CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày tháng năm 2020

BÁO CÁO KẾT QUẢ TỰ ĐÁNH GIÁ NHIỆM VỤ KHOA HỌC VÀ CÔNG NGHỆ CẤP QUỐC GIA

I. Thông tin chung về nhiệm vụ:

1. Tên nhiệm vụ, mã số:

Nghiên cứu, phát triển tích hợp hệ thống hỗ trợ giám sát, quản lý, vận hành an toàn cho hệ thống mạng và hạ tầng cung cấp dịch vụ công trực tuyến

Mã số đề tài, dự án: KC.01.01/16-20

Thuộc:

- Chương trình: Chương trình khoa học và công nghệ trọng điểm cấp quốc gia giai đoạn 2016-2020: "Nghiên cứu các công nghệ và phát triển sản phẩm công nghệ thông tin phục vụ Chính phủ điện tử", Mã số: KC.01/16-20

- Khác *(ghi cụ thể)*:

2. Mục tiêu nhiệm vụ:

Đề tài có định hướng mục tiêu: Làm chủ công nghệ chế tạo thiết bị phần cứng, phát triển phần mềm chuyên dụng, tích hợp hệ thống hỗ trợ giám sát, quản lý, đảm bảo vận hành an toàn và an ninh thông tin cho các hệ thống mạng và hạ tầng cung cấp dịch vụ công trực tuyến tại các cơ quan nhà nước.

Các mục tiêu cụ thể của đề tài như sau:

- **Nghiên cứu, chế tạo thiết bị phần cứng chuyên dụng** (Tủ mạng thông minh): Thiết bị có khả năng tự động giám sát môi trường vận hành (nhiệt độ, độ ẩm) của tủ mạng và các thiết bị. Trên mỗi tủ sẽ được trang bị một máy chủ tích hợp phần mềm chuyên dụng (Rack Controller) hỗ trợ (1) Thu thập thông tin từ các thiết bị mạng và máy trạm đầu cuối; (2) Phát hiện và xử lý các lỗi mạng vật lý như tràn cổng, đứt cáp, thiết bị không hoạt động; (3) Giao tiếp thông tin, nhận lệnh điều khiển từ máy chủ khu vực, thực hiện cấu hình/cấu hình lại thiết bị mạng trong phạm vi quản lý; và (4) Khai thác hiệu quả kênh truyền dự phòng. Yêu cầu đặt ra đối với thiết bị phần cứng chuyện dụng là cung cấp cảnh báo đến máy chủ khu vực trong vòng 60 giây về các sự cố mạng liên quan đến môi trường vận hành. Hai thiết bị phần cứng chuyên dụng cho phép quản lý 1000 thiết bị vật lý kết nối trong mạng. Thông tin truyền và gửi đều được mã hóa để đảm bảo vấn đề an ninh và bảo mật.

- **Nghiên cứu, xây dựng hệ thống giám sát tại máy chủ khu vực**: Chức năng của máy chủ khu vực gồm tiếp nhận dữ liệu nhận được từ Rack Controller, giải mã và tổ chức lưu trữ. Một sự thay đổi được chúng tôi đề xuất so với yêu cầu ban đầu đó chính là việc đặt mô-đun quản lý truy cập tại máy chủ khu vực. Điều này cho phép công việc quản trị được linh hoạt và phù hợp với đặc thù của từng đơn vị trong cơ quan Bộ. Mô-đun cảnh báo bất thường được phát triển dựa trên phân tích và mô hình hóa hành vi của người sử dụng dịch vụ công trực tuyến, phân tích khả năng xuất hiện mã độc tấn công xâm nhập mạng. Trên cơ sở phân tích và báo cáo nhận được liên quan đến sự cố, máy chủ khu vực phát lệnh điều khiển tới Rack Controller để xử lý hoặc cách ly các phân vùng bị tấn công. Một nhiệm vụ khác của máy chủ khu vực chính là tổng hợp và gửi báo cáo về máy chủ trung tâm. Nó cũng cung cấp giao diện để hiển thị tình trạng hoạt động, trạng thái kết nối, thông lượng của hệ thống đặt tại máy chủ khu vực.

