. Bộ xử lí mật mã dòng ZUC thực hiện việc giải mã dữ liệu video gốc bằng cách thực hiện phép XOR giữa khóa dòng được sinh ra và dữ liệu video đã mã hóa mật mã. Bộ điều khiển chung CONTROL UNIT thực hiện việc đọc/ghi dữ liệu từ/vào FIFO và thực hiện điều khiển hoạt động của bộ giải mã RSA, bộ giải mã ZUC, cũng như hoạt động

đổi khóa. Sáng chế này khai thác được ưu điểm của hệ mật mã khóa công khai và hệ mật mã dòng, nhằm nâng cao khả năng bảo mật và tốc độ giải mã dữ liệu. Sáng chế này cũng cho phép việc thay đổi khóa bí mật trong quá trình hoạt động nhằm tối đa hóa khả năng bảo mật. Ngoài ra, bộ xử lí mật mã dòng ZUC cũng được tối ưu độ trễ để nâng cao tần số hoạt động bằng bộ cộng Carry Save Adder (độ trễ của mỗi bộ cộng Carry Save Adder bằng độ trễ của bộ cộng toàn phần).

2.1.2 Quản lý Danh tính và Truy cập

- **Hệ thống xác thực yêu cầu đăng nhập các dịch vụ trực tuyến sử dụng thẻ thông minh**

Số đơn: VN 2-2024-00786

Ngày công bố đơn: 03/02/2025

Chủ đơn/Tác giả: Trần Tuấn Anh, Chu Văn Cường, Vũ Đức Mạnh

Tóm tắt: Giải pháp hữu ích đề cập đến hệ thống xác thực yêu cầu đăng nhập các dịch vụ trực tuyến không mật khẩu sử dụng thẻ thông minh, hệ thống bao gồm thẻ thông minh, máy khách dịch vụ trực tuyến, thiết bị di động và máy chủ xác thực, trong đó, thiết bị di động có chức năng truyền thông trường gần (NFC) và có hệ điều hành để chạy các ứng dụng. Hệ thống không cần sử dụng đầu đọc thẻ để kết nối với các ứng dụng trực tuyến trên máy tính cá nhân. Hệ thống hướng tới cung cấp một giải pháp đăng nhập các dịch vụ trực tuyến một cách tiện lợi do không cần phải ghi nhớ mật khẩu để đăng nhập vào từng dịch vụ trực tuyến khác nhau. Hệ thống xác thực đăng nhập thông qua chữ kí số được thực hiện trên thẻ thông minh với chi phí rẻ và độ bảo mật cao. Việc lược bỏ đi đầu đọc thẻ giúp giảm chi phí cho người dùng và giúp người dùng dễ dàng tiếp cận và sử dụng giải pháp được đề cập ở đây hơn so với các giải pháp khác hiện đang có trên thị trường.

- **Hệ thống quản lý và chia sẻ dữ liệu dùng chung mà tích hợp các nền tảng xử lý, phân tích dữ liệu lớn và phát triển mô hình học máy**

Số đơn: VN 2-2024-00210

Ngày công bố đơn: 25/06/2024

Chủ đơn: Viện Công nghệ thông tin - Viện Hàn lâm Khoa học và Công nghệ Việt Nam

Tác giả: ThS. Phùng Công Định, PGS.TS. Nguyễn Long Giang, TS. Võ Sỹ Nam, TS. Đinh Văn Dũng

Tóm tắt: Giải pháp hữu ích đề cập đến hệ thống quản lý và chia sẻ dữ liệu dùng chung mà tích hợp các nền tảng xử lý, phân tích dữ liệu lớn và phát triển học mô hình máy bao gồm: mô đun giao diện người dùng được tạo cấu hình để thực hiện định danh và xác thực người dùng điện tử, phân cấp truy cập và tạo cơ chế đăng nhập một lần cho người dùng; mô đun thu thập dữ liệu được tạo cấu hình để thu thập dữ liệu và tích hợp dữ liệu từ nhiều nguồn dữ liệu khác nhau, các nguồn dữ liệu bao gồm: tệp dữ liệu, cơ sở dữ liệu quan hệ, hệ thống phần mềm dạng dịch vụ, dữ liệu luồng từ các thiết bị truyền dữ liệu theo thời gian thực; mô đun lưu trữ trên nền tảng điện toán đám mây được tạo cấu hình để lưu trữ dữ liệu lớn sau khi được chuyển đổi từ mô đun thu thập dữ liệu; mô đun xử lý dữ liệu được tạo cấu hình để xử lý dữ liệu được lưu trữ trong mô đun lưu trữ hoặc xử lý dữ liệu luồng được thu thập trực tiếp, kết quả xử lý dữ liệu được lưu trữ trong mô đun lưu trữ phục vụ các tác vụ phân tích dữ liệu tiếp theo; mô đun phát triển mô hình học máy được tạo cấu hình để cung cấp các thư viện nền tảng hoặc môi trường cộng tác mà cho phép người dùng quản lý và thực thi quy trình phát triển mô hình học máy, bao gồm xây dựng mô hình, huấn luyện, kiểm thử và quản lý mô hình và tích hợp với các công cụ triển khai phần mềm. Hệ thống quản lý và chia sẻ dữ liệu dùng chung mà tích hợp các nền tảng xử lý, phân tích dữ liệu lớn và phát triển mô hình học máy đáp ứng được yêu cầu về xử lý dữ liệu lớn về các tài liệu khoa học cũng như đáp ứng đầy đủ các tiêu chí về tính chính xác, an toàn và bảo mật.

- **Phương pháp bảo mật dữ liệu cho các thiết bị camera sử dụng vi mạch tích hợp mô-đun nền tảng đáng tin cậy và thiết bị tạo khoá**

Số đơn: VN 1-2022-01989

Ngày công bố đơn: 25/10/2023

Chủ đơn: Công ty Cổ phần BKAV

Tác giả: Trần Việt Hải, Nguyễn Tử Quảng

Tóm tắt: Sáng chế đề xuất một phương pháp bảo mật dữ liệu giữa việc truyền và nhận dữ liệu từ camera và các máy tính "khách" muốn truy cập, bằng cách, sử dụng đồng thời vi mạch tích hợp bảo mật phần cứng TPM (Trusted Platform Module) trên thiết kế của camera và USB Token cắm vào máy tính "khách", USB Token được dùng để tạo ra một cặp khóa gồm Khóa riêng tư và Khóa công khai. Bằng cách chứng thực các khóa để cho phép kết nối giữa camera và các máy tính "khách". Sau đó, dữ liệu từ camera sẽ được truyền đi dưới dạng mã hóa dựa vào vi mạch tích hợp TPM. Máy tính sẽ mở được khóa và giải mã dữ liệu video được gửi từ camera bằng chức năng của USB Token.

2.1.3 Bảo mật Dữ liệu

- **Hệ thống và phương pháp chống giả mạo mã QR ứng dụng công nghệ trí tuệ nhân tạo**

Số đơn: VN 1-2024-01427

Ngày công bố đơn: 25/07/2024

Chủ đơn: Trường Đại học Cần Thơ

Tác giả: Lê Hoàng Thảo, Cù Vĩnh Lộc, Trần Hoàng Việt, Nguyễn Hoàng Việt, Trương Xuân Việt

Tóm tắt: Hệ thống chống giả mạo mã QR ứng dụng công nghệ trí tuệ nhân tạo bao gồm mô-đun tạo mã QR (110), mô-đun tạo thông tin bảo mật (120), mô-đun bộ nhớ (130), mô-đun ẩn thông tin bảo mật (140), mô-đun sản xuất (150), mô-đun trích xuất thông tin ẩn (160), mô-đun ước lượng độ tương đồng (170), mô-đun xác thực (180). Ngoài ra, sáng chế còn cung cấp một phương pháp chống giả mạo mã QR ứng dụng công nghệ trí tuệ nhân tạo gồm các bước sau: i) tạo mã QR gốc; ii) lưu trữ mã QR gốc; iii) tạo thông tin bảo mật; iv) tạo mã QR thuỷ vân số có chứa thông tin bảo mật; v) quét mã QR trên sản phẩm/hàng hoá nhờ các thiết bị thông minh; vi) so sánh thông tin ẩn trong mã QR thuỷ vân số đã được trích xuất ở bước v); vii) ước lượng độ tương đồng giữa mã QR thuỷ vân số và mã QR gốc được lưu trữ ở bước ii); viii) xác định mã QR trên sản phẩm/hàng hoá bằng việc sử dụng kết quả thu được ở bước vi) và bước vii) để đưa ra kết luận mã QR thật hay giả.

- **Hệ thống sách điện tử dưới dạng NFT kết hợp chip bảo mật RFID**

Số đơn: VN 1-2024-00665

Ngày công bố đơn: 25/07/2024

Chủ đơn: Công ty Cổ phần Phygital Labs

Tác giả: Nguyễn Tuấn Minh, Nguyễn Huy, Đỗ Hoài Nam, Đinh Đức Hoàng

Tóm tắt: Sáng chế đề cập đến hệ thống sách điện tử dưới dạng NFT kết hợp chip bảo mật RFID. Hệ thống chuỗi khối tạo ra mỗi NFT ứng với mỗi sản phẩm sách vật lý; và lưu trữ liên kết dữ liệu giữa khóa công khai (public key), mã định danh chip (chip ID) của chip RFID và NFT. Người dùng sẽ sử dụng điện thoại để scan vào chip, sau đó điện thoại sẽ gửi yêu cầu tới hệ thống bảo mật để kiểm tra tính xác thực của con chip, nếu hợp lệ thì trả về người dùng nội dung sách trên nền tảng trình duyệt web. Chip RFID áp dụng công nghệ bảo mật bất đối xứng (asymmetric key), nội dung mỗi lần scan đều

được mã hóa, giúp con chip không thể bị làm giả, đảm bảo sự tồn tại độc bản duy nhất của chip và tạo ra mối liên kết 1-1 duy nhất tới tài sản vật lý. Giải pháp nhằm số hóa sách không chỉ giúp trình bày nội dung sách một cách sinh động, đẹp mắt, mà còn tích hợp những tính năng sản phẩm vật lý không có được như video, audio, cùng các tính năng tùy chọn thuận tiện như: tự động phân số trang sách dựa trên kích thước thật của thiết bị sử dụng, cho phép chỉnh sửa độ lớn của chữ, cho phép chỉnh sửa màu sắc của chữ và màu nền, mở sách chỉ bằng thao tác scan chip, ghi nhớ và mở lại trang sách đọc lần cuối, ghi chú và đánh dấu trên nội dung đọc.

- **Phương pháp nhận diện và quản lý dữ liệu chứa nội dung nhạy cảm**

Số đơn: VN 1-2021-08261

Ngày công bố đơn: 26/06/2023

Chủ đơn: Công ty Cổ phần BKAV

Tác giả: Vũ Ngọc Sơn, Nguyễn Tử Quảng

Tóm tắt: Sáng chế đề xuất phương pháp nhận diện và quản lý dữ liệu có nội dung nhạy cảm giải quyết được hạn chế của phương pháp nhận diện thủ công và lưu trữ dữ liệu truyền thống trước đó bằng cách xác định để cảnh báo và lưu trữ dữ liệu một các bảo mật hơn. Giải pháp này giúp những người dùng thiết bị thông minh nâng cao ý thức cảnh giác, nhận định được chính xác các dữ liệu quan trọng, những hậu quả của việc mất dữ liệu mang lại và cung cấp nơi lưu trữ dữ liệu an toàn.

2.1.4 Bảo mật Ứng dụng

- **Hệ thống chuyển mạch dựa trên OpenFlow sử dụng phần cứng tái cấu hình**

Số bằng: VN2-0003177-000

Ngày cấp bằng: 19/05/2023

Chủ bằng: Trường Đại học Bách khoa - Đại học Quốc gia TP.HCM

Tác giả: Ngô Đức Minh, Trần Ngọc Thịnh

Tóm tắt: Giải pháp hữu ích đề cập đến hệ thống chuyển mạch dựa trên OpenFlow có khả năng ngăn chặn tấn công từ chối dịch vụ phân tán trong môi trường mạng tốc độ cao được thiết kế dựa trên phần cứng tái cấu hình. Hệ thống cho phép quản lý các phiên kết nối TGP dựa trên giao thức luồng mở (OpenFlow protocol) và có khả năng phát hiện, phát sinh cảnh báo tấn công mạng. Thêm vào đó, hệ thống hoạt động tách bạch giữa đường dữ liệu với đường điều khiển, giữa đường chuyển mạch và

đường bảo mật, có áp dụng linh hoạt các phương pháp khác nhau để đưa ra phương pháp tối ưu và hoạt động linh hoạt ở tốc độ cao.

- **Thiết bị USB an toàn dùng để lưu trữ dữ liệu an toàn, hạn chế lây lan vi rút**

Số bằng: VN1-0016526-000

Ngày cấp bằng: 24/01/2017

Chủ bằng: Viện Khoa học và Công nghệ Quân sự

Tác giả: Trần Xuân Kiên, Phạm Xuân Bảo

Tóm tắt: Sáng chế đề cập đến thiết bị lưu trữ USB để lưu trữ dữ liệu an toàn bao gồm vùng nhớ flash, trong đó vùng nhớ flash được chia làm ba phân vùng: phân vùng thứ nhất được cấu trúc thành dạng CDROM ảo (Read-Only Memory) chứa phần mềm quản lý chuyên dụng; phân vùng thứ hai chứa mật khẩu bảo mật; và phân vùng thứ ba có định dạng phi chuẩn để lưu trữ dữ liệu, phân vùng thứ ba này ẩn trong hệ điều hành hay nói cách khác là hệ điều hành không truy cập được dữ liệu. Khi kết nối thiết bị lưu trữ USB vào máy tính, hệ điều hành tự động nhận được phần phân vùng thứ nhất và tự động chạy chương trình quản lý chuyên dụng được lưu trên phân vùng này, tiếp theo phần mềm chuyên dụng sẽ xác thực mật khẩu người dùng, nếu đúng phần mềm sẽ truy xuất vào vùng thứ hai chứa mật khẩu bảo mật để lấy mã khóa truy nhập cho phép nhận dạng hệ thống tệp tin lưu trong phân vùng thứ ba có định dạng phi chuẩn và thực hiện các thao tác đọc/ghi.

2.1.5 Bảo mật Thiết bị đầu cuối

- **Phương pháp và hệ thống để đánh giá bảo mật**

Số đơn: VN 1-2021-07145

Ngày công bố đơn: 25/05/2023

Chủ đơn: Công ty Cổ phần Nghiên cứu và Ứng dụng Trí tuệ nhân tạo VinAI

Tác giả: Phùng Thị Quỳnh, Trần Tuấn Anh, Nguyễn Tuấn Anh

Tóm tắt: Sáng chế đề cập đến phương pháp và hệ thống để đánh giá bảo mật. Phương pháp này bao gồm các bước: mô phỏng, bởi bộ mô phỏng, cuộc tấn công cửa sau dựa trên màu sắc, trong đó các kích hoạt cửa sau được tạo ra dựa vào tông màu; đánh giá, bởi môđun đánh giá, bảo mật và đưa ra cảnh báo về nguy cơ của cuộc tấn công cửa sau dựa vào kết quả đánh giá; và làm giảm nhẹ, bởi môđun phòng thủ, cuộc tấn công cửa sau dựa trên màu sắc bằng cách thu nhỏ độ sâu màu sắc.

