**TRƯỜNG ĐẠI HỌC HỒNG ĐỨC**



**BÀI TẬP LỚN**

**XỬ LÝ SONG SONG VÀ HỆ THỐNG PHÂN TÁN**

**THỰC HIỆN BẢO MẬT TRONG HỆ THỐNG PHÂN TÁN**

**NGHIÊN CỨU SO SÁNH**

**THANH HÓA, THÁNG 11 /2022**

**TRƯỜNG ĐẠI HỌC HỒNG ĐỨC**

**BÀI TẬP LỚN**

**XỬ LÝ SONG SONG VÀ HỆ THỐNG PHÂN TÁN**

**THỰC HIỆN BẢO MẬT TRONG HỆ THỐNG PHÂN TÁN**

**NGHIÊN CỨU SO SÁNH**

Sinh viên thực hiện: Đặng Thị Thuỳ Linh

Lớp: K22 CNTT

Khoa: Công nghệ thông tin và Truyền thông

Giảng viên hướng dẫn: ThS.Lê Việt Nam

**THANH HÓA, THÁNG 11 /2022**

# LỜI NÓI ĐẦU

Hiện nay, công nghệ thông tin là mối quan tâm hàng đầu của Việt Nam và toàn thế giới. Chính mối quan tâm này đã làm nên cuộc cách mạng về khoa học và công nghệ. Khởi đầu cho cuộc cách mạng khoa học và công nghệ này là sự hình thành và phát triển hàng loạt máy tính và các phương tiện xử lý thông tin khác. Với sự phát triển nhanh chóng của khoa học máy tính cũng như nhu cầu trao đổi thông tin trong mọi hoạt động của xã hội đòi hỏi sự phát triển đồng bộ các phương tiện truyền thông. Các thành tựu của ngành khoa học trí tuệ này đã góp phần quan trọng vào việc thay đổi bộ mặt của thế giới vả về bề mặt lẫn chiều sâu. Việc ứng dụng các thành tựu của nền công nghệ hiện đại này trở thành vấn đề chủ chốt, quan trọng, quyết định sự thành bại của các thành phần tham gia vào lĩnh vực hoạt động trên thế giới từ kinh tế, văn hoá, chính trị đến quân sự.

Trên thực thế, một xu hướng kỹ thuật mới được hình thành, xu hướng phân tán các thành phần tạo nên hệ tin học theo hướng tiếp cận nơi sử dụng và sản xuất thông tin trên cơ sở mạng máy tính. Nhằm khai thác có hiệu quả toàn hệ, vấn đề quan trọng hàng đầu cần tính đến là các tài nguyên và chiến lược khai thác, sử dụng chúng một cách có hiệu quả nhất.

Báo cáo này trình bày một nghiên cứu so sánh hệ thống phân tán và các vấn đề an ninh liên quan đến các hệ thống này. Bốn hệ thống phân tán thường được sử dụng xem xét để phân tích chi tiết về công nghệ liên quan, vấn đề an ninh phải đối mặt và giải pháp đề xuất để phá vỡ những vấn đề này. Cuối cùng, các vấn đề an ninh và giải pháp được tóm tắt và so sánh với nhau.

Được sự giúp đỡ tận tình của thầy Lê Việt Nam em đã hoàn thành bản báo cáo. Tuy nhiên thời gian và kiến thức có hạn nên bản báo cáo chắc chắn còn nhiều khuyết điểm, em rất mong nhận được sự góp ý của thầy và mọi người. Cho phép em được bày tỏ lòng biết ơn đối với thầy Lê Việt Nam đã giúp đỡ em hoàn thành bản báo cáo này.

Trân trọng cảm ơn!

# GIỚI THIỆU

Trong thế giới mạng ngày nay, máy tính hiếm khi làm việc một cách độc lập. Chúng cộng tác với nhau nhằm đảm bảo mục đích giao tiếp, xử lý, truyền dữ liệu, lưu trữ… Khi các hệ thống làm việc theo kiểu cộng tác này với hệ thống khác ở vị trí địa lý cách xa nhau được xem như là hệ thống phân tán. Trong tin học, các nhà nghiên cứu đã sử dụng các định nghĩa khác nhau để phác thảo hệ thống phân tán là gì.