- **Nghiên cứu, xây dựng hệ thống giám sát tại máy chủ trung tâm**: Chức năng máy chủ trung tâm là giữ vai trò thực hiện giám sát toàn bộ tổ chức. Nó thực hiện liên kết các máy chủ khu vực, cung cấp thông tin giám sát, quản lý tổng hợp toàn bộ hệ thống mạng. Hệ thống tại máy chủ trung tâm cũng hỗ trợ thống kê báo cáo về trạng thái hạ tầng CNTT và sẵn sàng liên thông với các hệ thống mạng khác khi có yêu cầu.

3. Chủ nhiệm nhiệm vụ:

Họ và tên: Trần Quang Đức

Ngày, tháng, năm sinh: 16/04/1982 Nam/ Nữ: Nam

Học hàm, học vị: TS

Chức danh khoa học: Giảng viên Chức vụ:

Điện thoại: Tổ chức: 024.3869 2463 Mobile: 0942481255

Fax: 024.3869 2406 E-mail: ductq@hust.edu.vn

Tên tổ chức đang công tác: Viện Công nghệ thông tin và Truyền thông

Địa chỉ tổ chức: Nhà B1, Số 1 Đại Cồ Việt, Hai Bà Trưng, Hà Nội

Địa chỉ nhà riêng: P. 1711, CC. 170 Đê La Thành, Đống Đa, Hà Nội

4. Tổ chức chủ trì nhiệm vụ:

Tên tổ chức chủ trì đề tài: Viện Công nghệ thông tin và Truyền thông

Điện thoại: 024.3869 2463 Fax: 024.3869 2406

Website: https://soict.hust.edu.vn

Địa chỉ: Nhà B1, Số 1 Đại Cồ Việt, Hai Bà Trưng, Hà Nội

Họ và tên thủ trưởng tổ chức: PGS. TS. Tạ Hải Tùng

Số tài khoản: 3713.0.9081584.00000

Kho bạc nhà nước Hai Bà Trưng, Hà Nội

Tên cơ quan chủ quản đề tài: Viện Công nghệ thông tin và Truyền thông

5. Tổng kinh phí thực hiện: 5.100 triệu đồng.

Trong đó, kinh phí từ ngân sách SNKH: 5.100 triệu đồng.

Kinh phí từ nguồn khác: 0 triệu đồng.

6. Thời gian thực hiện theo Hợp đồng:

Bắt đầu: 10/2017

Kết thúc: 9/2019

Thời gian thực hiện theo văn bản điều chỉnh của cơ quan có thẩm quyền: 12/2019

7. Danh sách thành viên chính thực hiện nhiệm vụ nêu trên gồm:

Số TT	Họ và tên	Chức danh khoa học, học vị	Cơ quan công tác
1	Trần Quang Đức	TS	Viện CNTT&TT
2	Trần Hải Anh	TS	Viện CNTT&TT
3	Hà Quốc Trung	PGS. TS	Trung tâm CNTT, Bộ KHCN
4	Nguyễn Ngọc Hóa	PGS. TS	Trường ĐHCN, ĐHQGHN
5	Nguyễn Hải Châu	PGS. TS	Trường ĐHCN, ĐHQGHN
6	Trần Hoàng Hải	TS	Viện CNTT&TT
7	Nguyễn Linh Giang	PGS. TS	Viện CNTT&TT
8	Ngô Lam Trung	TS	Viện CNTT&TT
9	Chu Văn Quang	ThS	Trung tâm CNTT, Bộ KHCN
10	Bùi Trọng Tùng	ThS	Viện CNTT&TT