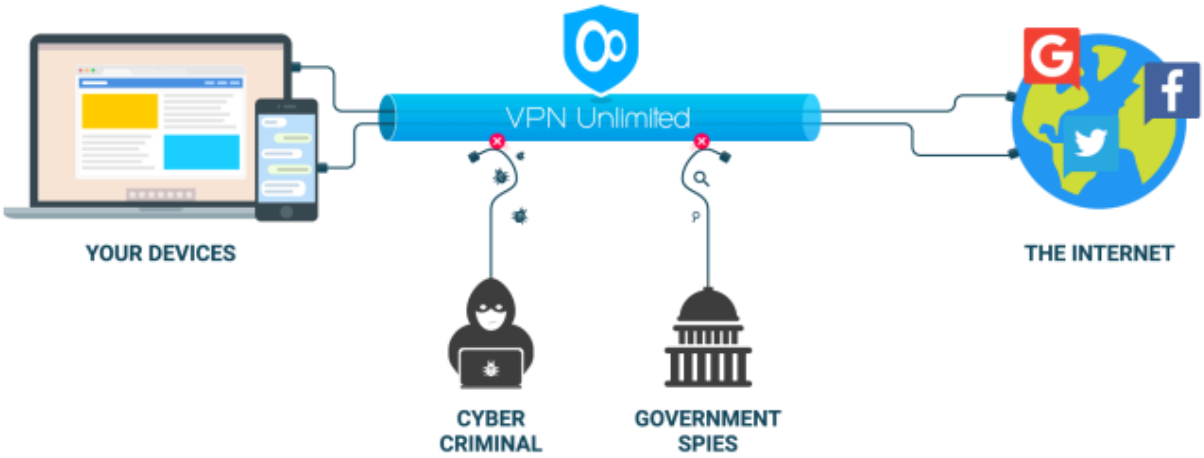
2.2 Một số kết quả nghiên cứu công nghệ an ninh mạng trong nước

2.2.1 Nghiên cứu, thiết kế, chế tạo thiết bị định tuyến (router) tốc độ cao, bảo mật an toàn thông tin

Tác giả: PGS.TS. Hoàng Trang - Giảng viên cao cấp Khoa Điện-Điện tử, Trưởng phòng Khảo thí - Bảo đảm chất lượng, Trường ĐH Bách khoa (Đại học Quốc gia TP.HCM)

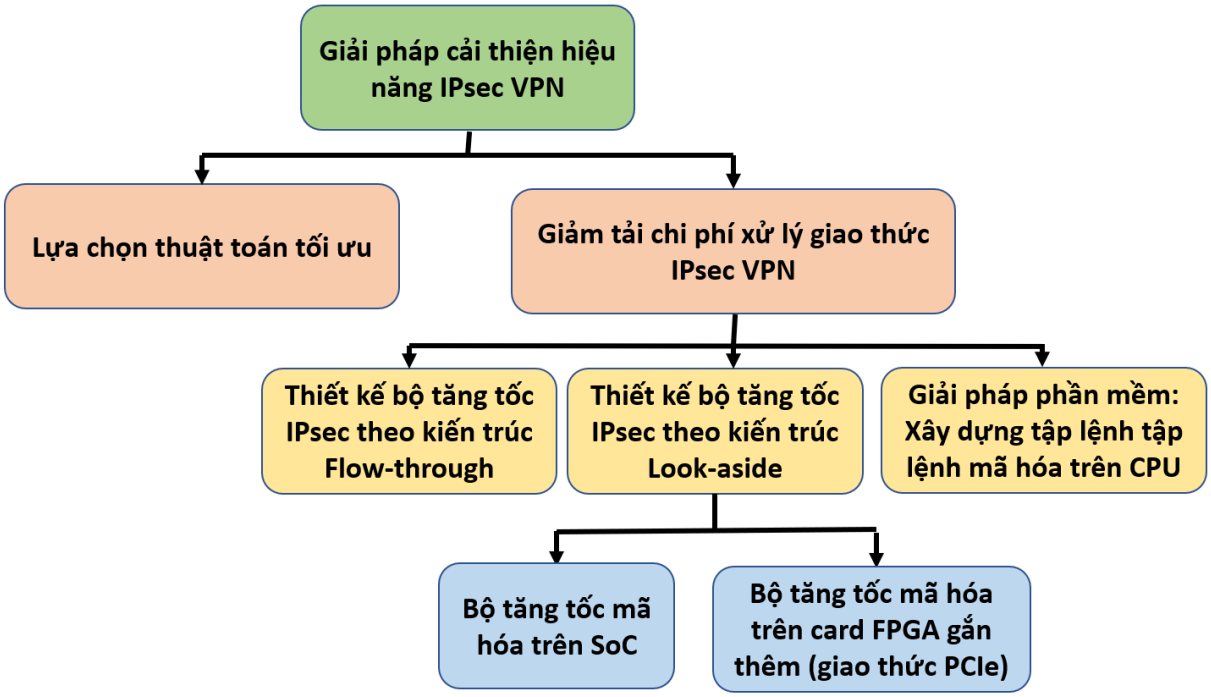
Nguồn gốc công nghệ: là kết quả nghiên cứu từ nhiệm vụ KH&CN cấp Quốc gia được nghiệm thu vào năm 2020, "*Nghiên cứu thiết kế chế tạo thử nghiệm thiết bị định tuyến tích hợp đa dịch vụ có tính năng bảo đảm an toàn bảo mật thông tin*" do PGS.TS. Hoàng Trang làm chủ nhiệm nhiệm vụ, nhóm nghiên cứu tại Trường ĐH Bách khoa (Đại học Quốc gia TP.HCM) cùng tham gia thực hiện.

Nội dung: Hiện nay, các thiết bị Router gia đình và doanh nghiệp nhỏ đang tồn tại nhiều lỗ hổng nghiêm trọng về an toàn thông tin, cụ thể như sau: Phần lớn Router sử dụng hệ điều hành Linux phiên bản cũ, đã ngừng được hỗ trợ và cập nhật bảo mật từ năm 2011, tiềm ẩn nhiều nguy cơ bị khai thác. Mật khẩu quản trị bị thiết lập cố định (hardcoded) trong firmware hoặc giao diện quản trị không hỗ trợ giao thức HTTPS, dẫn đến nguy cơ lộ thông tin xác thực. Hệ thống tường lửa đơn giản, thiếu các cơ chế phát hiện và phòng chống tấn công từ chối dịch vụ (DoS/DDoS). Không hỗ trợ VPN hoặc khả năng xử lý VPN rất hạn chế do giới hạn phần cứng, gây suy giảm hiệu năng khi mã hóa lưu lượng. Những hạn chế trên khiến Router trở thành điểm yếu trong hạ tầng mạng, đặc biệt trong bối cảnh yêu cầu bảo mật và kết nối an toàn ngày càng gia tăng.



Hình 2.1 Thực trạng lỗ hổng bảo mật đối với các thiết bị Router gia đình và doanh nghiệp nhỏ

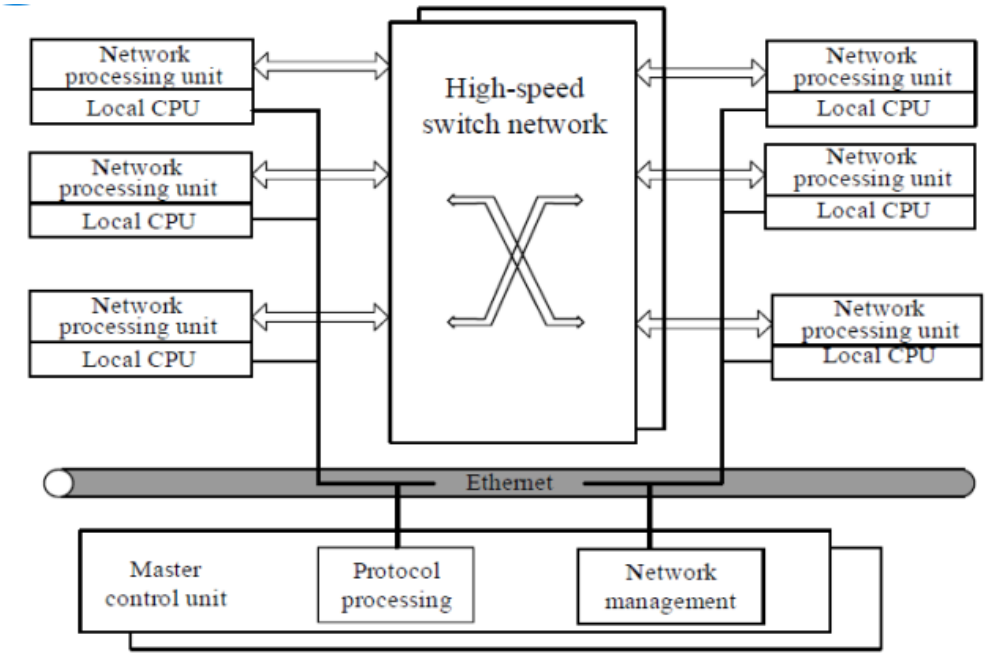
Giải pháp nhóm nghiên cứu đề xuất: Xây dựng lại toàn bộ phần mềm dựa trên mã nguồn mở, làm chủ công nghệ cốt lõi và không phụ thuộc vào các thư viện đóng; Thiết kế phần cứng chuyên dụng, tích hợp card tăng tốc FPGA để hỗ trợ mã hóa VPN theo kiến trúc Look-aside, giúp nâng cao hiệu năng xử lý; và Phát triển firmware BKRouter với các tính năng bảo mật nâng cao như hỗ trợ HTTPS, lưu trữ mật khẩu dưới dạng hash và tích hợp cơ chế phòng chống tấn công DDoS.



Hình 2.2 Giải pháp cải thiện hiệu năng Ipsec VPN

Về thiết kế phần cứng, bao gồm: Vi xử lý trung tâm (SoC): Sử dụng Marvell Cortex-A9 (kiến trúc ARMv7), đáp ứng yêu cầu xử lý mạng tốc độ cao; Card tăng tốc FPGA: Kết nối với SoC thông qua giao tiếp PCIe, đảm nhiệm xử lý mã hóa/giải mã AES-GCM, giúp giảm tải cho CPU và nâng cao hiệu năng VPN; Hệ thống cổng kết nối: 04 cổng Gigabit Ethernet (WAN/LAN), 01 cổng SFP, cổng quản lý RS232 và USB phục vụ cấu hình và mở rộng.

Về thiết kế phần mềm, bao gồm: Hệ điều hành: Dựa trên Linux Kernel phiên bản 4.14.176; Chức năng tích hợp: WiFi Access Point, Firewall (fw3), VPN (StrongSwan & OpenVPN), VoIP, QoS, Routing; Cơ chế Driver: Gồm lớp OS-Specific (giao tiếp với nhân Linux) và Device-Specific (điều khiển trực tiếp khối mã hóa trên FPGA qua DMA/PCIe)



Hình 2.3 Kiến trúc tổng quát của Router

Kết quả thử nghiệm và đánh giá:

- Thông số kỹ thuật chính (so sánh với Cisco ISR 2901) đạt 2 Gbps, vượt yêu cầu thiết kế;

- Số kết nối VPN đồng thời: 2.137 kết nối, vượt trội so với các thiết bị cùng phân khúc;

- Thông lượng VPN (IPSec): đạt khoảng 360-370 Mbps khi sử dụng FPGA tăng tốc, cao hơn đáng kể so với các sản phẩm phổ biến như Asus, Draytek hoặc Buffalo;

- Tính năng an toàn thông tin - Bảo mật kênh truyền: Hỗ trợ đầy đủ các thuật toán mã hóa và xác thực như DES, 3DES, AES, RSA và Diffie-Hellman;

- Khả năng chống tấn công: Tích hợp cơ chế phát hiện và phòng chống xâm nhập theo thời gian thực, chống DDoS và chặn lọc các dịch vụ P2P không mong muốn.

- Hiệu năng chống DDoS: Khi chịu tấn công với lưu lượng 200 Mbps, mức sử dụng CPU của BKRouter chỉ khoảng 70%, trong khi các Router thông thường (ví dụ Asus) gần như bị quá tải ở mức 100%.

Kết quả thử nghiệm và đánh giá cho thấy thiết bị router nghiên cứu đạt hiệu năng cao, khả năng chống tấn công DDoS tốt, thông lượng VPN vượt trội so với nhiều sản phẩm thương mại cùng phân khúc, đồng thời đáp ứng các tiêu chuẩn kỹ thuật, đo kiểm phát xạ điện từ theo quy định hiện hành. Nghiên cứu góp phần làm chủ công nghệ router bảo mật, tạo nền tảng cho việc phát triển các thiết bị mạng an toàn phục vụ cơ quan nhà nước và các hệ thống thông tin quan trọng.

2.2.2 Vấn đề phát hiện tấn công có chủ đích (APT) sử dụng trí tuệ nhân tạo

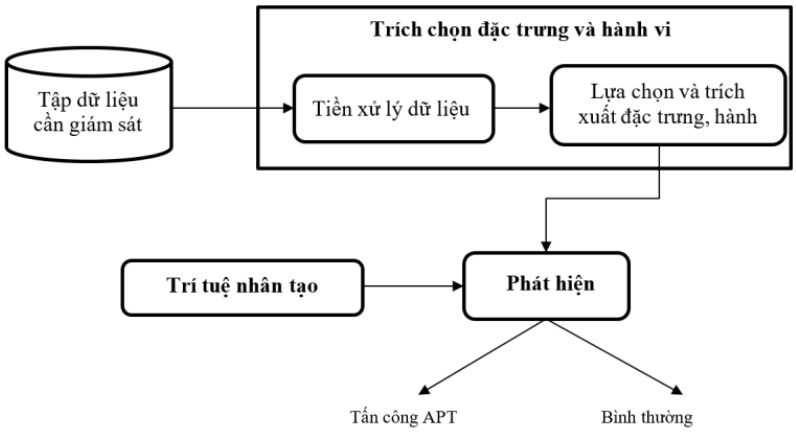
Tác giả: PGS.TS. Đỗ Xuân Chợ - Học viện Công nghệ Bưu chính Viễn thông.

Nguồn gốc công nghệ: là kết quả nghiên cứu từ nhiệm vụ KH&CN cấp Bộ được nghiệm thu cuối năm 2024, "*Nghiên cứu và xây dựng ứng dụng phát hiện tấn công có chủ đích (APT) dựa trên phân tích kết nối bất thường sử dụng trí tuệ nhân tạo*" do PGS.TS. Đỗ Xuân Chợ làm chủ nhiệm nhiệm vụ, nhóm nghiên cứu tại Học viện Công nghệ Bưu chính Viễn thông (Bộ KH&CN) cùng tham gia thực hiện.

Nội dung: Các nguy cơ mất an toàn thông tin cho hệ thống ngày càng tăng nhanh về số lượng và mức độ nguy hiểm. Một số kỹ thuật bao gồm: Tấn công bằng mã độc; tấn công DOS, DDOS, Tấn công lừa đảo, tấn công APT. Đối tượng và phạm vi tán công của APT ngày càng mở rộng và hầu hết các tổ chức chính phủ, các cơ quan trọng yếu đều có thể là nạn nhân của các chiến dịch APT. Nhiều tài liệu quan trọng đã bị đánh cắp, gây thiệt hại lớn về tài sản và uy tín cho tổ chức. Tấn công có chủ đích (APT) là một trong những dạng tấn công mạng nguy hiểm nhất hiện nay bởi tính âm thầm, kéo dài và có chủ đích rõ ràng. Do đó, để giải quyết vấn đề, nhóm nghiên cứu đã đề xuất tiếp cận theo 2 hướng:

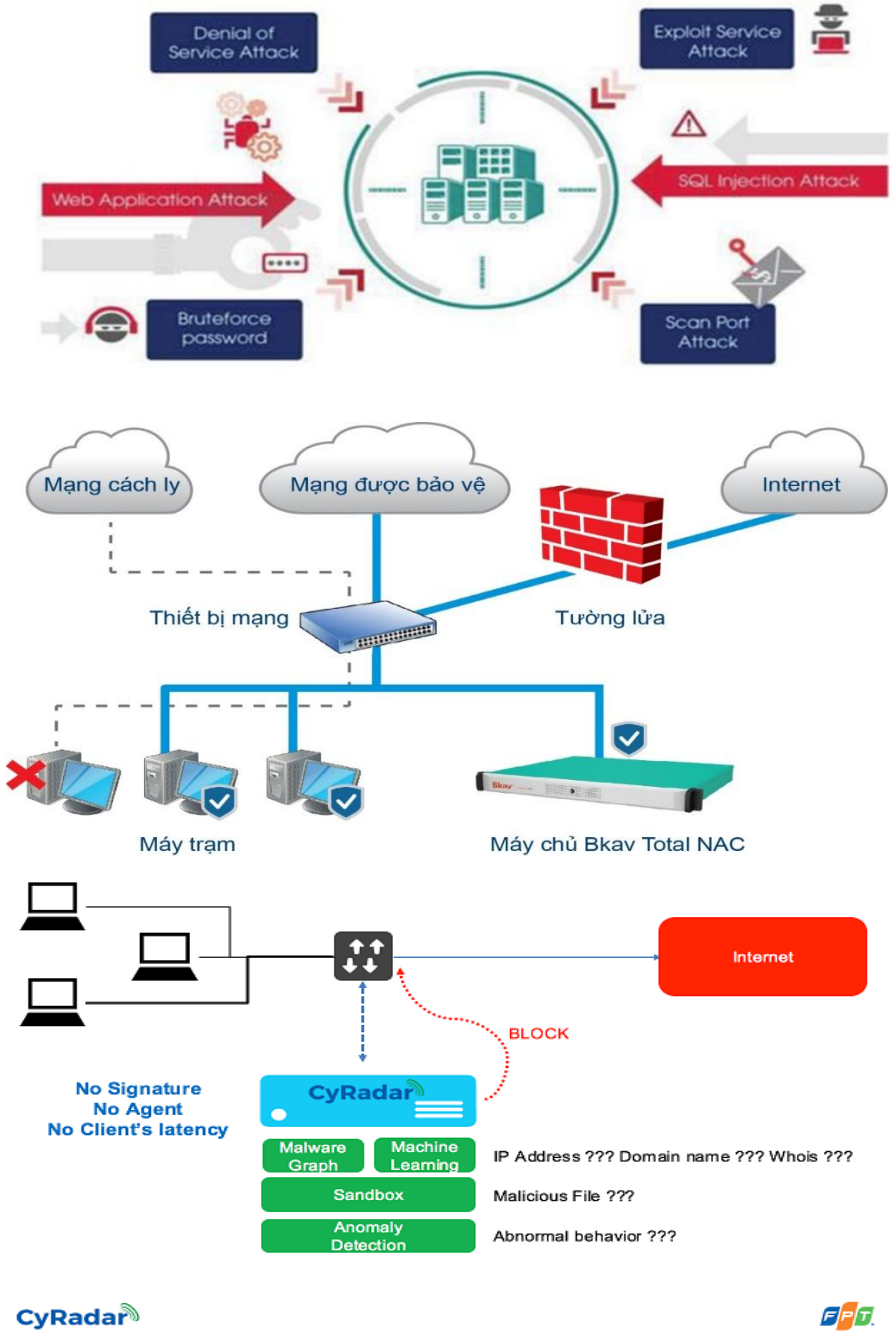
- Hướng tiếp cận 1: Phát hiện bất thường dựa trên giám sát các hành vi trên máy người dùng: Theo đó, các nghiên cứu theo hướng tiếp cận này thường tập trung vào việc thu thập các tiến trình, hành vi trên máy người dùng, thiết bị đầu cuối rồi từ đó phân tích và đưa ra cảnh báo. Có 2 phương pháp chính để phát hiện các hành vi này là Phát hiện dựa trên tập dấu hiệu và Phát hiện dựa trên kỹ thuật phân tích hành vi.

