BAN CƠ YẾU CHÍNH PHỦ
HỌC VIỆN KỸ THUẬT MẬT MÃ

TIỂU LUẬN

MÔN HỌC: PHƯƠNG PHÁP NGHIÊN CỨU KHOA HỌC

TÊN TIỂU LUẬN: XÂY DỰNG ĐỀ CƯƠNG VỚI ĐỀ TÀI "NGHIÊN CỨU BẢO ĐẢM AN TOÀN CHO ĐIỆN TOÁN ĐÁM MÂY"

Họ và tên học viên: Phạm Quang Long
Khóa: CHAT10
Giảng viên hướng dẫn: PGS.TS. Bùi Thu Lâm – Học viện Kỹ thuật Mật Mã.

Hà Nội – năm 2024

BAN CƠ YẾU CHÍNH PHỦ
HỌC VIỆN KỸ THUẬT MẬT MÃ

PHẠM QUANG LONG

ĐỀ CƯƠNG LUẬN VĂN THẠC SĨ

ĐỀ TÀI: NGHIÊN CỨU BẢO ĐẢM AN TOÀN CHO ĐIỆN TOÁN ĐÁM MÂY
Chuyên ngành: ATTT
Mã số: 8480202

HÀ NỘI – 2024

BAN CƠ YẾU CHÍNH PHỦ
HỌC VIỆN KỸ THUẬT MẬT MÃ

ĐỀ CƯƠNG LUẬN VĂN THẠC SĨ

ĐỀ TÀI: NGHIÊN CỨU BẢO ĐẢM AN TOÀN CHO ĐIỆN TOÁN ĐÁM MÂY
Chuyên ngành: ATTT
Mã số: 8480202

Họ và tên học viên: Phạm Quang Long
Khóa: CHAT10

Người hướng dẫn khoa học: PGS.TS. Bùi Thu Lâm – Học viện Kỹ thuật Mật Mã.

HÀ NỘI – 2024

I. MỞ ĐẦU

1. Tính cấp thiết của đề tài

Trong kỷ nguyên số hóa hiện đại, điện toán đám mây (cloud computing) đã trở thành một phần không thể thiếu trong quá trình chuyển đổi số của các doanh nghiệp và tổ chức trên toàn thế giới. Các dịch vụ điện toán đám mây như Infrastructure as a Service (IaaS), Platform as a Service (PaaS), và Software as a Service (SaaS) mang lại nhiều lợi ích rõ rệt, bao gồm tối ưu hóa chi phí, tính linh hoạt cao, và khả năng mở rộng không giới hạn [1]. Tuy nhiên, sự phát triển nhanh chóng của các dịch vụ đám mây đồng nghĩa với việc gia tăng các mối đe dọa bảo mật .

Theo báo cáo từ Cloud Security Alliance (CSA) và ISC, các cuộc tấn công mạng ngày càng tinh vi, với nhiều tổ chức đã phải đối mặt với các sự cố nghiêm trọng như rò rỉ thông tin cá nhân, tấn công DDoS, và xâm nhập vào các hệ thống quản lý dữ liệu [2]. Một số vụ tấn công nổi bật như vụ Capital One vào năm 2019 đã làm lộ dữ liệu của hơn 100 triệu người dùng trên nền tảng đám mây AWS [3]. Điều này nhấn mạnh tầm quan trọng của việc tăng cường bảo mật cho điện toán đám mây .

Các nghiên cứu cũng chỉ ra rằng, nếu không có các biện pháp bảo mật nghiêm ngặt và linh hoạt, các hệ thống đám mây có thể trở thành mục tiêu dễ dàng cho các cuộc tấn công mạng [4]. Với sự gia tăng liên tục của các mối đe dọa, việc đảm bảo an toàn cho điện toán đám mây không chỉ bảo vệ dữ liệu mà còn đảm bảo tính liên tục của các hoạt động công nghệ và tránh các tổn thất tài chính lớn [5]. Đây chính là lý do khiến chủ đề "Bảo mật cho điện toán đám mây" trở nên cấp thiết hơn bao giờ hết, đặc biệt trong bối cảnh số hóa hiện nay.