II. Nội dung tự đánh giá về kết quả thực hiện nhiệm vụ:

1. Về sản phẩm khoa học:

1.1. Danh mục sản phẩm đã hoàn thành:

Số TT	Tên sản phẩm	Số lượng			Chất lượng		
		Xuất sắc	Đạt	Không đạt	Xuất sắc	Đạt	Không đạt
1	Thiết bị phần cứng		X			Đáp ứng đầy đủ yêu cầu	

	chuyên dụng có khả năng giám sát, quản lý hệ thống mạng (cáp và các thiết bị mạng)					chất lượng đã đặt ra; gồm tủ mạng thông minh tự động giám sát trạng thái vận hành (nhiệt độ, độ ẩm) của các thiết bị mạng và máy chủ đảm nhiệm chức năng Rack Controller.	
2	Máy chủ khu vực (*hệ thống phần mềm*)		X			Đã xây dựng được hệ thống phần mềm tại máy chủ khu vực đáp ứng đầy đủ yêu cầu đã đặt ra, gồm: - Quản lý, giám sát các cổng chuyển mạch của tất cả các thiết bị phần cứng chuyên dụng; tiếp nhận thông tin, chuyển lệnh điều khiển tới các thiết bị phần cứng chuyên dụng; - Thu thập thông tin từ các kết nối vật lý, thiết bị mạng, dịch vụ công trực tuyến; giám sát theo thời gian thực, phân tích hành vi, tự động sinh tập luật sử dụng trí tuệ nhân tạo và học máy để phát hiện bất thường và tấn công xâm nhập mạng; - Cảnh bảo sự cố, xử lý, giảm thiểu ảnh hưởng của tấn công; - Hỗ trợ giám sát tính sẵn sàng của các dịch vụ trực tuyến; - Trực quan hoá tôpô mạng, lưu đồ trạng thái kết nối, băng thông các cổng mạng.	
3	Máy chủ trung tâm (*hệ thống phần mềm*)		X			Đã xây dựng được hệ thống phần mềm tại máy chủ trung tâm đáp ứng đầy đủ	

						yêu cầu đã đặt ra, gồm: - Liên kết các máy chủ khu vực, cung cấp thông tin giám sát, quản lý tổng hợp của toàn bộ hệ thống mạng; - Hỗ trợ quản lý tập trung và phân quyền; giám sát truy cập của người sử dụng dựa trên các cơ chế xác thực; - Hỗ trợ thống kê, báo cáo về trạng thái hạ tầng CNTT được giám sát, quản lý; - Sẵn sàng liên thông với các hệ thống mạng khác khi có yêu cầu.	
4	Tài liệu đặc tả về giải pháp, kiến trúc hệ thống tích hợp đa tầng bao gồm phần cứng và phần mềm		X			Đã đáp ứng đầy đủ yêu cầu khoa học đặt ra trong tài liệu này.	
5	Thuyết minh thiết kế chi tiết hệ thống tích hợp, bao gồm phần cứng và phần mềm		X			Đã đáp ứng đầy đủ yêu cầu khoa học đặt ra trong thuyết minh này.	
6	Báo cáo đánh giá kết quả triển khai thử nghiệm tại ít nhất 01 trụ sở cơ quan bộ, ngành, ủy ban nhân dân tỉnh, thành phố trực thuộc trung ương		X			Đã đáp ứng đầy đủ yêu cầu khoa học đặt ra trong báo cáo này.	
7	Báo cáo tổng kết đề tài và báo cáo tóm tắt		X			Đã tổng hợp được toàn bộ những kết quả, cả về lý thuyết lẫn sản phẩm phần cứng, phần mềm đã đạt được trong đề tài.	
8	Báo cáo thuyết minh thiết bị phần cứng chuyên dụng	X				Đã mô tả chi tiết thiết bị phần cứng chuyên dụng.	
9	Tài liệu hướng dẫn	X				Đã mô tả chi tiết hướng dẫn	