- Hướng tiếp cận 2: Phát hiện bất thường dựa trên quá trình theo dõi và giám sát lưu lượng mạng: Theo đó, dựa trên việc thu thập và phân tích các dữ liệu về lưu lượng mạng thì các hệ thống giám sát sẽ đưa ra các cảnh báo về hành vi bất thường.



Hình 2.4 Phát hiện bất thường dựa trên giám sát các hành vi

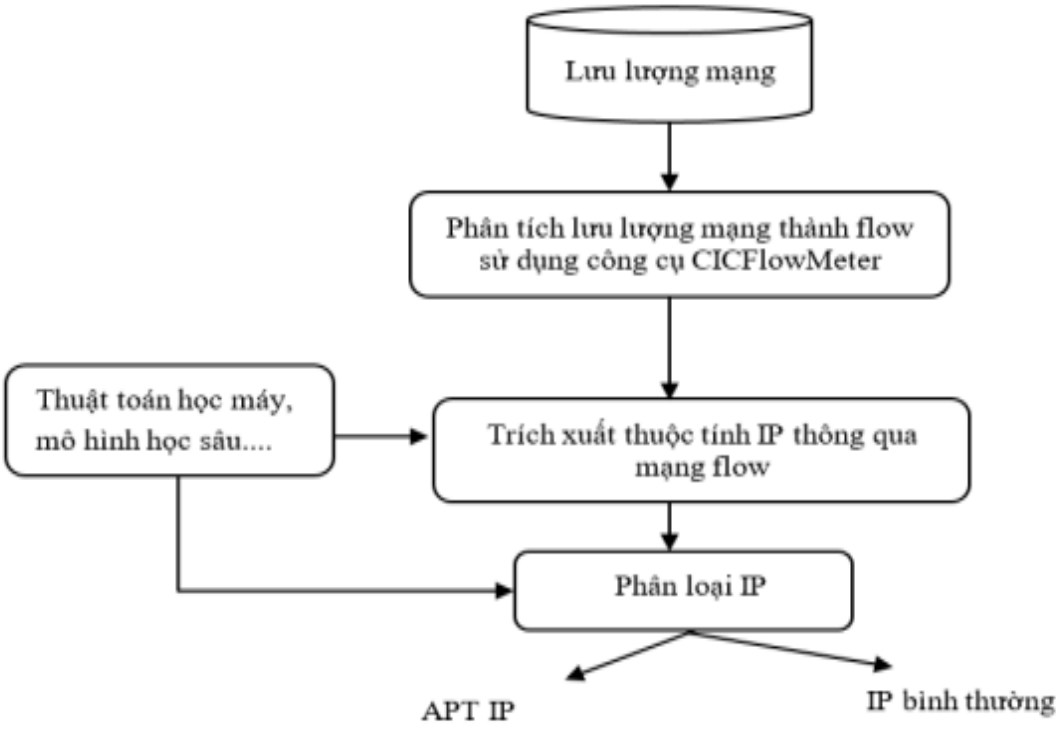
Có 4 bộ giải pháp chính phát hiện tấn công APT: (1) Giải pháp ngăn chặn tại giai đoạn lan truyền mã độc; (2) Giải pháp phát hiện mã độc APT phát tán; (3) Giải pháp ngăn ngừa rò rỉ dữ liệu; (4) Giải pháp truy vết.



Hình 2.5 Các giải pháp phát hiện tấn công APT, lần lượt của: Viettel, Bkav và FPT

Các hướng tiếp cận hiện nay trong phát hiện APT, gồm phát hiện dựa trên hành vi tại thiết bị đầu cuối và phát hiện dựa trên giám sát lưu lượng mạng. Trên cơ sở đó, nhóm nghiên cứu đưa ra đề xuất giải pháp phát hiện APT dựa trên phân tích kết nối mạng bất thường kết hợp trí tuệ nhân tạo, nhằm khắc phục hạn chế của các phương pháp

truyền thống. Giải pháp nghiên cứu được xây dựng theo quy trình gồm ba bước chính: (1) Phân tích lưu lượng mạng thành các luồng (flow) và trích xuất đặc trưng hành vi; (2) Trích xuất đặc trưng IP dựa trên các luồng mạng; (3) Phân loại IP tấn công APT và IP bình thường bằng các thuật toán học máy và học sâu.



Hình 2.6 Giải pháp phát hiện tấn công APT dựa trên trí tuệ nhân tạo được đề xuất

Nghiên cứu đã tiến hành thực nghiệm và đánh giá trên bộ dữ liệu lớn, bao gồm hơn 1,6 triệu luồng mạng và dữ liệu từ nhiều chiến dịch APT điển hình. Kết quả thực nghiệm cho thấy giải pháp có hiệu quả cao trong việc phát hiện các kết nối bất thường và IP tấn công APT, góp phần nâng cao năng lực giám sát an toàn thông tin mạng.

Trên cơ sở kết quả đạt được, nhóm nghiên cứu đưa ra khuyến nghị đối với cơ quan quản lý nhà nước về việc ứng dụng kết quả nghiên cứu vào việc hỗ trợ đảm bảo an toàn thông tin cho cơ quan nhà nước trong việc phòng chống tấn công mạng, tấn công APT, Botnet. Sử dụng kết quả của đề tài làm tài liệu hướng dẫn đào tạo, giúp nâng cao nhận thức về an toàn thông tin cho các nhân viên, người dùng trong tổ chức. Sử dụng kết quả nghiên cứu của đề tài như công cụ hướng dẫn đảm bảo an toàn thông tin cho cơ quan tổ chức. Cụ thể, bộ giải pháp trong đề tài có thể được sử dụng để xác định các nguy cơ điểm yếu và các nguy cơ mất an toàn thông tin đến các dịch vụ chính phủ điện tử

2.2.3 AI-Security - Từ bảo mật cơ sở dữ liệu đến bảo mật riêng tư trong học máy

Tác giả: PGS.TS. Nguyễn Đình Thúc - Trưởng Bộ môn Công nghệ tri thức, Trường ĐH Khoa học Tự nhiên (Đại học Quốc gia TP.HCM)

Nguồn gốc công nghệ: là kết quả từ nghiên cứu "*AI-SECURITY - Form database security to machine learning privacy*" do PGS.TS. Nguyễn Đình Thúc thực hiện chính.

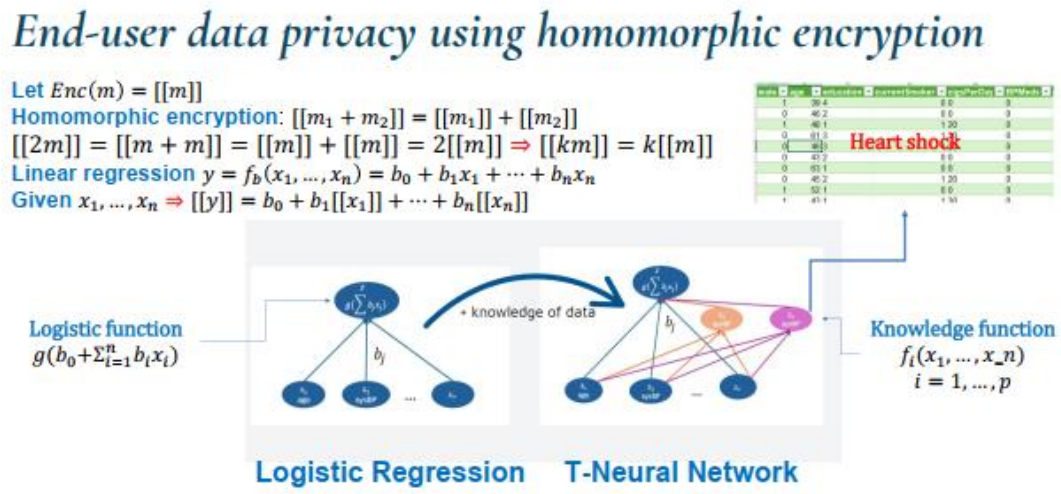
Nội dung: Hiện nay, các vấn đề an ninh và bảo mật trong hệ thống thông tin công cộng, với trọng tâm là bảo mật cơ sở dữ liệu và quyền riêng tư trong học máy, trong bối cảnh các hệ thống thông minh và dịch vụ công ngày càng phụ thuộc vào dữ liệu và trí tuệ nhân tạo. Các hệ thống thông tin, bao gồm cả hệ thống thông minh, hoạt động nhờ dữ liệu luân chuyển trong hệ thống từ và đến người dùng. Có thể xem dữ liệu như *"máu"* mang chất liệu cho các thành phần hệ thống hoạt động, và cơ sở dữ liệu (CSDL) chính là *"trái tim"* cung cấp máu cho toàn bộ hệ thống. Bảo mật CSDL vì thế là khía cạnh quan trọng cần xem xét cẩn trọng khi triển khai các hệ thống vào thực tế.

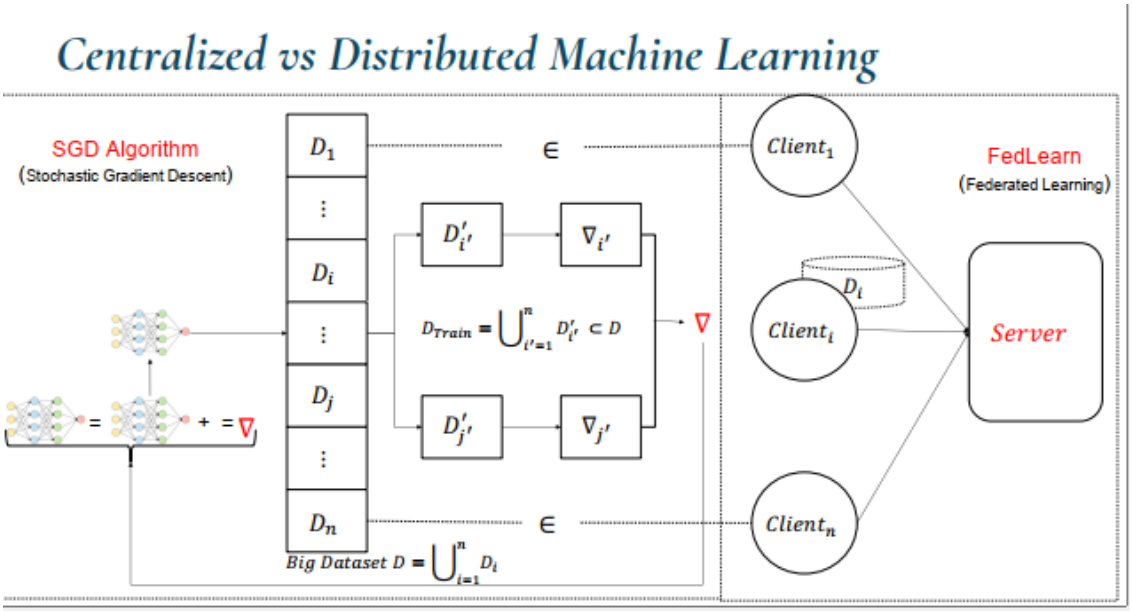
Các CSDL, tập hợp các dữ liệu có cấu trúc cho mục đích chính là tìm kiếm; trong khi đó, mật mã với mục đích chính là mã hóa dữ liệu sao cho không thể tìm kiếm nếu không có quyền truy xuất và đọc dữ liệu. Vì thế, bên cạnh các cơ chế và công cụ kiểm soát truy cập có sẵn để thiết lập *"hàng rào"* bảo vệ hệ thống an toàn, cần những phương pháp mật mã thích hợp được xây dựng dựa trên các thành tố mật mã có sẵn để bảo mật nội dung để ngay cả khi hệ thống có bị khống chế thì dữ liệu nhạy cảm cũng không bị rò rỉ.

Các hệ thống thông minh nhân tạo *"thông minh"* là nhờ khả năng *"học"* các *"kiến thức"* từ những gì đã xảy ra được tập hợp như các CSDL. *"Kiến thức"* càng *"đúng"* nếu nguồn dữ liệu cung cấp cho việc *"huấn luyện"* hệ thống càng đa dạng. Thách thức ở chỗ rất khó để một đơn vị có thể tập hợp được "đủ" dữ liệu cho huấn luyện mô hình, đặc biệt khi dữ liệu là giá trị, là *"tài sản"* của đơn vị. Giải pháp là *"góp"* dữ liệu của các đơn vị để huấn luyện mô hình chung. Để các đơn vị hoạt động trong cùng lãnh vực có thể chia sẻ *"dữ liệu tài sản"* của mình, cần nhưng phương pháp đảm bảo tính riêng tư dữ liệu để mọi đơn vị tham gia đều có mô hình mạnh nhưng dữ liệu vẫn thuộc riêng của từng đơn vị.

Để bảo vệ quyền riêng tư dữ liệu người dùng trong học máy, đặc biệt là trong các mô hình học phân tán và học liên kết (Federated Learning) cần xác định các nguy cơ tấn công vào quyền riêng tư như membership inference attack, cũng như các thách thức trong việc bảo vệ dữ liệu khi huấn luyện mô hình trên dữ liệu phân tán.

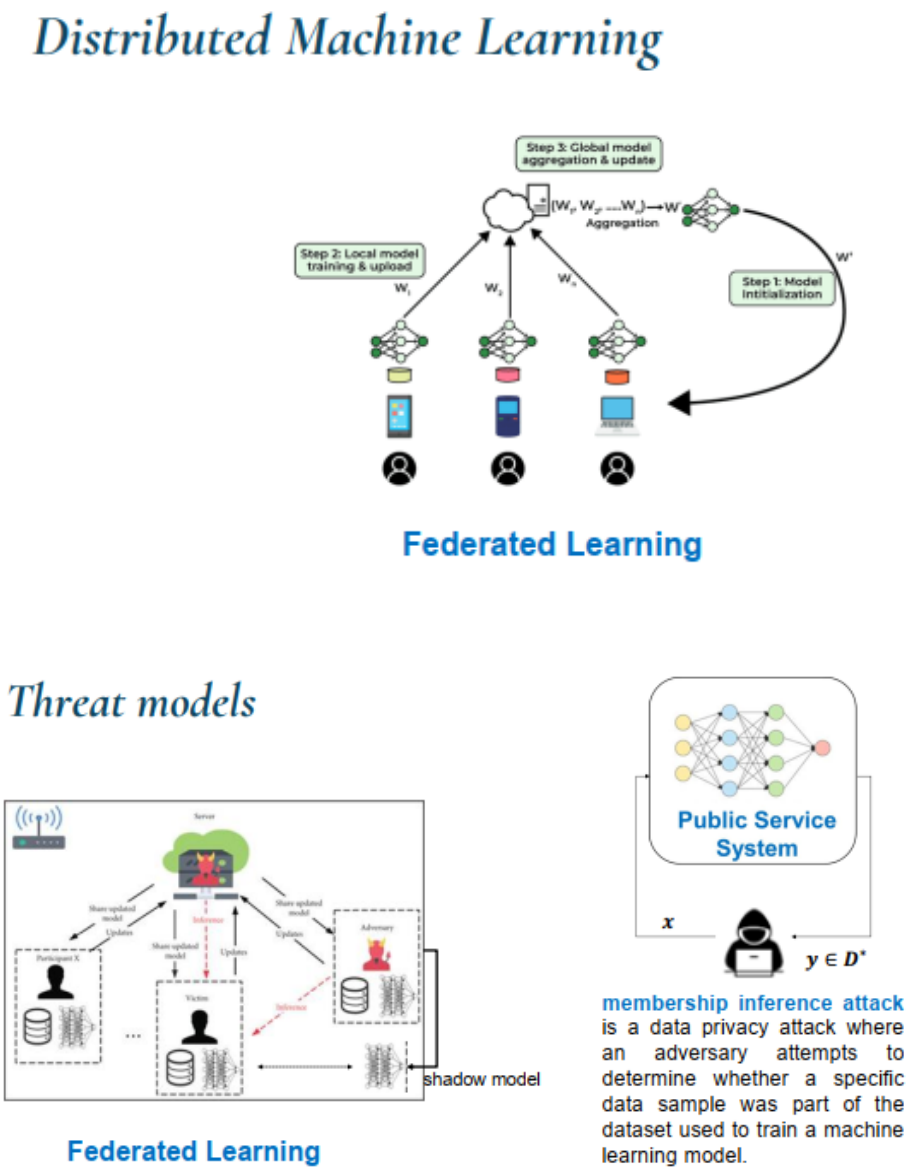
Một số giải pháp bảo mật và bảo vệ quyền riêng tư, bao gồm học liên kết an toàn, mã hóa đồng cấu trong học máy, mô hình máy chủ hai tầng và các kỹ thuật unlearning nhằm loại bỏ ảnh hưởng của dữ liệu không mong muốn khỏi mô hình học. Các giải pháp này góp phần nâng cao mức độ an toàn và tin cậy của hệ thống trí tuệ nhân tạo trong môi trường thực tế.





Hình 2.7. Các thuật toán học máy được sử dụng trong nghiên cứu

Chuyên gia khẳng định tầm quan trọng của việc kết hợp bảo mật dữ liệu truyền thống với các kỹ thuật bảo vệ quyền riêng tư trong học máy, coi đây là xu hướng tất yếu nhằm đảm bảo an toàn thông tin cho các hệ thống thông tin công và ứng dụng AI trong thời gian tới.



Hình 2.8. Các giải pháp bảo mật và bảo vệ quyền riêng tư trong CSDL trong học máy

2.2.4 Camera do thám và hiểm họa lộ lọt thông tin

Tác giả: TS. Võ Văn Khang - Viện trưởng Viện Ứng dụng Công nghệ mới.