2. Mục tiêu chính nghiên cứu của đề tài

Phân tích các thách thức và lỗ hổng bảo mật: Đánh giá các lỗ hổng phổ biến như mất kiểm soát quyền truy cập, cấu hình sai, và các cuộc tấn công trực tiếp vào giao thức [6].

Đánh giá các biện pháp bảo mật hiện tại: Xem xét các biện pháp bảo mật truyền thống như mã hóa, kiểm soát truy cập và so sánh với các công nghệ bảo mật tiên tiến như trí tuệ nhân tạo (AI) và chuỗi khối (blockchain) .

Sử dụng công cụ mã nguồn mở: Áp dụng công cụ Zeek và bộ dữ liệu CSE-CIC-IDS2018 để thực hiện thử nghiệm về các phương pháp phát hiện xâm nhập và phân tích lưu lượng mạng [7].

Thuyết phục về sự cần thiết của bảo mật trong điện toán đám mây: Chứng minh sự quan trọng của việc đầu tư vào các giải pháp bảo mật linh hoạt và hiện đại nhằm bảo vệ toàn vẹn dữ liệu và hệ thống.

3. Đối tượng và phạm vi nghiên cứu

Đối tượng nghiên cứu bao gồm các giải pháp và công cụ bảo mật trong môi trường điện toán đám mây, đặc biệt là các dịch vụ IaaS, PaaS, và SaaS [8]. Trong đó, tập trung vào việc phân tích lưu lượng mạng, phát hiện các hành vi xâm nhập bất thường, và kiểm tra khả năng chống lại các cuộc tấn công phổ biến bằng cách sử dụng các công cụ mã nguồn mở như OpenStack, Kubernetes, và Zeek. Phạm vi nghiên cứu bao gồm việc đánh giá các lỗ hổng bảo mật, phân tích các mối đe dọa an ninh và thử nghiệm các giải pháp bảo mật tiên tiến trong bối cảnh thực tế của môi trường đám mây.

4. Các nhiệm vụ chính cần thực hiện

Thu thập và phân tích tài liệu: Tiến hành nghiên cứu các tài liệu khoa học liên quan đến bảo mật điện toán đám mây, tập trung vào các lỗ hổng và mối đe dọa bảo mật đang nổi lên [9].

So sánh các giải pháp bảo mật: Đánh giá các giải pháp bảo mật hiện tại và so sánh chúng với các công nghệ tiên tiến như AI và Blockchain để tìm ra phương pháp tối ưu [10].

Phân tích nguyên nhân và hậu quả của các rủi ro bảo mật: Xác định các nguyên nhân dẫn đến các lỗ hổng bảo mật như cấu hình sai, quản lý yếu kém, và

phân tích hậu quả từ các sự cố bảo mật điển hình như việc mất dữ liệu hoặc hệ thống ngừng hoạt động.

Miêu tả chi tiết các công cụ và kỹ thuật bảo mật: Tập trung vào các công cụ bảo mật mã nguồn mở như Zeek, Snort, và OSSEC, cũng như các phương pháp bảo mật hiện đại như mã hóa và phân quyền trong môi trường đám mây [11].

5. Kết quả dự kiến

Bài nghiên cứu dự kiến sẽ cung cấp một cái nhìn toàn diện và thực tiễn về các phương pháp bảo mật điện toán đám mây, bao gồm phân tích hiệu quả của các công cụ bảo mật mã nguồn mở như Zeek [7]. Đồng thời, đề tài cũng hướng đến việc đưa ra các giải pháp bảo mật thiết thực, phù hợp với các hệ thống đám mây hiện tại và tương lai. Ngoài ra, nghiên cứu sẽ đóng góp vào việc định hướng các doanh nghiệp trong việc đầu tư vào các công nghệ bảo mật phù hợp, giúp họ bảo vệ dữ liệu, giảm thiểu rủi ro an ninh, và tăng cường khả năng chống lại các mối đe dọa mạng [12].