	sử dụng, vận hành, khai thác hệ thống phần mềm tại máy chủ khu vực					sử dụng, vận hành và khai thác hệ thống phần mềm tại máy chủ khu vực.	
10	Tài liệu hướng dẫn sử dụng, vận hành, khai thác hệ thống phần mềm tại máy chủ trung tâm	X				Đã mô tả chi tiết hướng dẫn sử dụng, vận hành và khai thác hệ thống phần mềm tại máy chủ trung tâm.	
11	Bài báo tạp chí khoa học	X (4)			02 bài ISI/ Scopus 02 bài tạp chí trong nước		
12	Bài báo hội nghị khoa học	X (3)			3 bài quốc tế WoS/ Scopus		
13	Đào tạo thạc sỹ	X			X		
14	Tiến sỹ (tham gia đào tạo)		X			X	
15	Bằng độc quyền sáng chế	X				X	

(chi tiết tham khảo thêm trong Báo cáo tổng kết đề tài)

1.2. Danh mục sản phẩm khoa học dự kiến ứng dụng, chuyển giao (nếu có):

Số TT	**Tên sản phẩm**	**Thời gian dự kiến ứng dụng**	**Cơ quan dự kiến ứng dụng**	**Ghi chú**
1	Hệ thống hỗ trợ giám sát, quản lý, vận hành an toàn cho hệ thống mạng và hạ tầng cung cấp dịch vụ công trực tuyến	2020	Bộ Khoa học và Công nghệ, Bộ Thông tin và Truyền thông, Trường Đại học Bách khoa Hà Nội	Hệ thống cần được thiết lập cấu hình và hiệu chỉnh để phù hợp với môi trường triển khai thực tế

1.3. Danh mục sản phẩm khoa học đã được ứng dụng *(nếu có)*:

Số TT	Tên sản phẩm	Thời gian ứng dụng	Tên cơ quan ứng dụng	Ghi chú
...				

2. Về những đóng góp mới của nhiệm vụ:

Trong lĩnh vực KHCN, đề tài có tác động và mạng lại lợi ích đối với ngành mạng máy tính, truyền thông dữ liệu, khoa học máy tính và an toàn thông tin. Những đóng góp cụ thể của đề tài gồm:

- Đề xuất mô hình và triển khai tích hợp hệ thống giám sát tổng thể bao gồm thiết bị phần cứng chuyên dụng, hệ thống phần mềm tại máy chủ khu vực và hệ thống phần mềm tại máy chủ trung tâm. Hệ thống được thiết kế theo kiến trúc đa tầng, hướng dịch vụ, khả mở để phù hợp với thực tế triển khai tại các bộ, ngành. Hệ thống cũng cung cấp bộ thư viện hỗ trợ liên thông với hệ thống khác trong Chính phủ điện tử. Bộ thư viện gồm tập hợp các API được viết theo chuẩn RESTful và được khuyến nghị áp dụng tại tiểu mục 1.15 trong mục III Tiêu chuẩn kỹ thuật ứng dụng CNTT thuộc Khung tham chiếu CPĐT Việt Nam;

- Đề xuất và triển khai cơ chế thu thập và phân tích thông tin dựa trên SNMP Trap phục vụ phát hiện nhanh sự cố liên quan đến tràn cổng, đứt cáp, thiết bị mạng không hoạt động với hiệu năng và độ chính xác cao;

- Xây dựng và tích hợp thuật toán xử lý dữ liệu cấu trúc có khả năng phát hiện chính xác các liên kết và tự động xây dựng sơ đồ hình trạng mạng để quản trị viên có thể tương tác, thực hiện cấu hình và có cái nhìn tổng thể về toàn bộ hạ tầng công nghệ thông tin của đơn vị;