Nguồn gốc công nghệ: là kết quả nghiên cứu từ nhiệm vụ KH&CN cấp Tỉnh/Thành phố được nghiệm thu vào năm 2022 "*Nghiên cứu đánh giá hiện trạng về bảo mật thông tin cho hệ thống các thiết bị Camera thông dụng có kết nối Internet tại Thành Phố Hồ Chí Minh*" do TS. Võ Văn Khang làm chủ nhiệm nhiệm vụ, nhóm nghiên cứu tại Trung tâm An ninh mạng TP.HCM cùng tham gia thực hiện.

Nội dung: Hiện nay, nguy cơ mất an toàn thông tin xuất phát từ các thiết bị camera do thám và thiết bị gián điệp công nghệ cao đang trở thành một vấn đề nổi cộm, đặc biệt trong bối cảnh chuyển đổi số mạnh mẽ và sự phổ cập rộng rãi của các thiết bị IoT. Các thiết bị do thám hiện đại ngày càng có kích thước siêu nhỏ, hoạt động âm thầm và có khả năng ẩn mình ngay trong hạ tầng mạng của tổ chức mà rất khó bị phát hiện. Cụ thể, camera ngụy trang (Hidden Cameras) được tích hợp tinh vi vào các vật dụng quen thuộc như đầu báo cháy, ổ cắm điện, đồng hồ treo tường hoặc đồ gia dụng. Thiết bị nghe lén (Audio Bugs) sử dụng các module thu âm siêu nhỏ, có khả năng truyền dữ liệu qua sóng GSM hoặc Wi-Fi. Bên cạnh đó, trong mạng nội bộ còn tồn tại các thiết bị "rogue" – là những thiết bị lạ tự ý kết nối vào hệ thống Wi-Fi nội bộ nhằm thu thập và gửi dữ liệu ra bên ngoài mà không được sự cho phép của quản trị hệ thống.

Thực trạng này ngày càng đáng báo động khi các thiết bị camera ngụy trang, thiết bị nghe lén và thiết bị "rogue" trở nên tinh vi hơn, khó phát hiện hơn và có khả năng xâm nhập trực tiếp vào không gian riêng tư, phòng họp, khu vực nhạy cảm của cơ quan, doanh nghiệp và cả hộ gia đình. Nhiều vụ việc nghiêm trọng đã được ghi nhận cả ở nước ngoài và tại Việt Nam. Không chỉ các camera quay lén bất hợp pháp, mà ngay cả các hệ thống camera giám sát hợp pháp cũng tiềm ẩn nguy cơ bị chiếm quyền điều khiển do tồn tại lỗ hổng bảo mật hoặc backdoor.

Trên thế giới, đã xảy ra nhiều sự kiện điển hình như vụ việc hơn 1.600 khách lưu trú tại nhà nghỉ ở Hàn Quốc bị quay lén và phát trực tiếp trên Internet, hay việc phát hiện các thiết bị giám sát ẩn trong phích cắm sạc, chậu hoa tại Trung Quốc. Tại Việt Nam, thị trường "chợ đen" rao bán camera ngụy trang siêu nhỏ diễn ra công khai, khó kiểm soát. Ước tính có hơn 800.000 camera giám sát đang hoạt động có nguy cơ bị lộ thông tin và dễ bị hacker chiếm quyền điều khiển, đặc biệt là các dòng camera giá rẻ, trôi nổi, tồn tại nhiều lỗ hổng bảo mật và backdoor.

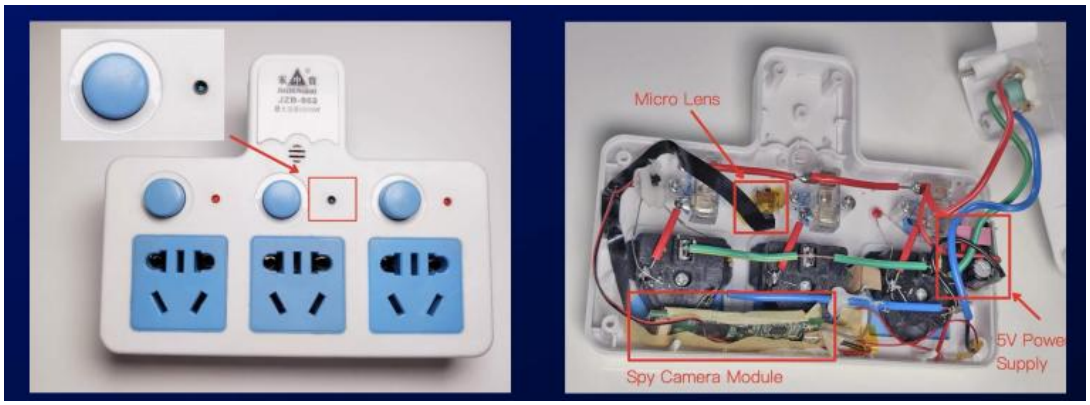
Những rủi ro tiềm ẩn trong mạng nội bộ bao gồm việc ghi lại hình ảnh, âm thanh nhạy cảm tại các phòng họp kín của lãnh đạo, gây xâm phạm nghiêm trọng đến quyền riêng tư. Ngoài ra, các thiết bị lạ có thể tạo ra cửa hậu (backdoor), trở thành điểm xâm nhập cho tin tặc tấn công toàn bộ hệ thống mạng. Nguy hiểm hơn, việc nghe lén và đánh cắp bí mật kinh doanh có thể dẫn đến thất thoát chiến lược, quy trình công nghệ và thông tin quan trọng ngay từ bên trong tổ chức.

Tùy theo mục đích sử dụng và phương thức triển khai, camera do thám hiện nay thường hoạt động theo ba hình thức chính:

- Ghi hình cục bộ (Offline): Thiết bị ghi hình và lưu trữ dữ liệu trực tiếp trên thẻ nhớ, không kết nối mạng và không phát sóng. Camera thường sử dụng pin độc lập, hoạt động trong thời gian nhất định. Do không tạo ra tín hiệu truyền thông, hình thức này chỉ có thể được phát hiện thông qua kiểm tra vật lý trực tiếp tại khu vực nghi vấn.

- Truyền hình trực tiếp (Live Streaming): Camera kết nối vào mạng Wi-Fi nội bộ hoặc tự phát một điểm truy cập (Hotspot) riêng, cho phép người điều khiển theo dõi hình ảnh từ xa thông qua ứng dụng hoặc trình duyệt. Đây là hình thức phổ biến và có khả năng bị phát hiện cao hơn do phát sinh lưu lượng mạng và tín hiệu không dây.

- Lưu trữ đám mây (Cloud & 4G): Thiết bị sử dụng SIM 4G/5G riêng hoặc lợi dụng hạ tầng mạng LAN sẵn có để truyền dữ liệu hình ảnh, âm thanh lên các máy chủ lưu trữ đám mây. Dữ liệu có thể được truy cập từ xa mà không phụ thuộc vào mạng nội bộ tại nơi lắp đặt, gây khó khăn trong việc phát hiện và kiểm soát.



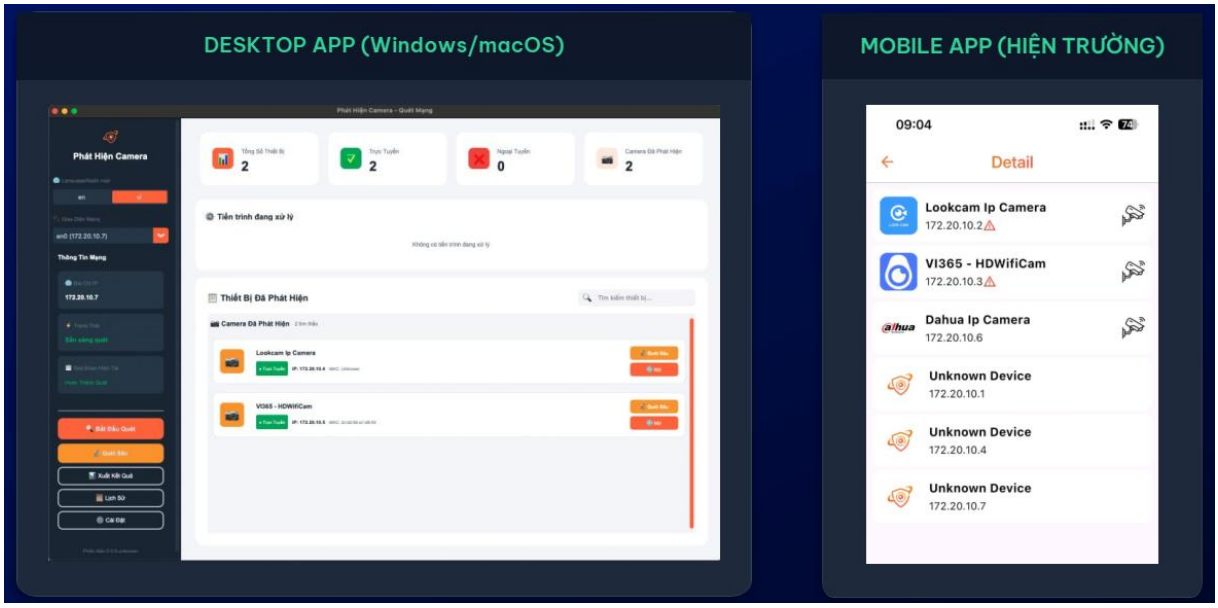
Hình 2.9. Các hình thức hoạt động của camera do thám

Các thiết bị camera do thám hiện đại thường sử dụng thấu kính pinhole siêu nhỏ, được ngụy trang tinh vi trong các vật dụng đang hoạt động bình thường, chẳng hạn vừa sạc điện thoại vừa thực hiện quay lén. Ngoài ra, thiết bị thường hoạt động ở chế độ thụ động, chỉ kích hoạt khi phát hiện chuyển động. Chúng có thể ẩn SSID Wi-Fi, giả mạo địa chỉ MAC hoặc sử dụng các kỹ thuật che giấu lưu lượng nhằm tránh bị phát hiện trong quá trình rà soát mạng.

- Các phương pháp dò tìm: Dò tìm vật lý, áp dụng các biện pháp như sử dụng đèn hồng ngoại để tìm phản xạ của thấu kính camera, quét sóng vô tuyến (RF) nhằm phát hiện tín hiệu phát bất thường, hoặc sử dụng camera nhiệt để xác định các vùng tỏa nhiệt không bình thường trong không gian kín; Rà soát mạng nội bộ; thực hiện quét phát hiện thiết bị lạ (Asset Discovery) trong mạng nội bộ và phân tích lưu lượng

(Traffic Analysis) để nhận diện các luồng dữ liệu hình ảnh/âm thanh được gửi ra các máy chủ hoặc địa chỉ IP không rõ nguồn gốc.

- Giải pháp phòng chống: Đối với người dùng và cán bộ quản lý: Sử dụng các ứng dụng dò quét trên điện thoại hoặc máy tính cá nhân để phát hiện thiết bị lạ, kết hợp kiểm tra định kỳ phòng họp, khu vực nhạy cảm. Đồng thời, cấu hình bộ định tuyến (Router) nhằm kiểm soát thiết bị truy cập và chặn các tên miền, máy chủ không tin cậy. Đối với chuyên gia an toàn thông tin: Triển khai các công cụ phân tích mạng chuyên sâu như card mạng hoạt động ở chế độ Monitor Mode để giám sát và phân tích hành vi gói tin. Thường xuyên cập nhật cơ sở dữ liệu về thiết bị gián điệp, dấu hiệu nhận biết (IOC) và phối hợp xử lý, vô hiệu hóa các máy chủ điều khiển và thu thập dữ liệu (C2) khi phát hiện nguy cơ.



Hình 2.10 "Quick Scan" Wi-Fi khi vào phòng họp. Phát hiện nhanh thiết bị lạ xung quanh

PHẦN 3 - KẾT LUẬN

3.1 Về xu hướng phát triển công nghệ an ninh mạng trên thế giới

Sáng chế liên quan đến công nghệ an ninh mạng được ghi nhận đăng ký sớm nhất vào năm 1973 và có sự tăng trưởng liên tục, vượt mốc 100 sáng chế/năm vào năm 1993, đến năm 2001 đã vượt mốc 1000 sáng chế/năm, đến năm 2018 là hơn 10.000 sáng chế/năm, và đạt mức cao nhất là 32.991 sáng chế vào năm 2023. Đến nay, số lượng đăng ký bảo hộ trên toàn thế giới đã hơn 252.000 họ sáng chế, với tốc độ tăng trưởng CAGR trong vòng 10 năm qua (2015 - 2024) là 15,3%. Sáng chế về công nghệ an ninh mạng được công bố ngày càng nhiều cho thấy sự đầu tư mạnh mẽ vào đổi mới công nghệ nhằm chống lại các mối đe dọa mạng đang gia tăng không ngừng. Mặc dù số lượng sáng chế về an ninh mạng đạt mức cao, nhưng phần lớn các sáng chế bảo hộ trong nước, chỉ có 27,8% (tương ứng với 27,8% họ sáng chế) được bảo hộ ở quy mô quốc tế và đang có xu hướng giảm dần tỷ lệ IPFs/Tổng số họ sáng chế trong các năm gần đây.

Xét theo quốc gia bảo hộ, sáng chế về công nghệ an ninh mạng được đăng ký bảo hộ tại 64 quốc gia, vùng lãnh thổ và 2 tổ chức quốc tế. Trong đó, Trung Quốc là quốc gia có nhiều sáng chế đăng ký bảo hộ nhất, chiếm đến 58,7% tổng số họ sáng chế trên toàn thế giới, kế đến là Mỹ, Hàn Quốc, Nhật Bản,... Tuy nhiên, Mỹ, WIPO (PCT) và EPO mới là thị trường được nhắm mục tiêu chính trong chiến lược bảo hộ sáng chế quốc tế với tần suất bảo hộ lên tới 87,9% đối với sáng chế đăng ký tại Mỹ, 67,1% tại WIPO (PCT) và 55% tại EPO.

Theo các lĩnh vực an ninh mạng, *Bảo mật Hạ tầng mạng*, *Bảo mật Dữ liệu*, *Quản lý Danh tính và Truy cập* có tổng số lượng họ sáng chế và IPFs nhiều nhất, kế đến là *Bảo mật Thiết bị đầu cuối*, *Bảo mật Ứng dụng* và có số lượng họ sáng chế thấp nhất là *Bảo mật hạ tầng/thiết bị IoT*. Trong lĩnh vực *Bảo mật Hạ tầng mạng*, phần lớn sáng chế liên quan đến Giao thức bảo mật mạng. Trong lĩnh vực *Bảo mật Dữ liệu*, các sáng chế chủ yếu đề cập đến vấn đề *Kiểm soát quyền truy cập dữ liệu*. Trong lĩnh vực *Quản lý Danh tính và Truy cập*, các sáng chế chủ yếu đề cập đến vấn đề *Xác thực người dùng*. Trong lĩnh vực Bảo mật Thiết bị đầu cuối, các sáng chế chủ yếu đề cập đến vấn đề *Chứng nhận hoặc duy trì các nền tảng máy tính đáng tin cậy*. Còn trong lĩnh vực *Bảo mật Ứng dụng*, các sáng chế chủ yếu đề cập đến các biện pháp chống phần mềm độc hại. Bảo mật hạ tầng/thiết bị

IoT và Bảo mật Hạ tầng mạng có xu hướng phát triển nhanh nhất với tốc độ tăng trưởng vòng trong 10 năm gần đây (2015-2024) lần lượt là 57,9% và 23,6%.

Phân tích theo xu hướng ứng dụng một số công nghệ mới nổi trong thời gian gần đây, công nghệ *Blockchain*, *Trí tuệ nhân tạo và Học máy* đang được ứng dụng nhiều trong các sáng chế về an ninh mạng. Tuy nhiên, tốc độ tăng trưởng trong vòng 5 năm gần đây cho thấy công nghệ *Blockchain* ứng dụng trong an ninh mạng chưa có sự phát triển tích cực, chỉ ghi nhận tốc độ tăng trưởng rất nhanh ở các lĩnh vực *Bảo mật lượng tử*, *Bảo mật hậu lượng tử* và *Bảo mật Zero-Trust*. Công nghệ *Trí tuệ nhân tạo và Học máy* cho thấy vẫn tiếp tục có sự tăng trưởng ổn định và liên tục trong giai đoạn 2020-2024.

Theo xu hướng ứng dụng công nghệ an ninh mạng trong các ngành công nghiệp, *Giao thông vận tải* là ngành được nghiên cứu và ứng dụng nhiều nhất, tập trung chủ yếu vào các giải pháp bảo mật mạng kết nối với phương tiện và hệ thống giao thông thông minh. Đứng thứ hai là ngành *Tài chính-Ngân hàng-Bảo hiểm*, với phần lớn các sáng chế liên quan đến quản lý danh tính, xác thực và bảo mật dữ liệu. Ngành *Sản xuất* xếp ở vị trí tiếp theo, tập trung vào các giải pháp đảm bảo an toàn an ninh mạng cho hệ thống thiết bị và dây chuyền công nghiệp thông minh. Mặc dù ngành Năng lượng có số lượng sáng chế khá khiêm tốn, nhưng có tốc độ tăng trưởng nhanh nhất trong 10 năm gần đây, phản ánh mối quan tâm ngày càng gia tăng đối với an ninh mạng trong các hệ thống hạ tầng năng lượng. Bên cạnh đó, các ngành Y tế - Chăm sóc sức khỏe, Thương mại và Viễn thông cũng đạt mức tăng trưởng dương hai con số, cho thấy công nghệ an ninh mạng đang được nghiên cứu và ứng dụng ngày càng rộng rãi trong hầu hết các lĩnh vực. Điều này đồng thời khẳng định rủi ro an ninh mạng là thách thức mang tính đa ngành, không loại trừ bất kỳ lĩnh vực nào.