6. Phương pháp và công cụ nghiên cứu

Xây dựng môi trường điện toán đám mây bằng OpenStack: Sử dụng nền tảng mã nguồn mở OpenStack để mô phỏng một hệ thống đám mây, giúp kiểm tra và đánh giá các biện pháp bảo mật trong điều kiện thực tế [13]. OpenStack cho phép thiết lập môi trường hạ tầng như IaaS, từ đó thực hiện phân tích các lỗ hổng bảo mật tiềm ẩn.

Sử dụng Zeek để phân tích lưu lượng mạng: Công cụ Zeek sẽ được sử dụng để giám sát và phân tích lưu lượng mạng nhằm phát hiện các hành vi bất thường và các cuộc tấn công mạng trong môi trường đám mây [7]. Zeek giúp theo dõi các giao thức phổ biến và tạo ra các bản ghi sự kiện mạng chi tiết.

Sử dụng bộ dữ liệu CSE-CIC-IDS2018: Đây là bộ dữ liệu công khai và đã được gán nhãn, mô phỏng các cuộc tấn công mạng trong môi trường đám mây, bao gồm DDoS, Brute-force, và Botnet. Sử dụng bộ dữ liệu này để huấn luyện và đánh giá các mô hình học máy nhằm phát hiện xâm nhập [14].

Phương pháp so sánh: So sánh hiệu quả của các giải pháp bảo mật truyền thống với các công nghệ bảo mật hiện đại như AI và Blockchain, từ đó đề xuất các phương pháp bảo mật phù hợp cho điện toán đám mây [15].

II. DỰ KIẾN CÁC CHƯƠNG MỤC

MỤC LỤC

DANH MỤC CÁC TỪ VIẾT TẮT

DANH MỤC CÁC BẢNG BIỂU

DANH MỤC CÁC HÌNH VẼ

MỞ ĐẦU

CHƯƠNG 1: TỔNG QUAN VỀ BẢO MẬT ĐIỆN TOÁN ĐÁM MÂY

- Mục đích của chương:

Cung cấp cái nhìn tổng quan, làm nổi bật các rủi ro và thách thức trong bảo mật đám mây, đồng thời khẳng định sự cần thiết của các công nghệ bảo mật mới trong môi trường này.

- 1.1. Giới thiệu về điện toán đám mây và mô hình dịch vụ:

Trình bày các mô hình dịch vụ đám mây như IaaS, PaaS, SaaS, và các đặc thù bảo mật của chúng.

- 1.2. Các thách thức bảo mật trong đám mây:

Đề cập đến các mối đe dọa phổ biến như DDoS, tấn công MitM, lỗ hổng bảo mật trong các dịch vụ đám mây.

- 1.3. Các giải pháp bảo mật truyền thống và hạn chế:

Mô tả các biện pháp bảo mật truyền thống như tường lửa, mã hóa dữ liệu, và các khó khăn trong việc áp dụng chúng trong môi trường đám mây.

CHƯƠNG 2: PHÂN TÍCH NGUYÊN NHÂN VÀ HẬU QUẢ CỦA CÁC RỦI RO BẢO MẬT TRONG ĐIỆN TOÁN ĐÁM MÂY

- Mục đích của chương:

Phân tích chi tiết các nguyên nhân chính dẫn đến rủi ro bảo mật trong điện toán đám mây, từ đó làm sáng tỏ những lý do cơ bản khiến các hệ thống đám mây dễ bị tấn công. Xác định các yếu tố kỹ thuật và chỉ ra các hậu quả tiềm ẩn từ những

cuộc tấn công mạng, như mất dữ liệu, gián đoạn dịch vụ, gây ra thiệt hại về uy tín và tài chính

- 2.1. Nguyên nhân của các rủi ro bảo mật:

Phân tích các nguyên nhân chính như quản lý truy cập không chặt chẽ, cấu hình sai, và lỗ hổng bảo mật trong các dịch vụ đám mây.