- Triển khai tích hợp bộ giải pháp bảo vệ máy chủ cung cấp dịch vụ công trực tuyến gồm (1) phần mềm dò quét lỗ hổng cấu hình máy chủ và mã nguồn của dịch vụ, (2) phân hệ phát hiện mã độc trong tệp tin văn bản với o-checker, và (3) phần mềm tường lửa lớp ứng dụng dựa trên học máy thống kê, mô hình hóa hành vi truy vấn của người dùng với độ chính xác 94,67%;

- Đề xuất và xây dựng phân hệ phát hiện mã độc dựa trên tên miền do mã độc sinh ra với độ chính xác 98,42% và có thể hoạt động theo thời gian thực. Phân hệ kết hợp phương pháp Long Short-Term Memory (LSTM) và hàm chi phí, trong đó giá trị chi phí được tính toán theo số lượng mẫu tên miền độc hại

có trong cơ sở dữ liệu. Phương pháp đa trở thành tiêu chuẩn đối sánh tại nhiều công trình nghiên cứu khác nhau, đồng thời cũng được mở rộng với mô hình học tăng cường và ứng dụng trong phát hiện thiết bị bị nhiễm mã độc;

- Tích hợp phân hệ quản trị người dùng tập rung với cơ chế phân quyền theo vai Role Based Access Control (RBAC) và Domain Controller. Thông qua phân hệ, quản trị viên có thể gửi lệnh điều khiển và tương tác trực tiếp với hệ thống Mail Exchange để cài đặt một số cấu hình quan trọng như kiểm soát nội dung, chống thư rác, lưu trữ và phân phối thư điện tử một cách an toàn và tin cậy;

Những đóng góp mới của nhiệm vụ được cụ thể hóa với 07 bài báo khoa học trong các tạp chí và hội nghị có uy tín thuộc lĩnh vực công nghệ thông tin (01 SCIE-Q1, 01 Scopus, 03 WoS/Scopus, 02 tạp chí trong nước) và 01 Bằng độc quyền sáng chế được chấp nhận đơn hợp lệ theo Quyết định số 100499/QĐ-SHTT vào ngày 12/11/2019. Bên cạnh đó, đề tài cũng tham gia đào tạo 02 tiến sỹ và đào tạo 04 thạc sỹ thuộc nhóm ngành Công nghệ thông tin, chuyên ngành mạng máy tính và an toàn thông tin.

3. Về hiệu quả của nhiệm vụ:

3.1. Hiệu quả kinh tế

Các cơ quan, tổ chức nhà nước có thể tích hợp sản phẩm của đề tài để hỗ trợ giám sát mạng, quản lý đảm bảo an toàn hệ thống mạng và hạ tầng kỹ thuật của các dịch vụ công trực tuyến trong các phạm vi khác nhau nhưng vẫn luôn đảm bảo được tính đồng bộ và tập trung. Đối với nhà quản lý, hệ thống cung cấp báo cáo trực quan về hoạt động của hệ thống công nghệ thông tin, làm cơ sở để lên kế hoạch nâng cấp hạ tầng thiết bị, dịch vụ mạng cần thiết, tránh đầu tư dàn trải. Đối với quản trị viên, hệ thống là công cụ quản trị với đầy đủ các tính năng gồm thu thập thông tin, đánh giá tình trạng vận hành hạ tầng thiết bị, hỗ trợ khắc phục sự cố mạng, xác định và cô lập phân vùng bị tấn công mã độc, tấn công xâm nhập mạng.

Sản phẩm của đề tài được phát triển dựa trên phần mềm mã nguồn mở kết hợp với nhiều công nghệ tiên tiến như học máy thống kê, trí tuệ nhân tạo, có chi phí thấp và đáp ứng nhiều chức năng tương đương với giải pháp thương mại khác. Mặc khác, do sản phẩm của đề tài tương thích và hoạt động tốt với rất nhiều các thiết bị mạng phổ biến hiện nay nên khi triển khai không cần thay đổi toàn bộ hệ thống hiện trạng, không cần chi phí xây dựng hệ thống mới.