Dẫn đầu sở hữu sáng chế về công nghệ an ninh mạng trên thế giới chủ yếu là các tập đoàn công nghệ lớn như: Tập đoàn Huawei (Trung Quốc), Tập Đoàn IBM (Mỹ), Tập đoàn Samsung (Hàn Quốc), Tập đoàn Microsoft (Mỹ). Trong Top 20 đơn vị sở hữu nhiều sáng chế, phần lớn là các tập đoàn công nghệ của Trung Quốc (9), kế tiếp là Mỹ (7), Nhật Bản (3) và Hàn Quốc (1). Đối với các sáng chế quốc tế, tập đoàn Huawei (Trung Quốc) vẫn tiếp tục dẫn đầu số lượng sáng chế sở hữu. Ngoài ra, trong các tổ chức sở hữu nhiều IPFs, có sự xuất hiện 1 đại diện của Châu Âu là Tập đoàn Ericsson (Thụy Điển), còn lại các tập đoàn công nghệ của Châu Á vẫn tiếp chiếm ưu thế lớn so với các khu vực khác.

3.2 Các nghiên cứu, ứng dụng công nghệ an ninh mạng tại Việt Nam

Theo cơ sở dữ liệu WIPO Publish của Cục Sở hữu Trí tuệ, tính đến tháng 10/2025, có 131 sáng chế, giải pháp hữu ích đề cập đến công nghệ an ninh mạng đã được đăng ký bảo hộ tại Việt Nam từ năm 1999 đến nay. Trong đó, có 32 chủ đơn là các viện nghiên cứu, trường đại học, cơ quan quản lý nhà nước và doanh nghiệp công nghệ Việt Nam (Viện Công nghệ thông tin - Đại học Quốc gia Hà Nội, Trường Đại học Bách khoa - Đại học Quốc gia TP.HCM, Viện Công nghệ thông tin - Viện Hàn lâm Khoa học và Công nghệ Việt Nam, Viện Khoa học và Công nghệ Quân sự, Sở Khoa học và Công nghệ TP.HCM, Trường Đại học Khoa học Tự nhiên - Đại học Quốc gia TP.HCM - Sở Khoa học và Công nghệ TP.HCM, Trường Đại học Cần Thơ, Công ty Cổ phần BKAV, Công ty Cổ phần Phygital Labs, Công ty Cổ phần Nghiên cứu và Ứng dụng Trí tuệ nhân tạo VinAI,...), còn lại là các chủ đơn đến từ Trung Quốc (Tập đoàn Huawei, Tập đoàn Tencent, Công ty Honor,...), Mỹ (Tập đoàn Qualcomm), Phần Lan (Tập đoàn Nokia), Anh (Công ty Advanced New Technologies),... Các sáng chế, giải pháp hữu ích về công nghệ an ninh mạng đăng ký bảo hộ tại Việt Nam chủ yếu đề cập đến Bảo mật Hạ tầng mạng và Quản lý Danh tính và Truy cập. Với mức độ quan tâm của các nhà khoa học và cộng đồng ngày càng tăng, các giải pháp ứng dụng công nghệ an ninh mạng được dự báo sẽ tiếp tục phát triển theo chiều hướng tích cực.

Tại Hội thảo "*Xu hướng công nghệ an ninh mạng*", được Trung tâm Thông tin, Thống kê và Ứng dụng tiến bộ khoa học công nghệ TP.HCM tổ chức vào ngày 18/12/2025, một số nội dung liên quan đến việc nghiên cứu, ứng dụng công nghệ an ninh mạng đã được giới thiệu: (1) Trường Đại học Bách Khoa (Đại học Quốc gia TP.HCM) với "*Nghiên cứu, thiết kế, chế tạo thiết bị định tuyến (router) tốc độ cao, bảo mật an toàn thông tin*", đã đề xuất xây dựng lại toàn bộ nền tảng phần mềm và phần cứng router dựa trên mã nguồn mở, làm chủ công nghệ, tăng cường khả năng bảo mật và nâng cao hiệu năng xử lý, đánh giá cho thấy thiết bị router nghiên cứu đạt hiệu năng cao, khả năng chống tấn công DDoS tốt, thông lượng VPN vượt trội so với nhiều sản phẩm thương mại cùng phân khúc, đồng thời đáp ứng các tiêu chuẩn kỹ thuật, đo kiểm phát xạ điện từ theo quy định hiện hành; (2) Học viện Công nghệ Bưu chính Viễn thông với nghiên cứu "*Vấn đề phát hiện tấn công có chủ đích (APT) sử dụng trí tuệ nhân tạo*", đã trình bày các hướng tiếp cận hiện nay trong phát hiện APT, gồm phát hiện dựa trên hành vi tại thiết bị đầu cuối và phát hiện dựa trên giám sát lưu lượng mạng, trên cơ sở đó đưa ra đề xuất giải

pháp phát hiện APT dựa trên phân tích kết nối mạng bất thường kết hợp trí tuệ nhân tạo, nhằm khắc phục hạn chế của các phương pháp truyền thống; (3) Trường Đại học Khoa học Tự nhiên (Đại học Quốc gia TP.HCM) với nghiên cứu *"AI Security - Từ bảo mật cơ sở dữ liệu đến bảo mật riêng tư trong học máy"*, đã giới thiệu một số giải pháp bảo mật và bảo vệ quyền riêng tư, bao gồm học liên kết an toàn, mã hóa đồng cấu trong học máy, mô hình máy chủ hai tầng và các kỹ thuật unlearning nhằm loại bỏ ảnh hưởng của dữ liệu không mong muốn khỏi mô hình học, các giải pháp này góp phần nâng cao mức độ an toàn và tin cậy của hệ thống trí tuệ nhân tạo trong môi trường thực tế; (4) Viện Ứng dụng Công nghệ mới với giải pháp *"Camera do thám và hiểm họa lộ lọt thông tin"*, đã phân tích nguy cơ mất an toàn thông tin từ các thiết bị camera do thám và thiết bị gián điệp công nghệ cao, và đề xuất giải pháp tổng thể kết hợp giữa rà soát vật lý định kỳ và giám sát an ninh mạng nội bộ, trong đó, việc quét phát hiện thiết bị lạ trong mạng LAN/Wi-Fi, phân tích lưu lượng dữ liệu bất thường, cấu hình router chặt chẽ và kiểm soát kết nối ra bên ngoài được xem là biện pháp then chốt.

3.3 Một số nhận xét, khuyến nghị

Theo các chuyên gia, để có thể nghiên cứu, ứng dụng công nghệ an ninh mạng đạt hiệu quả, một số điểm cần lưu ý như sau:

- Xu thế tấn công mạng hiện nay đang thay đổi theo các xu hướng mới, bao gồm gián điệp mạng, sự phát triển của các công nghệ mới, các kỹ thuật tấn công APT, một số kỹ thuật tấn công ứng dụng học máy, học sâu và trí tuệ nhân tạo, khai thác các lỗ hổng phần cứng, phần mềm, các công cụ tấn công do AI hỗ trợ, nền tảng Blockchain, cùng với yêu cầu phát triển đồng bộ chính sách và công nghệ kèm theo. Tuy nhiên, hiện nay các chính sách và tiêu chuẩn về an toàn thông tin vẫn chưa được ban hành đầy đủ, mới chỉ có Luật An ninh mạng. Do đó, cần ưu tiên xây dựng chính sách trước hết, tiếp theo là xây dựng các quy chuẩn, tiêu chuẩn và hợp chuẩn liên quan. Việc xây dựng tiêu chuẩn có thể thực hiện theo hai cách: (1) áp dụng đầy đủ các tiêu chuẩn hiện có, sử dụng lại 100% các tiêu chuẩn này; hoặc (2) tiến hành đánh giá, lựa chọn tiêu chuẩn trên cơ sở xem xét các xu thế công nghệ, điều kiện kinh tế, cũng như một số yếu tố văn hóa, chính trị và các yếu tố liên quan khác.

Trí tuệ nhân tạo (AI) đang được sử dụng trong các hoạt động tấn công mạng, bao gồm việc tạo ra mã độc trên các nền tảng tự động trong thời gian rất ngắn. Dựa trên các nền tảng này, mã độc có thể được tạo ra theo cách khó bị giám sát và phát hiện,

đồng thời sinh ra các URL, đường liên kết độc hại, loại bỏ những đặc trưng cũ một cách đơn giản và tạo ra các văn phong khó bị nghi ngờ. Bên cạnh đó, AI còn được sử dụng để tìm kiếm lỗ hổng với tốc độ rất nhanh, trở thành nguồn tài nguyên đặc biệt hữu ích cho các đối tượng tấn công. Theo nhận định của ông, AI đang khiến các cuộc tấn công mạng trở nên khó phát hiện hơn rất nhiều, do đó chúng ta buộc phải thích nghi với bối cảnh mới này

- Rào cản lớn nhất hiện nay để các sản phẩm "Make in Vietnam" có thể được triển khai rộng rãi trong các hệ thống trọng yếu của Nhà nước và doanh nghiệp chủ yếu nằm ở chính sách, cụ thể là việc cơ quan nhà nước chấp nhận các sản phẩm công nghệ thông tin do các nhà khoa học Việt Nam chế tạo tham gia thị trường, nguyên nhân là do vẫn còn tồn tại tâm lý ưu tiên hàng ngoại, vì vậy cần phải đưa ra các so sánh với sản phẩm nước ngoài và các hãng lớn.

- Đối với người dân bình thường, việc phát hiện các dấu hiệu bất thường hoặc ghi nhận sự kiện trên thực tế là rất khó, bởi hiện nay camera được lắp đặt ở hầu khắp các hộ gia đình; tuy nhiên, phần lớn các camera này chỉ phục vụ nhu cầu cá nhân, thường là các thiết bị giá rẻ, xuất xứ không rõ ràng và tiềm ẩn sẵn các lỗ hổng bảo mật, tạo điều kiện để hacker dễ dàng phát hiện và tấn công sau các đợt dò quét. Do đó, người sử dụng cần nắm được loại camera đang dùng, tìm hiểu rõ nguồn gốc xuất xứ, các lỗi bảo mật đã được công bố (nếu có), không phó thác hoàn toàn cho nhân viên lắp đặt, đồng thời chủ động thay đổi mật khẩu, xóa tài khoản mặc định và tạo tài khoản mới.

- Đối với những người có chuyên môn kỹ thuật, cần sử dụng các công cụ kỹ thuật để kiểm tra, xác định camera thuộc hãng nào và đánh giá xem thiết bị có tồn tại lỗ hổng hay không. Riêng đối với camera quay lén, TS. Khang cho biết các thiết bị này thường có những điểm yếu như thời lượng pin ngắn, tỏa nhiệt, và vào ban đêm có thể xuất hiện mắt hồng ngoại. Tại các khu vực đông người, mỗi cá nhân cần nâng cao ý thức cảnh giác để kịp thời phát hiện, bởi nếu rơi vào tay những đối tượng có động cơ trục lợi thì mức độ nguy hiểm là rất lớn.

PHẦN PHỤ LỤC

Phụ lục 1

MỘT SỐ KẾT QUẢ NGHIÊN CỨU VỀ CÔNG NGHỆ AN NINH MẠNG TẠI VIỆT NAM

STT	Tên đề tài	Chủ nhiệm đề tài	Cấp quản lý	Cơ quan chủ trì	Thời gian thực hiện
1	Nghiên cứu thử nghiệm tổng hợp, giảm thiểu cảnh báo về sự kiện an toàn, an ninh mạng theo thời gian thực	ThS. Đặng Hữu Thành	Bộ	Trung tâm Công nghệ thông tin và chuyển đổi số (Bộ Kế hoạch và Đầu tư)	01/3/2024-20/12/2024
2	Vấn đề an ninh phi truyền thống, trọng tâm là an ninh mạng trong nền an ninh quốc gia	PGS.TS. Nguyễn Thị Trường Giang	Quốc gia	Học viện Báo chí và Tuyên truyền (Học viện Chính trị Quốc gia Hồ Chí Minh)	01/04/2022-01/04/2025
3	Nghiên cứu và xây dựng ứng dụng phát hiện tấn công có chủ đích (APT) dựa trên phân tích kết nối bất thường sử dụng trí tuệ nhân tạo	PGS.TS. Đỗ Xuân Chợ	Bộ	Học viện Công nghệ Bưu chính Viễn thông (Bộ KH&CN)	01/05/2024-30/11/2024
4	Nghiên cứu và xây dựng giải pháp bảo mật cho một số dịch vụ chuyển đổi số dựa trên kỹ thuật đảm bảo an toàn thông tin trên các thiết bị đầu cuối	PGS.TS. Đỗ Xuân Chợ	Bộ	Học viện Công nghệ Bưu chính Viễn thông (Bộ KH&CN)	01/01/2023-01/12/2023
5	Quản lý Nhà nước về hoạt động ngân hàng số - thực tiễn kinh nghiệm quốc tế và giải pháp đối với Việt Nam	ThS. Lê Anh Dũng	Bộ	Ngân hàng Nhà nước Việt Nam	01/06/2021-01/01/2023
6	Nghiên cứu nâng cao bảo mật phần cứng cho các hệ thống Internet vạn vật	PGS. TS. Hoàng Văn Phúc	Quốc gia	Học viện Kỹ thuật Quân sự (Bộ Quốc phòng)	01/10/2020-01/04/2023
7	Nghiên cứu xây dựng hệ thống tự động phát hiện cảnh báo và ngăn chặn tấn công mạng nhằm vào các thiết bị IoT cỡ nhỏ sử dụng mạng lưới tác tử thông minh	TS. Ngô Quốc Dũng	Quốc gia	Học viện Công nghệ Bưu chính Viễn thông (Bộ KH&CN)	01/10/2020-01/04/2023
8	Nghiên cứu đề xuất giải pháp đảm bảo an ninh mạng cho Đài Tiếng nói Việt Nam trong tình hình mới	KS. Cao Hòa Bình	Bộ	Trung tâm Nghiên cứu và Ứng dụng Công nghệ Truyền thông (Đài Tiếng nói Việt Nam)	01/01/2022-01/12/2022
9	Nghiên cứu xây dựng thử nghiệm hệ thống kiểm tra đánh giá an toàn thông tin đối với các thiết bị IoT dân dụng	ThS. Vũ Hoài Nam	Bộ	Học viện Công nghệ Bưu chính Viễn thông (Bộ KH&CN)	01/05/2022-01/12/2022

10	Phân tích và tối ưu khả năng bảo mật của mạng vô tuyến nhận thức thu thập năng lượng	PGS. TS. Hồ Văn Khương	Quốc gia	Trường ĐH Bách khoa (Đại học Quốc gia TP.HCM)	01/04/2020-01/11/2022
11	Nghiên cứu đánh giá hiện trạng về bảo mật thông tin cho hệ thống các thiết bị Camera thông dụng có kết nối Internet tại Thành Phố Hồ Chí Minh	TS. Võ Văn Khang	Tỉnh/ Thành phố	Trung tâm An ninh mạng (UBND TP. Hồ Chí Minh)	01/12/2020-01/12/2022
12	Nghiên cứu xây dựng hệ thống HoneyWall phục vụ công tác bảo vệ website các đơn vị hành chính sự nghiệp trên địa bàn thành phố Cần Thơ	ThS. Nguyễn Văn Kha	Tỉnh/ Thành phố	Trung tâm Thông tin Khoa học và Công nghệ Cần Thơ (UBND TP. Cần Thơ)	01/11/2018-01/06/2021
13	Nghiên cứu thiết kế và chế tạo thiết bị IoT Gateway tích hợp giải pháp bảo mật trên nền tảng IoT ứng dụng thí điểm quan trắc chất lượng không khí tại Khu công nghệ cao TP.HCM	TS. Trịnh Xuân Thắng	Tỉnh/ Thành phố	Trung tâm nghiên cứu triển khai khu công nghệ cao (UBND TP.HCM)	01/12/2018-01/06/2021
14	Nghiên cứu các giải pháp bảo mật trong mạng cảm biến không dây (WSN) phục vụ xây dựng đô thị thông minh	ThS. Trần Huy Long	Bộ	Viện khoa học kỹ thuật bưu điện (Bộ KH&CN)	01/02/2021-01/11/2021
15	Nghiên cứu thiết kế và chế tạo vi mạch bảo mật dữ liệu ứng dụng trong IoT và phát triển thiết bị ứng dụng	PGS.TS. Trần Xuân Tú	Quốc gia	Trường Đại học Công nghệ (Đại học Quốc gia Hà Nội)	01/07/2019-01/08/2021
16	Nghiên cứu thiết kế chế tạo thiết bị vô tuyến sóng ngắn băng rộng định nghĩa bằng phần mềm sử dụng cấu trúc đổi tần trực tiếp bảo mật thông tin thoại và dữ liệu	TS. Tạ Việt Hùng	Quốc gia	Trung tâm Kỹ Thuật Thông tin Công nghệ cao (Bộ Quốc phòng)	01/10/2017-01/09/2021
17	Phương pháp mật mã dữ liệu ảnh dựa trên hỗn loạn và thiết kế trên phần cứng	PGS.TS. Hoàng Mạnh Thắng	Quốc gia	Viện Điện tử - Viễn thông (Bộ Giáo dục và Đào tạo)	01/12/2018-01/12/2021
18	Thiết kế vi mạch dùng SoCFPGA cho các ứng dụng IoT có tính bảo mật cao	TS. Huỳnh Hữu Thuận	Tỉnh/ Thành phố	Trường ĐH Khoa học Tự nhiên (Đại học Quốc gia TP.HCM)	2021
19	Nghiên cứu xây dựng phần mềm giám sát cảnh báo hỗ trợ công tác phòng chống tấn công trên mạng cục bộ đảm bảo an toàn thông tin trong các cơ quan nhà nước trên địa bàn tỉnh Hà Tĩnh	ThS Nguyễn Thanh Lâm	Tỉnh/ Thành phố	Trung tâm Công nghệ Thông tin và Truyền thông (Bộ KH&CN)	01/05/2019-01/05/2020
20	Nghiên cứu thiết kế chế tạo thử nghiệm thiết bị định tuyến tích hợp đa dịch vụ có tính năng bảo đảm an toàn bảo mật thông tin	PGS.TS. Hoàng Trang	Quốc gia	Trường ĐH Bách khoa (Đại học Quốc gia TP.HCM)	01/07/2019-01/12/2020