- 2.2. Hậu quả của các cuộc tấn công mạng trong đám mây:

Trình bày các tác động như mất dữ liệu, ảnh hưởng đến uy tín doanh nghiệp và các thiệt hại kinh tế.

- 2.3. Phương pháp ngăn chặn và giảm thiểu rủi ro: Đưa ra các biện pháp giảm thiểu như mã hóa dữ liệu, kiểm soát truy cập và giám sát lưu lượng mạng cùng với việc áp dụng các công nghệ mới như học máy.

CHƯƠNG 3: CÔNG CỤ ZEEK VÀ ỨNG DỤNG TRONG PHÁT HIỆN XÂM NHẬP

- Mục đích của chương:

Giới thiệu và phân tích công cụ Zeek trong việc phát hiện và ngăn chặn các cuộc tấn công mạng trong hệ thống điện toán đám mây. Làm rõ vai trò của Zeek trong việc bảo mật đám mây và lý do chọn công cụ này để thử nghiệm và nghiên cứu trong bối cảnh các mối đe dọa mạng ngày càng tinh vi.

- 3.1. Giới thiệu về Zeek:

Cung cấp thông tin chi tiết về Zeek, một công cụ phân tích lưu lượng mạng mạnh mẽ.

- 3.2. Hoạt động của Zeek trong môi trường đám mây:

Mô tả cách Zeek có thể giám sát và phát hiện các cuộc tấn công trong môi trường đám mây.

- 3.3. So sánh Zeek với các công cụ bảo mật khác:

So sánh Zeek với các công cụ khác như Suricata, Snort, Wireshark.

CHƯƠNG 4: PHÁT HIỆN XÂM NHẬP SỬ DỤNG HỌC MÁY VỚI BỘ DỮ LIỆU CSE-CIC-IDS2018

- Mục đích của chương:

Triển khai và thử nghiệm việc phát hiện xâm nhập trong hệ thống điện toán đám mây bằng cách sử dụng các mô hình học máy kết hợp với bộ dữ liệu CSE-CIC-IDS2018. Phân tích khả năng áp dụng học máy để tự động phát hiện và xử lý các mối đe dọa bảo mật phức tạp, đặc biệt là các tấn công mạng như DDoS, Brute-force, và Botnet.

- 4.1. Giới thiệu về bộ dữ liệu CSE-CIC-IDS2018:

Trình bày nội dung và cấu trúc của bộ dữ liệu, cùng với các loại tấn công được mô phỏng.

- 4.2. Áp dụng học máy trong phát hiện tấn công:

Mô tả các mô hình học máy (Random Forest, SVM, Deep Learning) và cách chúng được áp dụng vào bộ dữ liệu.

- 4.3. Kết quả thử nghiệm và đánh giá:

Phân tích và đánh giá hiệu quả của các mô hình học máy trong việc phát hiện tấn công.

CHƯƠNG 5: ĐỀ XUẤT GIẢI PHÁP NÂNG CAO BẢO MẬT ĐIỆN TOÁN ĐÁM MÂY

- Mục đích của chương:

Đề xuất các giải pháp nâng cao bảo mật cho hệ thống điện toán đám mây, dựa trên các phân tích và kết quả thử nghiệm từ các chương trước. Tập trung vào việc tối ưu hóa và kết hợp các công nghệ hiện đại như Zeek, học máy, đồng thời đề xuất hướng nghiên cứu với AI và blockchain để tạo ra một hệ thống bảo mật linh hoạt và hiệu quả hơn.

- 5.1. Tăng cường bảo mật với Zeek và học máy:

Đề xuất các giải pháp kết hợp giữa Zeek và học máy để tăng cường bảo mật.

- 5.2. Tích hợp AI và Blockchain vào bảo mật đám mây:

Phân tích tiềm năng của AI và Blockchain trong bảo mật đám mây.

- 5.3. Đề xuất hướng nghiên cứu tương lai:

Đề xuất hướng nghiên cứu về việc nâng cao khả năng phát hiện tấn công bằng cách sử dụng AI hoặc các công nghệ bảo mật mới.