3.2. Hiệu quả xã hội

Kết quả nghiên cứu của đề tài có những tác động tích cực tới những lĩnh vực quan trọng, cung cấp giải pháp tiên tiến để nâng cao khả năng quản lý, giám sát và vận hành, bảo đảm an toàn thông tin. Đối với các cơ quan tổ chức nhà nước, việc ứng dụng CNTT vào trong việc quản lý và thực hiện các thủ tục hành chính công có ý nghĩa rất quan trọng. Tăng cường sự quản lý, giám sát cho phép hệ thống công nghệ thông tin của tổ chức đáp ứng được các tiêu chuẩn khắt khe về vấn đề an toàn và bảo mật thông tin với các dữ liệu và thông tin nhạy cảm của các cơ quan tổ chức nhà nước. Việc liên kết và quản lý một cách đồng bộ các hệ thống này sẽ giúp tinh giảm bộ máy nhà nước, tiến tới xây dựng thành công Chính phủ điện tử.

Đối với người dân, doanh nghiệp, việc triển khai và đảm bảo được hoạt động ổn định của các dịch vụ hành chính công trực tuyến sẽ giúp giảm thiểu rất nhiều các thủ tục hành chính phức tạp, tạo sự đơn giản thuật lợi, nhanh chóng cho người dân và doanh nghiệp khi làm các thủ tục hành chính. Từ đó sẽ cải thiện được hệ thống hành chính, môi trường kinh doanh, tăng cường tính thu hút đầu tư đối với các doanh nghiệp và tổ chức nước ngoài.

Kết quả nghiên cứu của đề tài hiện đã được triển khai thử nghiệm tại Trung tâm Công nghệ thông tin, Bộ Khoa học và Công nghệ và Trung tâm thông tin, Bộ Thông tin và Truyền thông. Ngoài địa chỉ ứng dụng trên, với mô hình và các chức năng được xây dựng bám sát tổ chức và hoạt động thực tiễn tại các Bộ/Ngành/Tỉnh/Thành, sản phẩm của đề tài hoàn toàn có thể mở rộng, triển khai trên nhiều đơn vị quản lý nhà nước khác tại cả 63 tỉnh/thành lẫn 22 bộ/ngành trên cả nước sau khi được nghiệm thu, phê duyệt kết quả của đề tài.

Kết quả của đề tài cũng được cụ thể hóa thông qua hoạt động đào tạo nguồn nhân lực chất lượng cao trong các lĩnh vực tiên tiến, có tiềm năng ứng dụng như hệ thống giám sát mạng, kiểm soát truy cập và lĩnh vực đặc biệt quan trọng như an toàn bảo mật thông tin.

III. Tự đánh giá, xếp loại kết quả thực hiện nhiệm vụ

1. Về tiến độ thực hiện: *(đánh dấu √ vào ô tương ứng*):

- *Nộp hồ sơ đúng hạn* ☒
- *Nộp chậm từ trên 30 ngày đến 06 tháng* ☐
- *Nộp hồ sơ chậm trên 06 tháng* ☐

2. Về kết quả thực hiện nhiệm vụ:

- *Xuất sắc* ☐
- *Đạt* ☒
- *Không đạt* ☐

Giải thích lý do: Các sản phẩm đạt các yêu cầu khoa học đề ra trong Thuyết minh được duyệt, đáp ứng đầy đủ các yêu cầu về số lượng và chất lượng.

Cam đoan nội dung của Báo cáo là trung thực; Chủ nhiệm và các thành viên tham gia thực hiện nhiệm vụ không sử dụng kết quả nghiên cứu của người khác trái với quy định của pháp luật.

CHỦ NHIỆM NHIỆM VỤ	**THỦ TRƯỞNG** **TỔ CHỨC CHỦ TRÌ NHIỆM VỤ**
TS. Trần Quang Đức	PHÓ VIỆN TRƯỞNG VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG PGS.TS. Huỳnh Thị Thanh Bình