21	Nghiên cứu xây dựng bộ tiêu chuẩn về các kỹ thuật an toàn công nghệ thông tin (Lựa chọn triển khai và vận hành các hệ thống phát hiện và ngăn chặn xâm nhập (IDPS) và các tiêu chuẩn ISO/IEC về an toàn thông tin)	ThS. Nguyễn Tiến Đức	Bộ	Cục An toàn thông tin (Bộ KH&CN)	01/04/2020-01/11/2020
22	Nghiên cứu vấn đề bảo mật và xây dựng các hướng dẫn bảo mật cho hệ thống thu phí điện tử không dừng ETC sử dụng công nghệ RFID tại Việt Nam	ThS. Phạm Đình Chung	Bộ	Tổng cục Đường bộ Việt Nam (Bộ Giao thông Vận tải)	01/03/2019-01/07/2020
23	Phát triển ứng dụng hệ thống xác thực bảo mật đa vai trò sử dụng vân tay trong lĩnh vực an ninh ngân hàng	TS. Trần Thiện Chính	Quốc gia	Viện khoa học kỹ thuật bưu điện (Bộ KH&CN)	01/04/2018-01/12/2020
24	Nghiên cứu thiết kế chế tạo thiết bị chuyển mạch (Switch) có tính năng an toàn bảo mật thông tin trên nền tảng FPGA và mã nguồn mở	TS. Thái Trung Kiên	Quốc gia	Viện Công nghệ thông tin/Viện KH-CN quân sự (Bộ Quốc phòng)	01/11/2018-01/11/2020
25	Nghiên cứu xây dựng hệ thống hỗ trợ bảo vệ ngăn chặn rò rỉ dữ liệu trong hoạt động Chính phủ điện tử	TS. Hoàng Tuấn Hảo	Quốc gia	Viện Công nghệ Mô phỏng (Bộ Quốc phòng)	01/07/2018-01/06/2020
26	Nghiên cứu phát triển thử nghiệm hệ thống phát hiện botneet trong thiết bị công kết nối IoT	PGS.TS. Hà Hải Nam	Bộ	Viện khoa học kỹ thuật bưu điện (Bộ KH&CN)	01/01/2020-01/12/2020
27	Nghiên cứu thiết kế và chế tạo hệ thống Camera có tính bảo mật cao	TS. Phạm Hùng Mạnh	Quốc gia	Công ty CP Công nghệ Công nghiệp Bưu chính Viễn thông (VNPT Technology)	01/07/2018-01/06/2020
28	Nghiên cứu phát triển máy tính an toàn phục vụ Chính phủ điện tử	ThS. Hoàng Mạnh Cường	Quốc gia	Công ty CP Công nghệ Công nghiệp Bưu chính Viễn thông (VNPT Technology)	01/07/2018-01/03/2020
29	Nghiên cứu xây dựng hướng dẫn đảm bảo an toàn thông tin trong đô thị thông minh	TS. Cao Minh Thắng	Bộ	Học viện Công nghệ Bưu chính Viễn thông (Bộ KH&CN)	01/04/2019-01/11/2019
30	An toàn bảo mật phần cứng: Phương pháp công nghệ và ứng dụng	PGS.TS. Hoàng Văn Phúc	Quốc gia	Trường Đại học Kỹ thuật Lê Quý Đôn (Bộ Giáo dục và Đào tạo)	01/08/2018-01/06/2019
31	Nghiên cứu xây dựng các bài đo và bộ công cụ đo kiểm đánh giá các lỗ hổng bảo mật với thiết bị IP camera	TS. Cao Minh Thắng	Bộ	Viện Công nghệ Thông tin và Truyền thông CDIT (Bộ KH&CN)	01/04/2018-01/11/2018

32	Nghiên cứu triển khai cung cấp ứng dụng bảo mật khóa công khai (Resource Public Key Infrastructure - RPKI) phục vụ xác thực thông tin định tuyến trong công tác quản lý địa chỉ IP/số hiệu mạng ASN của Việt Nam	ThS. Nguyễn Thị Thu Thủy	Bộ	Trung tâm Internet Việt Nam (Bộ KH&CN)	01/05/2018-01/11/2018
33	Nghiên cứu áp dụng các chuẩn an toàn bảo mật thông tin cho các ứng dụng web dịch vụ công Bộ Tài nguyên và Môi trường	KS. Phạm Thanh Tùng	Bộ	Cục Công nghệ Thông tin và Dữ liệu tài nguyên môi trường (Bộ Tài nguyên và Môi trường)	01/01/2016-01/06/2018
34	Nghiên cứu các lõi phần cứng mã hóa nhận thực công suất siêu thấp tốc độ cao cho các mạng không dây tiên tiến	TS. Hoàng Văn Phúc	Quốc gia	Học viện Kỹ thuật Quân sự	01/05/2016-01/05/2018
35	Nghiên cứu và xây dựng hệ thống tường lửa thông minh cho các ứng dụng WEB-IWAF	ThS. Huỳnh Hoàng Tân	Tỉnh/ Thành phố	Trung tâm phát triển phần mềm (UBND Tỉnh Đồng Nai)	2018
36	Ứng dụng công nghệ bảo đảm an ninh an toàn mạng và bí mật thông tin ở mức cao để phát triển bộ giải pháp an toàn an ninh mạng LAN cho cơ quan nhà nước và doanh nghiệp	TS. Lê Quang Minh	Quốc gia	Viện Công nghệ Thông tin (Đại học Quốc gia Hà Nội)	01/07/2015-01/12/2017
37	Phát triển thiết bị phần cứng firewall tốc độ cao	TS. Nguyễn Hoài Đức	Tỉnh/ Thành phố	Trung tâm Vi mạch Đà Nẵng (UBND TP. Đà Nẵng)	11/2015-10/2017
38	Nghiên cứu kinh nghiệm xây dựng chiến lược quốc gia về an toàn không gian mạng và đề xuất cho Việt Nam	ThS. Nguyễn Kim Quang, ThS. Cao Minh Thắng	Bộ	Học viện Công nghệ Bưu chính Viễn thông (Bộ KH&CN)	03/2017-11/2017
39	Nghiên cứu các vấn đề bảo mật trong hệ thống thông tin di động 4G LTE	ThS. Lê Xuân Trung	Bộ	Viện khoa học kỹ thuật bưu điện (Bộ KH&CN)	03/2017-11/2017
40	Hoàn thiện công nghệ bảo mật hệ thống PACS (Picture Archiving and Communication System) ứng dụng chẩn đoán hình ảnh số tại bệnh viện	ThS. Nguyễn Chí Ngọc	Tỉnh/ Thành phố	Công ty Cổ phần Công nghệ Thông minh Ưu Việt	06/2015-01/2017
41	Xây dựng giải pháp phần mềm Deface Tracking hỗ trợ kiểm soát thông tin bảo mật thông tin cho cổng/trang thông tin điện tử của các cơ quan nhà nước trên địa bàn tỉnh Bình Dương	ThS. Đinh Thị Thu Hương, PGS.TS. Vũ Thanh Nguyên	Tỉnh/ Thành phố	Trường đại học Thủ Dầu Một (UBND Tỉnh Bình Dương)	2016

42	Nghiên cứu áp dụng ISO 27001 để quản lý an toàn an ninh mạng máy tính và quản lý hệ thống lưu trữ dữ liệu tại Bộ Khoa học và Công nghệ	KS. Đặng Huỳnh Kim	Bộ	Trung tâm tin học - Bộ Khoa học và Công nghệ	01/2016-12/2016
43	Nghiên cứu xây dựng giải pháp giám sát phân tích và nhận biết các hình thức tấn công vào Website của các đơn vị trực thuộc Bộ KH&CN	KS. Vũ Văn Phán	Bộ	Trung tâm tin học - Bộ KH&CN	01/2015-06/2016
44	Nghiên cứu thiết kế và đánh giá các giao thức liên lạc có khả năng đảm bảo an toàn thông tin ở lớp vật lý	TS. Hà Đắc Bình	Quốc gia	Trường Đại học Duy Tân (Bộ Giáo dục và Đào tạo)	03/2014-03/2016
45	Nghiên cứu phương pháp nâng cao bảo mật trong truyền tin sử dụng kỹ thuật hỗn loạn	PGS.TS. Hoàng Mạnh Thắng	Quốc gia	Trường ĐH Bách Khoa Hà Nội (Bộ Giáo dục và Đào tạo)	12/2013-12/2016
46	Giải pháp an ninh cho hotpost công cộng	PGS.TS. Nguyễn Đình Thúc		Trường ĐH Khoa học Tự nhiên (Đại học Quốc gia TP.HCM)	2013
47	Chế tạo các thiết bị điện tử chuyên dụng có độ bảo mật cao phục vụ công tác quản lý điều hành	KS. Nguyễn Văn Dư	Quốc gia	Viện Điện tử, Viện KHCN Quân sự (Bộ Quốc phòng)	2009-2010
48	Nghiên cứu xây dựng phần mềm quản lý danh tính của người dùng và hỗ trợ bảo mật dữ liệu dựa trên môi trường PKI cho doanh nghiệp	Nguyễn Đình Lượng	Bộ	Viện NC Điện tử-Tin học-Tự động hóa (Bộ Công thương)	2009
49	Xây dựng và triển khai ứng dụng Grid có tính bảo mật cao	TS. Trần Văn Lăng		Phân viện Công nghệ Thông tin tại TP. Hồ Chí Minh	2004-2006
50	Nghiên cứu một số vấn đề kỹ thuật công nghệ chủ yếu trong thương mại điện tử và triển khai thử nghiệm - Nghiên cứu xây dựng giải pháp bảo mật thông tin trong thương mại điện tử - hệ thống cấp phát và quản lý chứng chỉ số	TS. Lê Danh Vĩnh	Quốc gia	Trung tâm thông tin thương mại (Bộ Công Thương)	2006
51	Xây dựng giải pháp và công cụ bảo mật (cho các hệ thống thông tin trên mạng của các cơ quan quản lý Nhà nước tỉnh Bà Rịa - Vũng Tàu)	TS. Nguyễn Xuân Dũng	Tỉnh/ Thành phố	Sở KH&CN Bà Rịa - Vũng Tàu (UBND Tỉnh Bà Rịa-Vũng Tàu)	2006

52	Nghiên cứu xây dựng qui trình tổng thể giải pháp đảm bảo an toàn an ninh thông tin ứng dụng cho hội nghị truyền hình (video-conferencing) - Nghiên cứu khảo sát tình hình triển khai dịch vụ hội nghị truyền hình trên thế giới và ở Việt Nam	TS. Trần Hồng Quân	Quốc gia	Viện khoa học kỹ thuật bưu điện (Bộ Thông tin và Truyền thông)	2003-2005
53	Nghiên cứu và triển khai một số phương pháp bảo vệ dữ liệu trong giao dịch điện tử	TS. Dương Đức Anh	Tỉnh/ Thành phố	Trường ĐH Khoa học Tự nhiên (Đại học Quốc gia TP.HCM)	2005
54	Hỗ trợ bảo vệ hệ thống thông tin cho các mạng tin học Việt Nam	Trịnh Ngọc Minh	Tỉnh/ Thành phố	Trung tâm Phát triển Công nghệ thông tin (Đại học Quốc gia TP.HCM)	2004
55	Hỗ trợ bảo vệ hệ thống thông tin cho các mạng tin học Việt Nam			Trung tâm Phát triển Công nghệ thông tin (Đại học Quốc gia TP.HCM)	2004
56	Nghiên cứu thiết kế chế tạo thiết bị bảo mật thông tin tiếng nói trên mạng điện thoại công cộng	TS. Đào Thế Long		Trung tâm Toán - Máy tính (UBND TP. Hồ Chí Minh)	1998

Phụ lục 2

MỘT SỐ SÁNG CHẾ, GIẢI PHÁP HỮU ÍCH VỀ CÔNG NGHỆ AN NINH MẠNG ĐÃ ĐĂNG KÝ BẢO HỘ TẠI VIỆT NAM

STT	Tên sáng chế/giải pháp hữu ích	Số đơn/ Số bằng	Chủ đơn/Chủ bằng
1	Máy để truyền thông không dây tại thiết bị người dùng và thực thể mạng	1-2023-07779	QUALCOMM INCORPORATED
2	Hệ thống thông tin thủy âm số sử dụng công nghệ đa truy cập phân chia theo mã (CDMA) và phương pháp bù dịch tần Doppler kết hợp khôi phục dữ liệu trong miền thời gian cho hệ thống này	1-2025-01702	Đại học Bách khoa Hà Nội
3	Quản lý khóa bảo mật trong hoạt động kết nối kép	1-2025-00893	NOKIA TECHNOLOGIES OY
4	Phương pháp xác thực, phân quyền và bảo mật kết nối giữa các dịch vụ nhỏ trong hệ thống kiến trúc dịch vụ phân tán tầm trung	1-2024-09792	TẬP ĐOÀN CÔNG NGHIỆP - VIỄN THÔNG QUÂN ĐỘI
5	Phương pháp bảo mật thiết bị điện tử, thiết bị điện tử và hệ thống khóa	1-2024-06644	ABSOLUTE SOFTWARE CORPORATION
6	Phương pháp và máy để phát tín hiệu và để thu tín hiệu	1-2024-06509	QUALCOMM INCORPORATED
7	Phương pháp và máy truyền thông không dây	1-2024-06247	QUALCOMM INCORPORATED
8	Hệ thống xác thực yêu cầu đăng nhập các dịch vụ trực tuyến sử dụng thẻ thông minh	2-2024-00786	TRẦN TUẤN ANH
9	Thiết bị và phương pháp hỗ trợ bảo mật hóa thông tin trạng thái định vị trong mạng di động	1-2024-03771	QUALCOMM INCORPORATED
10	Hệ thống, phương pháp, và phương tiện không tạm thời đọc được bằng máy tính để tạo các bit vectơ chức năng vật lý không thể sao chép	1-2024-05695	QUALCOMM INCORPORATED
11	Thiết bị người dùng và phương pháp để bảo mật hoạt động truyền thông của luồng phương tiện	1-2024-05916	QUALCOMM INCORPORATED
12	Thiết bị người dùng, trạm gốc và phương pháp ngăn chặn các cuộc tấn công bảo mật chủ động trong mạng không dây	1-2023-08532	QUALCOMM INCORPORATED
13	Phương pháp quản lý kết nối mạng, nút chức năng liên kết, thực thể chức năng quản lý truy cập và di động, và thiết bị người dùng	1-2024-04106	NOKIA SOLUTIONS AND NETWORKS OY
14	Hệ thống xử lý của phương tiện và phương pháp được thực hiện bởi bộ xử lý của hệ thống xử lý của phương tiện để phát hiện hành vi sai trái	1-2024-02455	QUALCOMM INCORPORATED

15	Hệ thống và phương pháp chống giả mạo mã QR ứng dụng công nghệ trí tuệ nhân tạo	1-2024-01427	Trường Đại học Cần Thơ
16	Hệ thống sách điện tử dưới dạng NFT kết hợp chip bảo mật RFID	1-2024-00665	CÔNG TY CỔ PHẦN PHYGITAL LABS
17	Hệ thống và phương pháp tiến hành các giao dịch bảo mật	1-2023-07651	DATA MESH GROUP PTY LTD
18	Hệ thống trên chip, phương pháp cung cấp bảo mật trong hệ thống trên chip và phương tiện bất biến đọc được bằng bộ xử lý	1-2024-01486	QUALCOMM INCORPORATED
19	Hệ thống quản lý và chia sẻ dữ liệu dùng chung mà tích hợp các nền tảng xử lý, phân tích dữ liệu lớn và phát triển mô hình học máy	2-2024-00210	Viện Công nghệ thông tin - Viện Hàn lâm Khoa học và Công nghệ Việt Nam
20	Phương pháp, thực thể mạng bảo mật tài nguyên PRS và thiết bị người dùng xử lý tài nguyên PRS được bảo mật để định vị UE trong mạng truyền thông không dây	1-2023-06724	QUALCOMM INCORPORATED
21	Phương pháp và hệ thống nhận ngữ cảnh bảo mật, và thiết bị truyền thông	1-2024-01319	HONOR DEVICE CO., LTD.
22	Hệ thống xử lý của phương tiện và phương pháp phát hiện hành vi sai lệch được thực hiện bởi bộ xử lý của hệ thống xử lý này	1-2024-00112	QUALCOMM INCORPORATED
23	Hệ thống lõi bảo mật lớp IP (ipsec core) bằng giải thuật mã hóa nâng cao kết hợp bộ đếm trường galois (aes-gcm) sử dụng hai máy trạng thái độc lập kết hợp phương pháp mở rộng bản mã đa luồng, được thiết kế ở cấp độ chuyển thanh ghi (RTL)	1-2023-07853	Trường Đại học Bách khoa - Đại học Quốc gia thành phố Hồ Chí Minh
24	Phương pháp bảo mật ví tài sản mã hóa	2-2023-00618	Công ty TNHH C98
25	Quy trình thiết kế phần cứng bảo mật cân bằng giữa chi phí thực thi và mức độ bảo mật	1-2023-06893	VIỆN CÔNG NGHỆ THÔNG TIN, ĐẠI HỌC QUỐC GIA HÀ NỘI
26	Phương pháp phát hiện bất thường trong mạng	VN1-0049501-000	Đỗ Xuân Chợ
27	Phương pháp và hệ thống triển khai mật khẩu thông minh, thiết bị điện tử và phương tiện có thể đọc được bằng máy tính	1-2023-03168	JIANG, Yunfan
28	Phương pháp và máy làm nhiễu loạn lệnh có thể thực thi	1-2023-04824	QUALCOMM INCORPORATED
29	Thiết bị truyền thông không dây và phương pháp truyền thông không dây bởi thiết bị này	1-2023-04367	QUALCOMM INCORPORATED