KẾT LUẬN

- Tóm tắt những kết quả đã làm được trong quá trình nghiên cứu.

- Khẳng định vai trò của việc đảm bảo an toàn cho môi trường điện toán đám mây.

- Đánh giá và đề xuất: Đưa ra đánh giá chung và đề xuất cho các hướng nghiên cứu và ứng dụng trong tương lai.

TÀI LIỆU THAM KHẢO

[[1] Chandrasekaran, S., et al. (2020). A study on cloud computing security challenges. Journal of Network and Computer Applications, 122, 153-161.

[2] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. National Institute of Standards and Technology Special Publication 800-145.

[3] Srinivasan, S., Sarukesi, K., Rodrigues, P., Manoj, M. S., & Revathy, P. (2020). State-of-the-art cloud computing security taxonomies: A survey. Computer Standards & Interfaces, 66, 103367.

[4] Hashizume, H., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1), 1-13.

[5] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11.

[6] Fernando, N., Loke, S. W., & Rahayu, W. (2013). Mobile cloud computing: A survey. Future Generation Computer Systems, 29(1), 84-106.

[7] Buyya, R., et al. (2019). A Manifesto for Future Generation Cloud Computing: Research Directions for the Next Decade. ACM Computing Surveys, 51(5), 1-38.

[8] Xiao, Z., & Gong, Y. (2017). A tutorial on secure cloud storage. IEEE Communications Surveys & Tutorials, 19(4), 2974-2995.

[9] Stallings, W. (2020). Cryptography and Network Security Principles and Practice. Pearson.

[10] Wang, Z., et al. (2020). Zeek: An efficient platform for analyzing network security. Journal of Network Security, 103, 55-67.

[11] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP).

[12] Zhou, Z., et al. (2020). Blockchain and Cloud Computing Fusion: A Survey, Key Challenges, and Future Directions. IEEE Communications Surveys & Tutorials, 22(3), 2049-2071.

[13] Al-Roomi, M., Al-Ebrahim, S., Buqrais, S., & Ahmad, I. (2013). Cloud computing pricing models: A survey. International Journal of Grid and Distributed Computing, 6(5), 93-106.

[14] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy, 305-316.

[15] Choo, K. K. R., Gai, K., & Sun, X. (2020). The role of cloud computing in supporting secure big data processing. Future Generation Computer Systems, 98, 36-46.

III. KẾ HOẠCH THỰC HIỆN

Luận văn dự kiến được hoàn thành trong khoảng ***6 tháng (25 tuần)*** kể từ khi ra quyết định giao đề tài. Cụ thể như sau:

ST	Thời gian	Nội dung thực hiện	Ghi chú
1	**1 Tuần:** Từ xx/xx/201x Đến xx/xx/201x	**Xây dựng đề cương chi tiết**	
2	**3 tuần:** Từ xx/xx/201x Đến xx/xx/201x	**CHƯƠNG 1: TỔNG QUAN VỀ BẢO MẬT ĐIỆN TOÁN ĐÁM MÂY**	
		1.1. Giới thiệu về điện toán đám mây và mô hình dịch vụ	
		1.2. Các thách thức bảo mật trong đám mây	
		1.3. Các giải pháp bảo mật truyền thống và hạn chế	
3	**3 tuần:** Từ xx/xx/201x Đến xx/xx/201x	**CHƯƠNG 2: PHÂN TÍCH NGUYÊN NHÂN VÀ HẬU QUẢ CỦA CÁC RỦI RO BẢO MẬT TRONG ĐIỆN TOÁN ĐÁM MÂY**	
		2.1. Nguyên nhân của các rủi ro bảo mật	
		2.2. Hậu quả của các cuộc tấn công mạng trong đám mây	
		2.3. Phương pháp ngăn chặn và giảm thiểu rủi ro	