30	Phương pháp bảo mật dữ liệu cho các thiết bị camera sử dụng vi mạch tích hợp mô-đun nền tảng đáng tin cậy và thiết bị tạo khoá	1-2022-01989	CÔNG TY CỔ PHẦN BKAV
31	Thiết bị và phương pháp bảo mật thông tin sinh trắc	1-2023-04521	QUALCOMM INCORPORATED
32	Hệ thống phát hiện sự bất thường, phương pháp phát hiện sự bất thường và phương tiện đọc được bằng máy tính dựa trên các đặc điểm hệ thống	1-2023-00380	CHUNGHWA TELECOM CO., LTD.
33	Phương pháp nhận diện và quản lý dữ liệu chứa nội dung nhạy cảm	1-2021-08261	CÔNG TY CP PHẦN MỀM DIỆT VIRUS BKAV
34	Phương pháp và thiết bị quản lý tin cậy tại bộ quản lý mạng, phương pháp và thiết bị quản lý truy cập tại đại lý tin cậy	1-2023-01060	QUALCOMM INCORPORATED
35	Phương pháp và hệ thống để đánh giá bảo mật	1-2021-07145	CÔNG TY CỔ PHẦN NGHIÊN CỨU VÀ ỨNG DỤNG TRÍ TUỆ NHÂN TẠO VINAI
36	Thiết bị đầu cuối, phương tiện lưu để lưu chương trình máy tính, hệ thống truyền thông tin và phương pháp truyền thông tin	VN1-0050131-000	AISLE SOFT CORPORATION
37	Phương pháp xác định thông tin tăng cường bảo mật mặt phẳng người dùng, thiết bị truyền thông và phương tiện lưu trữ đọc được bằng máy tính	1-2022-08640	HUAWEI TECHNOLOGIES CO., LTD.
38	Hệ thống và thiết bị mạng bảo mật di động	1-2022-06999	SECURKART LLC
39	Hệ thống đo thông minh có chức năng bảo mật	1-2021-07747	LEOTEK CO., LTD.
40	Phương pháp xác định tính xác thực của ảnh toàn ký bảo mật	1-2021-05840	INNOV8TIF SOLUTIONS SDN. BHD.
41	Phương pháp và hệ thống đánh giá bảo mật	1-2021-03426	CÔNG TY CỔ PHẦN NGHIÊN CỨU VÀ ỨNG DỤNG TRÍ TUỆ NHÂN TẠO VINAI
42	Quy trình xác thực và định danh hồ sơ sử dụng chữ ký số	VN2-0003565-000	Trần Minh Huy Nguyễn Ngọc Tâm
43	Phương pháp chia sẻ dữ liệu tài khoản, thiết bị điện tử, hệ thống chip và phương tiện lưu trữ đọc được bởi máy tính	1-2022-05725	HUAWEI TECHNOLOGIES CO., LTD.
44	Quy trình đánh giá mức độ bảo mật của phần cứng dựa trên lưu vết ước lượng công suất tiêu thụ	1-2022-05520	VIỆN CÔNG NGHỆ THÔNG TIN, ĐẠI HỌC QUỐC GIA HÀ NỘI
45	Thiết bị máy chủ truyền thông, phương pháp và hệ thống truyền thông để quản lý sự xác thực của người dùng, và phương tiện lưu trữ không chuyển tiếp	1-2022-06098	GRABTAXI HOLDINGS PTE. LTD.

46	Phương pháp, thiết bị và hệ thống thu thập khoá, thiết bị truyền thông, và phương tiện lưu trữ đọc được bằng máy tính	1-2022-05531	HUAWEI TECHNOLOGIES CO., LTD.
47	Thiết bị xử lý thông tin và phương pháp xử lý thông tin, thiết bị xác thực và phương pháp xác thực, hệ thống xác thực, phương pháp xác thực trong hệ thống xác thực và phương tiện lưu trữ đọc được bằng máy tính	1-2022-03323	FELICA NETWORKS, INC.
48	Phương pháp và máy hiển thị thông tin liên hệ, phương pháp và máy tạo thẻ liên hệ, thiết bị đầu cuối và phương tiện lưu trữ đọc được bằng máy tính	1-2022-04799	PETAL CLOUD TECHNOLOGY CO., LTD.
49	Thiết bị người dùng, phần tử chức năng quản lý tính di động và truy cập và phương pháp cập nhật tham số cấu hình thiết bị người dùng	1-2021-02483	NOKIA TECHNOLOGIES OY
50	Phương pháp thực hiện thương lượng bảo mật cho cấu hình mạng, thiết bị mạng, thiết bị truyền thông và vật ghi máy tính đọc được	VN1-0047821-000	HUAWEI TECHNOLOGIES CO., LTD.
51	Phương pháp, và thiết bị để tạo và quản lý khoá mã ứng dụng trong mạng truyền thông dùng cho truyền thông được mã hoá với các ứng dụng dịch vụ	1-2022-04660	ZTE CORPORATION
52	Thiết bị người dùng, phần tử mạng của mạng di động và phương pháp bảo vệ an ninh của thông điệp tầng không truy cập (NAS)	1-2021-02262	NOKIA TECHNOLOGIES OY
53	Thiết bị thu/phát không dây (WTRU) và phương pháp sử dụng trong thiết bị thu/phát không dây	1-2022-01085	IDAC Holdings, Inc.
54	Phương pháp hỗ trợ bảo vệ toàn vẹn mặt phẳng người dùng (up ip) cho truyền thông, thiết bị không dây và thiết bị tính toán mạng	1-2022-01859	QUALCOMM INCORPORATED
55	Phương pháp thay đổi mật khẩu cưỡng bức	1-2022-00210	GAMANIA DIGITAL ENTERTAINMENT CO., LTD.
56	Mạch tạo hàm không thể sao chép về vật lý (PUF) sử dụng bộ dao động vòng và tham số khoảng cách Euclid	2-2022-00218	Hoàng Văn Phúc Trịnh Quang Kiên Trần Văn Toàn
57	Dấu của đối tượng, phương pháp tạo ra dấu này và phương pháp xác thực	VN1-0050517-000	AUTHENTIC VISION GMBH
58	Phương pháp ngăn chặn tấn công từ chối dịch vụ kiểu TCP SYN	VN1-0039924-000	Đại học Bách Khoa Hà Nội
59	Thiết bị và phương pháp điều khiển sự cung cấp truy cập đến các dịch vụ nhà khai thác cục bộ bị hạn chế bởi thiết bị người dùng	1-2021-08002	NOKIA TECHNOLOGIES OY

60	Phương pháp và thiết bị để thực hiện việc điều khiển bảo vệ trong mạng lõi, mạng lõi, và phương tiện lưu trữ đọc được bằng máy tính	VN1-0050583-000	TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)
61	Thiết bị quét và quản lý việc tuân thủ bảo mật đám mây	VN1-0041316-000	TATUM INC.
62	Thiết bị và phương pháp quản lý bảo mật trong hệ thống truyền thông	1-2021-05288	NOKIA TECHNOLOGIES OY
63	Phương pháp và hệ thống được thực hiện bằng máy tính để đào tạo các mô hình hồi quy logictic bảo mật, và vật ghi lâu dài đọc được bằng máy tính	1-2019-06120	Advanced New Technologies Co., Ltd.
64	Phương pháp và thiết bị thu thập ngữ cảnh bảo mật, và hệ thống truyền thông	VN1-0041404-000	HONOR DEVICE CO., LTD.
65	Phương pháp cung cấp sự bảo mật mặt phẳng người dùng, nút mạng, và phương tiện lưu trữ đọc được bằng máy tính	VN2-0004121-000	TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)
66	Phương pháp thực hiện phân tích kênh bên không lập mẫu sử dụng mạng nơ-ron tích chập đối với thuật toán mã mật AES 128 bit	1-2021-07694	Đỗ Ngọc Tuấn Đoàn Văn Sáng Hoàng Văn Phúc
67	Hệ thống và phương pháp giao dịch an toàn	1-2021-04613	QRYPTED TECHNOLOGY PTE. LTD.
68	Thiết bị, phương pháp và vật dụng chế tạo để quản lý bảo mật	1-2021-05285	NOKIA TECHNOLOGIES OY
69	Thiết bị kết nối có bảo mật dữ liệu trên đường truyền	2-2020-00305	Viện Công nghệ thông tin - Viện Hàn lâm Khoa học và Công nghệ Việt Nam
70	Phương pháp, thiết bị và hệ thống phát tín hiệu điều khiển tài nguyên vô tuyến (RRC) bảo mật qua giao diện PC5 dành cho truyền thông đơn hướng	1-2021-06392	IDAC Holdings, Inc.
71	Phương pháp xác thực danh tính của khóa kỹ thuật số, thiết bị đầu cuối, và phương tiện lưu trữ đọc được bằng máy tính	VN1-0043595-000	HUAWEI TECHNOLOGIES CO., LTD.
72	Quy trình mã hóa và giải mã nhờ xử lý đồng thời phần cứng và phần mềm sử dụng thuật toán xác thực và định danh AES-GCM	1-2021-05898	VIỆN CÔNG NGHỆ THÔNG TIN, ĐẠI HỌC QUỐC GIA HÀ NỘI
73	Phương pháp nhận dạng khuôn mặt, thiết bị điện tử và phương tiện lưu trữ máy tính	VN1-0044710-000	Honor Device Co., Ltd.
74	Phương pháp truy nhập mạng và thiết bị đầu cuối	1-2021-03286	GUANGDONG OPPO MOBILE; TELECOMMUNICATIONS CORP., LTD.

75	Phương pháp tạo khóa và thiết bị truyền thông	VN1-0045765-000	HUAWEI TECHNOLOGIES CO., LTD.
76	Quy trình xác thực định danh (ID) cho mạch tích hợp (IC) ứng dụng mạch tạo hàm không thể sao chép về vật lý (PUF)	VN1-0034677-000	Hoàng Văn Phúc Trịnh Quang Kiên Trần Văn Toàn
77	Máy chủ xử lý và phương pháp cung cấp bảo mật dữ liệu bằng cách sử dụng mã xác thực một chiều	1-2020-05743	VISA INTERNATIONAL SERVICE ASSOCIATION
78	Phương pháp mã hóa và giải mã nhờ xử lý đồng thời phần cứng và phần mềm sử dụng thuật toán xác thực và định danh AES-CCM	1-2021-01093	Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội
79	Phương pháp và hệ thống bảo mật thông tin cho camera	VN1-0044459-000	Trần Minh Sơn
80	Phương pháp và thiết bị phát hiện bảo mật mạng không dây	1-2020-06461	SHANGHAI LIANSHANG NETWORK TECHNOLOGY CO., LTD.
81	Phương pháp mã hoá, giải mã trên đường truyền từ máy chủ đến thiết bị cổng kết nối Internet vạn vật (IOTs - Internet of Things)	1-2020-05601	Sở Khoa học và Công nghệ thành phố Hồ Chí Minh
82	Phương pháp thu ký hiệu nhận dạng thiết bị, đầu cuối và thiết bị mạng	VN1-0035944-000	HUAWEI TECHNOLOGIES CO., LTD.
83	Thiết bị định tuyến tăng tốc bảo mật dùng phần cứng mảng phần tử logic người dùng có thể lập trình được (FPGA)	VN1-0037864-000	TRƯỜNG ĐẠI HỌC BÁCH KHOA - ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
84	Phương pháp bảo vệ bảo mật, thiết bị truyền thông, vật ghi máy tính đọc được và hệ thống truyền thông	VN1-0041909-000	HUAWEI TECHNOLOGIES CO., LTD.
85	Phương pháp bảo vệ tính toàn vẹn dữ liệu, thiết bị truyền thông và phương tiện đọc được bằng máy tính	1-2020-01309	HUAWEI TECHNOLOGIES CO., LTD.
86	Phương pháp và hệ thống quản lý bảo mật mạng, và thiết bị mạng	VN1-0041207-000	HUAWEI INTERNATIONAL PTE. LTD.
87	Phương pháp truyền thông không dây bằng thiết bị người dùng và chức năng neo bảo mật	VN1-0039785-000	QUALCOMM INCORPORATED
88	Phương pháp giám sát bảo mật trên mạng wifi	1-2020-01731	SHANGHAI ZHANGMEN SCIENCE AND TECHNOLOGY CO., LTD.
89	Phương pháp cung cấp dịch vụ xác thực người dùng, máy chủ web, và thiết bị đầu cuối người dùng	1-2020-00661	BC CARD CO., LTD.
90	Phương pháp cấp phép một hoặc nhiều quyền thao tác đối với dữ liệu biểu mẫu	VN1-0048105-000	CHENGDU QIANNIUCAO INFORMATION TECHNOLOGY CO., LTD

91	Phương pháp, thiết bị và hệ thống kích hoạt xác thực mạng, phương pháp kích hoạt việc xác thực, thiết bị mạng thứ nhất, thực thể chức năng bảo mật thứ nhất, thiết bị truyền thông, và phương tiện lưu trữ đọc được bởi máy tính	VN1-0047797-000	HUAWEI TECHNOLOGIES CO., LTD.
92	Phương pháp và thiết bị để xác minh bảo mật dựa trên dấu hiệu sinh trắc học	VN1-0042720-000	Advanced New Technologies Co., Ltd.
93	Phương pháp và thiết bị thu thập khóa, phương pháp xử lý bảo mật khi di chuyển thiết bị đầu cuối và thiết bị truyền thông	VN1-0040151-000	HUAWEI TECHNOLOGIES CO., LTD.
94	Hệ thống và phương pháp được thực hiện bởi máy tính để tăng cường tính bảo mật của hợp đồng thông minh, và phương tiện lưu trữ đọc được bởi máy tính không chuyển tiếp	1-2019-01969	ADVANCED NEW TECHNOLOGIES CO., LTD.
95	Phương pháp thực hiện bảo mật, thiết bị truyền thông và thiết bị lưu trữ không tạm thời	VN1-0044064-000	HUAWEI TECHNOLOGIES CO., LTD.
96	Phương pháp, thiết bị và hệ thống xử lý các mã vạch hai chiều	VN1-0031024-000	Advanced New Technologies Co., Ltd.
97	Phương pháp truyền thông, thiết bị truyền thông, phần tử mạng nút bảo mật và phương tiện lưu trữ đọc được bằng máy tính	1-2019-02287	HUAWEI TECHNOLOGIES CO., LTD.
98	Phương pháp xử lý mã kiểm chứng và thiết bị đầu cuối di động	VN1-0036546-000	HUAWEI TECHNOLOGIES CO., LTD.
99	Phương pháp sử dụng mật mã xác thực của giao thức dành riêng tài nguyên nhằm bảo mật đường truyền dịch vụ trong mô hình mạng riêng ảo	1-2019-02463	Tập đoàn Công nghiệp - Viễn thông Quân đội (VIETTEL)
100	Phương pháp, thiết bị và hệ thống truyền dữ liệu	VN1-0037703-000	ADVANCED NEW TECHNOLOGIES CO., LTD.
101	Phương pháp và thiết bị ngăn ngừa máy chủ không bị tấn công	VN1-0033781-000	Advanced New Technologies Co., Ltd.
102	Phương pháp và thiết bị bảo mật tính di động liên hệ thống	VN1-0045538-000	Nokia Technologies Oy
103	Hệ thống chuyển mạch dựa trên OpenFlow sử dụng phần cứng tái cấu hình	VN2-0003177-000	Trường Đại học Bách Khoa - Đại Học Quốc Gia TP.HCM
104	Phương pháp và hệ thống xác thực bảo mật, thiết bị người dùng, thực thể quản lý di động, máy chủ thuê bao tại nhà, và vật lưu trữ máy tính đọc được	1-2018-04394	HUAWEI TECHNOLOGIES CO., LTD.
105	Thiết bị và phương pháp xác thực tin nhắn và vật ghi	VN1-0036499-000	Nokia Technologies Oy

106	Phương pháp xác thực thanh toán và thiết bị xác thực thanh toán dùng cho thiết bị đầu cuối di động và thiết bị đầu cuối di động	1-2018-01331	Honor Device Co., Ltd.
107	Phương pháp và thiết bị xác minh	VN1-0036413-000	ADVANCED NEW TECHNOLOGIES CO., LTD.
108	Thành phần mạng và phương pháp bảo mật định tuyến nguồn sử dụng chữ ký số dựa trên khóa công khai và nút mạng	1-2016-03105	HUAWEI TECHNOLOGIES CO., LTD.
109	Lõi IP (Intellectual Property core) thực hiện giải mã mật mã dùng hệ mật mã khóa công khai RSA (Rivest - Shamir - Adleman) và hệ mật mã dòng ZUC (ZuChongzi) trong truyền dữ liệu video	2-2014-00293	Trường Đại học Khoa học Tự nhiên, ĐHQG-HCM Sở Khoa học Công nghệ TP. Hồ Chí Minh
110	Phương pháp nâng cao tính bảo mật và giảm các thao tác thực hiện để thanh toán giao dịch thương mại	VN2-0001563-000	Công ty Cổ phần Công nghệ và Dịch vụ Moca
111	Thiết bị USB an toàn dùng để lưu trữ dữ liệu an toàn, hạn chế lây lan vi rút	VN1-0016526-000	Viện Khoa học và Công nghệ Quân sự
112	Thiết bị và phương pháp tự xác thực	VN1-0026635-000	FAST AND SAFE TECHNOLOGY PRIVATE LIMITED
113	Hệ thống bảo mật vật lý và phương pháp chia sẻ dữ liệu trong hệ thống bảo mật vật lý	VN1-0021499-000	AVIGILON CORPORATION
114	Phương pháp và hệ thống điều khiển việc truy nhập vào mạng của các chương trình ứng dụng	VN1-0022067-000	Tencent Technology (Shenzhen) Company Limited
115	Thiết bị và phương pháp xác thực người dùng và hệ thống bảo mật	VN1-0018367-000	FORTICOM GROUP LTD.
116	Phương pháp ngăn chặn các chương trình ứng dụng xâm phạm quyền riêng tư và thiết bị di động	VN1-0023341-000	Tencent Technology (Shenzhen) Company Limited
117	Phương pháp chuyển ngữ cảnh bảo mật, trạm xa và vật ghi chứa mã thực hiện	1-2013-00174	QUALCOMM INCORPORATED
118	Phương pháp xác thực hoạt động trong thiết bị và thiết bị xác thực	VN1-0025153-000	QUALCOMM INCORPORATED
119	Phương pháp và thiết bị bảo vệ theo thời gian thực	VN1-0019114-000	Tencent Technology (Shenzhen) Company Limited
120	Phương pháp thiết lập ngữ cảnh bảo mật và trạm xa	VN1-0018827-000	QUALCOMM INCORPORATED
121	Phương pháp và thiết bị vận hành ở nút chuyển tiếp	VN1-0018159-000	QUALCOMM INCORPORATED
122	Phương pháp và thiết bị kiểm tra mật khẩu động	VN1-0015929-000	Tencent Technology (Shenzhen) Company Limited

123	Phương pháp, thiết bị phân loại và xử lý dữ liệu trong hệ thống tin nhắn nhanh	VN1-0009811-000	Tencent Technology (Shenzhen) Company Limited
124	Phương pháp và thiết bị cho quá trình xác thực tương hỗ	VN1-0010307-000	Qualcomm Incorporated
125	Phương pháp hình thành và kiểm tra chữ ký số tập thể dựa trên đường cong elliptic, để chứng thực các văn bản điện tử	VN1-0008702-000	Nguyễn Hiếu Minh
126	Phương pháp và thiết bị xác thực trong hệ thống truyền thông	VN1-0009634-000	NOKIA TECHNOLOGIES OY
127	Hệ thống ngăn chặn gian lận cho điện thoại thanh toán khai thác trong mạng điện thoại	1-2007-01121	TELEKOM MALAYSIA BERHAD
128	Phương pháp nhập thông tin để bảo mật thông tin nhập vào	1-2006-02171	PARK, SEUNG-BAE
129	Bộ linh kiện với kết nối tín hiệu nguồn	VN1-0007586-000	INTEL CORPORATION
130	Hệ thống và phương pháp điều khiển việc truyền thông tin giữa máy thu và môđun bảo mật	VN1-0003465-000	NAGRACARD S.A.
131	Phương pháp sử dụng an toàn các chữ ký dạng số trong hệ thống mật mã thương mại	VN1-0002134-000	CERTCO, LLC

Phụ lục 3

MỘT SỐ SẢN PHẨM CÔNG NGHỆ AN NINH MẠNG ĐANG ĐƯỢC THƯƠNG MẠI HÓA TẠI VIỆT NAM

STT	Tên công nghệ	Lĩnh vực công nghệ	Tên doanh nghiệp
1	Nền tảng an ninh mạng CyStack Platform	Bảo mật Đám mây (Cloud Security)	Công ty Cổ phần CyStack Việt Nam
2	Trung tâm phần mềm và giải pháp an ninh mạng - Đại học Bách Khoa Hà Nội	Bảo mật mạng (Network Security)	Trung tâm phần mềm và giải pháp an ninh mạng - Đại học Bách Khoa Hà Nội
3	Giải pháp ảo háo máy tính để bàn Viettel Cloud Desktop (DaaS)	Bảo mật Đám mây (Cloud Security)	Viettel TP. HCM - Chi nhánh Tập đoàn Công nghiệp - Viễn thông Quân đội
4	Hệ thống kiểm soát vào ra	Quản lý Danh tính và Truy cập (Identity and Access Management - IAM)	KPS Việt Nam
5	Giải pháp an ninh thông minh Smartlook tích hợp công nghệ trí tuệ nhân tạo AI cho nhà máy/doanh nghiệp sản xuất	Bảo mật IoT/OT (Internet of Things/ Operational Technology Security)	Công ty TNHH Hệ thống Thông minh (SmartSys)
6	Giải pháp Trung Tâm Điều Hành An Ninh	Tình báo Đe dọa và Phân tích (Threat Intelligence & Analytics)	Chi Nhánh Công ty Cổ phần Tư vấn Chuyển giao công Nghệ ITC
7	Cổng an ninh thư viện thông minh INNO SG1356A	Quản lý Danh tính và Truy cập (Identity and Access Management - IAM)	Công ty TNHH Điện tử Công nghệ INNO Việt Nam
8	Phần mềm trung tâm an ninh PSafe-C3-Center	Quản lý Danh tính và Truy cập (Identity and Access Management - IAM) Bảo mật IoT/OT (Internet of Things/ Operational Technology Security)	Công ty Cổ phần Giải pháp Công nghệ Trực tuyến GTEL OTS
9	Phần mềm giám sát an ninh ngân hàng	Quản lý Danh tính và Truy cập (Identity and Access Management - IAM)	Công ty cổ phần HC-HiTeck
10	Cổng an ninh thư viện ứng dụng công nghệ RFIDCổng an ninh thư viện ứng dụng công nghệ RFID	Quản lý Danh tính và Truy cập (Identity and Access Management - IAM)	Công ty Cổ phần Dịch vụ Thương mại và Thông tin Kỹ thuật

11	Hệ thống kiểm soát an ninh tòa nhà	Quản lý Danh tính và Truy cập (Identity and Access Management - IAM)	Công ty Cổ phần Công Nghệ LogicBUY
12	Cổng an ninh ứng dụng công nghệ RFID Diamond™	Quản lý Danh tính và Truy cập (Identity and Access Management - IAM)	Công ty TNHH Nam Hoàng
13	Giải pháp giám sát an ninh từ xa	Quản lý Danh tính và Truy cập (Identity and Access Management - IAM)	Công ty cổ phần HC-HiTeck
14	Giải pháp kiểm soát an ninh ra vào Access Control	Quản lý Danh tính và Truy cập (Identity and Access Management - IAM)	Công ty TNHH Hệ thống Thông minh (SmartSys)
15	Cổng an ninh thư viện ứng dụng công nghệ RFIDCổng an ninh thư viện ứng dụng công nghệ EM	Quản lý Danh tính và Truy cập (Identity and Access Management - IAM)	Công ty TNHH Nam Hoàng
16	Giải pháp an ninh cho nhà máy sản xuất công nghiệp 5.0	Quản lý Danh tính và Truy cập (Identity and Access Management - IAM)	Công ty Cổ phần Công nghệ Biển Bạc Miền Nam
17	Cổng an ninh thư viện công nghệ sóng vô tuyến RFID Lyngsoe gates -PG45I	Quản lý Danh tính và Truy cập (Identity and Access Management - IAM)	Công ty Cổ phần Thông tin và công nghệ số
18	Cổng an ninh thư viện công nghệ sóng vô tuyến RFID Lyngsoe gates -PG50	Quản lý Danh tính và Truy cập (Identity and Access Management - IAM)	Công ty Cổ phần Thông tin và công nghệ số
19	Giải pháp bảo mật, kiểm tra rò rỉ thông tin, bảo vệ bản quyền số bằng XTI SOCRadar	Tình báo Đe dọa và Phân tích (Threat Intelligence & Analytics)	Công ty TNHH Thương mại và Công nghệ MVTECH
20	Mạng WAN ảo lưu trữ và bảo mật dữ liệu Viettel SD-WAN	Bảo mật Hạ tầng mạng (Network Security)	Viettel TP. HCM - Chi nhánh Tập đoàn Công nghiệp - Viễn thông Quân đội
21	Nền tảng giúp phát hiện và ngăn chặn tội phạm mạng ActiveFence	Tình báo Đe dọa và Phân tích (Threat Intelligence & Analytics)	Phòng Kinh tế & Thương mại - Đại sứ quán Israel
22	Giải pháp đám mây kết nối mạng chuyên biệt Viettel Hybrid Connect	Bảo mật Đám mây (Cloud Security)	Viettel TP. HCM - Chi nhánh Tập đoàn Công nghiệp - Viễn thông Quân đội
23	Bizfly VPN - Dịch vụ kết nối mạng riêng ảo an toàn, tốc độ cao	Bảo mật Hạ tầng mạng (Network Security)	Công ty Cổ phần VCCorp

24	Giải pháp chống tấn công mạng cho hệ thống đám mây Viettel Cloudrity (vCloudrity)	Bảo mật Dữ liệu (Data Security)	Viettel TP. HCM - Chi nhánh Tập đoàn Công nghiệp - Viễn thông Quân đội
25	Thiết bị bảo mật mạng - Radware Defense Pro	Bảo mật Hạ tầng mạng (Network Security)	Chi Nhánh Công ty Cổ phần Tư vấn Chuyển giao công Nghệ ITC
26	Phần mềm cấp phép & kiểm soát vào ra IOPermit	Quản lý Danh tính và Truy cập (Identity and Access Management - IAM)	Công ty Cổ phần IDTEK
27	Giải pháp VNPT DNS Protection	Bảo mật Hạ tầng mạng (Network Security)	Tổng Công ty Dịch vụ Viễn thông VNPT VinaPhone
28	Web Application Firewall (vWAF) - Dịch vụ tường lửa ứng dụng web	Bảo mật Hạ tầng mạng (Network Security)	VNG Cloud
29	Giải pháp chữ ký số Viettel CA	Quản lý Danh tính và Truy cập (Identity and Access Management - IAM) Bảo mật Dữ liệu (Data Security)	Viettel TP. HCM - Chi nhánh Tập đoàn Công nghiệp - Viễn thông Quân đội
30	Phần mềm quản lý tài sản cố định SIMPLY Fixed Asset	Quản lý Danh tính và Truy cập (Identity and Access Management - IAM) Bảo mật Dữ liệu (Data Security)	Công Ty TNHH Giải Pháp Phần Mềm Thiên Long
31	Giải pháp máy chủ bảo mật Viettel Server Leasing	Bảo mật Hạ tầng mạng (Network Security) Bảo mật Dữ liệu (Data Security)	Viettel TP. HCM - Chi nhánh Tập đoàn Công nghiệp - Viễn thông Quân đội
32	Hệ thống nhận dạng khuôn mặt FACE-RS	Quản lý Danh tính và Truy cập (Identity and Access Management - IAM) Bảo mật Dữ liệu (Data Security)	Công ty cổ phần HC-HiTeck
33	Hệ thống truyền thông và thông báo nội bộ TASKEN EMS	Quản lý Danh tính và Truy cập (Identity and Access Management - IAM) Bảo mật Dữ liệu (Data Security)	Công ty TNHH OPUS SOLUTION
34	FPT Virtual Private Cloud	Bảo mật Đám mây (Cloud Security)	Công ty TNHH FPT Smart Cloud
35	Giải pháp Blockchain ứng dụng trong kinh tế chia sẻ	Quản lý Danh tính và Truy cập (Identity and Access Management - IAM) Bảo mật Dữ liệu (Data Security)	Công ty Cổ phần Vietnam Blockchain

36	Giải pháp quản lý định danh và truy cập tập trung Identity & Access management (IAM)	Quản lý Danh tính và Truy cập (Identity and Access Management - IAM)	Công ty Cổ phần Dịch vụ Công nghệ Tin học HPT
37	Giải pháp tường lửa thế hệ mới FPT Next-Gen Firewall	Bảo mật Hạ tầng mạng (Network Security) Bảo mật Dữ liệu (Data Security)	Công ty TNHH FPT Smart Cloud
38	Hệ thống phần mềm chính phủ điện tử Worldsoft E-Government	Bảo mật Hạ tầng mạng (Network Security) Bảo mật Dữ liệu (Data Security)	Công ty CP WORLDSOFT
39	Camera AI nhận diện thông minh	Bảo mật Hạ tầng mạng (Network Security) Bảo mật Dữ liệu (Data Security)	Công ty CP Ứng dụng Di động Xanh
40	Phần mềm nhận dạng khuôn mặt AI	Quản lý Danh tính và Truy cập (Identity and Access Management - IAM)	Công ty Cổ phần Công nghệ Biển Bạc Miền Nam
41	Giải Pháp Nhận Diện Khuôn Mặt Ứng Dụng Công Nghệ AI	Quản lý Danh tính và Truy cập (Identity and Access Management - IAM)	Công Ty TNHH Công Nghệ MIND
42	Phần mềm chống mã độc Lock PC	Bảo mật Ứng dụng (Application Security)	Công ty TNHH Đảm bảo an toàn thông tin Việt Kiến Tạo
43	Giải pháp bảo vệ toàn diện cho các thiết bị đầu cuối Viettel Endpoint Security	Bảo mật Thiết bị đầu cuối (Endpoint Security)	Viettel TP. HCM - Chi nhánh Tập đoàn Công nghiệp - Viễn thông Quân đội
44	Giải pháp truy xuất nguồn gốc dựa trên công nghệ Blockchain phù hợp với tiêu chuẩn GS1	Quản lý Danh tính và Truy cập (Identity and Access Management - IAM)	Công ty Cổ phần Vietnam Blockchain
45	Giải pháp camera đám mây Viettel Cloud Camera	Bảo mật Đám mây (Cloud Security)	Viettel TP. HCM - Chi nhánh Tập đoàn Công nghiệp - Viễn thông Quân đội
46	Phần mềm tự động hóa quản lý giáo dục WEONE	Quản lý Danh tính và Truy cập (Identity and Access Management - IAM)	Công ty Cổ phần Đầu tư Thương mại và Phát triển Công nghệ FSI
47	Giải pháp giải pháp ảo hóa máy trạm	Bảo mật Đám mây (Cloud Security)	Viettel TP. HCM - Chi nhánh Tập đoàn Công nghiệp - Viễn thông Quân đội
48	Chứng thư số Viettel SSL	Bảo mật Dữ liệu (Data Security)	Viettel TP. HCM - Chi nhánh Tập đoàn Công nghiệp - Viễn thông Quân đội

49	Giải pháp lưu trữ thư điện tử bảo mật cao Viettel Email Hosting	Bảo mật Dữ liệu (Data Security)	Viettel TP. HCM - Chi nhánh Tập đoàn Công nghiệp - Viễn thông Quân đội
50	Giải pháp lưu trữ dữ liệu website Viettel Web Hosting	Bảo mật Đám mây (Cloud Security)	Viettel TP. HCM - Chi nhánh Tập đoàn Công nghiệp - Viễn thông Quân đội
51	Giải pháp Viettel Blockchain Node	Bảo mật Dữ liệu (Data Security) Công nghệ Blockchain	Viettel TP. HCM - Chi nhánh Tập đoàn Công nghiệp - Viễn thông Quân đội
52	Thiết bị bảo mật - Checkpoint Security Gateway	Bảo mật Hạ tầng mạng (Network Security)	Chi Nhánh Công ty Cổ phần Tư vấn Chuyển giao công Nghệ ITC
53	Hệ thống bảo mật KODIAK-APS series	Bảo mật Hạ tầng mạng (Network Security)	Công ty Cổ phần BSR Việt Nam
54	Phần mềm bảo mật phòng thí nghiệm Enhanced Data Security	Bảo mật Dữ liệu (Data Security)	Công ty Malvern Panalytical
55	Giải pháp bảo mật Oracle Audit Vault	Bảo mật Dữ liệu (Data Security)	Công ty Cổ phần Dịch vụ Công nghệ Tin học HPT
56	Giải pháp bảo mật Oracle Advanced Security	Bảo mật Dữ liệu (Data Security)	Công ty Cổ phần Dịch vụ Công nghệ Tin học HPT
57	Giải pháp bảo mật tự động Swimlane SOAR	Bảo mật Hạ tầng mạng (Network Security)	Công ty CP Giải Pháp Công Nghệ Lạc Hồng
58	Giải pháp bảo mật Oracle Database Vault	Bảo mật Dữ liệu (Data Security)	Công ty Cổ phần Dịch vụ Công nghệ Tin học HPT
59	Giải pháp tối ưu vận hành và bảo mật cho Multi cloud CloudSuite	Bảo mật Đám mây (Cloud Security)	Công ty TNHH Phần mềm FPT
60	Giải pháp bảo mật website all-in-one trên nền tảng đám mây Reblaze	Bảo mật Đám mây (Cloud Security)	Phòng Kinh tế & Thương mại - Đại sứ quán Israel