4	Từ xx/xx/201x Đến xx/xx/201x	**Báo cáo tiến độ**	
5	**5 tuần:** Từ xx/xx/201x Đến xx/xx/201x	**CHƯƠNG 3: CÔNG CỤ ZEEK VÀ ỨNG DỤNG TRONG PHÁT HIỆN XÂM NHẬP**	
		3.1. Giới thiệu về Zeek	
		3.2. Hoạt động của Zeek trong môi trường đám mây	
		3.3. So sánh Zeek với các công cụ bảo mật khác	
6	**5 tuần:** Từ xx/xx/201x Đến xx/xx/201x	**CHƯƠNG 4: PHÁT HIỆN XÂM NHẬP SỬ DỤNG HỌC MÁY VỚI BỘ DỮ LIỆU CSE-CIC-IDS2018**	
		4.1. Giới thiệu về bộ dữ liệu CSE-CIC-IDS2018	
		4.2. Áp dụng học máy trong phát hiện tấn công	
		4.3. Kết quả thử nghiệm và đánh giá	
7	Từ xx/xx/201x Đến xx/xx/201x	**Báo cáo tiến độ**	
8	**3 tuần:** Từ xx/xx/201x Đến xx/xx/201x	**CHƯƠNG 5: ĐỀ XUẤT GIẢI PHÁP NÂNG CAO BẢO MẬT ĐIỆN TOÁN ĐÁM MÂY**	
		5.1. Tăng cường bảo mật với Zeek và học máy	

		5.2. Tích hợp AI và Blockchain vào bảo mật đám mây	
		5.3. Đề xuất hướng nghiên cứu tương lai	
9	**02 tuần:** Từ xx/xx/201x	**Hoàn chỉnh luận văn** *(Thời gian dự trữ: 1 tuần)*	

*(**Ghi chú:** Quá thời hạn nêu trên mà chưa hoàn thành luận văn, học viên phải đến trường để làm thủ tục gia hạn theo quy định)*

IV. TÀI LIỆU THAM KHẢO XÂY DỰNG ĐỀ CƯƠNG

Tài liệu tham khảo trích dẫn trong đề cương luận văn cần được trích dẫn theo số thứ tự của tài liệu tham khảo ở danh mục tài liệu tham khảo của đề cương và số thứ tự đó được đặt trong ngoặc vuông.

[[1] Chandrasekaran, S., et al. (2020). A study on cloud computing security challenges. Journal of Network and Computer Applications, 122, 153-161.

[2] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. National Institute of Standards and Technology Special Publication 800-145.

[3] Srinivasan, S., Sarukesi, K., Rodrigues, P., Manoj, M. S., & Revathy, P. (2020). State-of-the-art cloud computing security taxonomies: A survey. Computer Standards & Interfaces, 66, 103367.

[4] Hashizume, H., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1), 1-13.

[5] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11.

[6] Fernando, N., Loke, S. W., & Rahayu, W. (2013). Mobile cloud computing: A survey. Future Generation Computer Systems, 29(1), 84-106.

[7] Buyya, R., et al. (2019). A Manifesto for Future Generation Cloud Computing: Research Directions for the Next Decade. ACM Computing Surveys, 51(5), 1-38.

[8] Xiao, Z., & Gong, Y. (2017). A tutorial on secure cloud storage. IEEE Communications Surveys & Tutorials, 19(4), 2974-2995.

[9] Stallings, W. (2020). Cryptography and Network Security Principles and Practice. Pearson.

[10] Wang, Z., et al. (2020). Zeek: An efficient platform for analyzing network security. Journal of Network Security, 103, 55-67.

[11] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP).

[12] Zhou, Z., et al. (2020). Blockchain and Cloud Computing Fusion: A Survey, Key Challenges, and Future Directions. IEEE Communications Surveys & Tutorials, 22(3), 2049-2071.

[13] Al-Roomi, M., Al-Ebrahim, S., Buqrais, S., & Ahmad, I. (2013). Cloud computing pricing models: A survey. International Journal of Grid and Distributed Computing, 6(5), 93-106.

[14] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy, 305-316.

[15] Choo, K. K. R., Gai, K., & Sun, X. (2020). The role of cloud computing in supporting secure big data processing. Future Generation Computer Systems, 98, 36-46.