Coulouris và cộng sự của ông ta đã định nghĩa một hệ phân tán là “Một hệ thống mà các thành phần phần cứng và phần mềm được cài đặt phân tán trên các máy tính ở những vị trí địa lý khác nhau”. Chúng phối hợp hành động thông qua tin nhắn. Tanenbaum và Van Steen đã định nghĩa một hệ thống phân tán là “Một tập hợp của hệ thống xuất hiện cho người sử dụng như là một hệ thống duy nhất”. Từ định nghĩa của ông Tanenbaum, có thể quan niệm rằng một hệ thống phân tán liên quan đến hệ thống phần mềm nhiều hơn là phần cứng có liên quan đến việc tạo ra các hệ thống. Kết hợp những định nghĩa này, có thể khẳng định rằng hệ thống phân tán là một ứng dụng mà việc giao tiếp với nhiều phần cứng và phần mềm phân tán để phối hợp hành động của nhiều tiến trình đang chạy trên những máy tính tự điều khiển khác nhau. Trong mạng truyền thông, để tất cả các thành phần phần cứng và phần mềm hợp tác với nhau để thực hiện một tập hợp các nhiệm vụ liên quan nhằm hướng tới mục tiêu chung. Hầu hết mọi người quan tâm đến hệ phân tán và mạng máy tính là như vậy. Tuy nhiên, hai thuật ngữ này là hai việc khác nhau nhưng có liên quan đến nhau. Một mạng máy tính là một bộ kết nối của các máy tính độc lập giao tiếp với nhau. Một người sử dụng mạng máy tính hiểu rằng anh ta đang sử dụng các nguồn lực khác nhau nằm trên các máy tính khác nhau như một mạng lưới máy tính. Nhưng mặt khác, một hệ phân tán tạo cho người sử dụng cảm giác đang làm việc trên một máy tính đồng nhất mạnh mẽ và nhiều nguồn lực hơn. Sự tồn tại của những máy tính độc lập là rõ ràng cho người dùng như là ứng dụng hệ phân tán đang chạy trên những máy tính sẽ lựa chọn máy tính phù hợp và bố trí công việc không cần sự can thiệp của người sử dụng.

Hệ phân tán được xây dựng với mục tiêu đạt được là:

* Sự trong suốt.
* Tính mờ.
* Độ tin cậy.
* Hiệu suất.
* Khả năng mở rộng.

Để đạt được các mục tiêu trên, an ninh của hệ thống phải được quan tâm đầy đủ như nó là một trong những vấn đề cơ bản của hệ phân tán. Phải chú ý tại mỗi công đoạn bao gồm thiết kế, hoạt động, thực hiện và quản lý hệ phân tán.

# HỆ PHÂN TÁN

Có nhiều hệ phân tán trong hoạt động ngày nay. Sau đây là một số hệ phân tán phổ biến nhất.

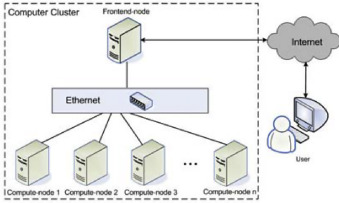
* Cụm máy tính.
* Lưới điều khiển máy tính.
* Hệ thống lưu trữ phân tán.
* Cơ sở dữ liệu phân tán.

1. **Cụm máy tính**

Giao tiếp máy tính qua mạng tốc độ cao có thể được thực hiện đề làm việc và trình bày chính nó như là một máy tính duy nhất cho người sử dụng. Một tập hợp các máy tính được nhóm lại với nhau trong một cách thức mà chúng tạo thành một vốn tài nguyên duy nhất được gọi là một cụm. Bất kỳ nhiệm vụ nào đã được gán cho cụm thì đều có thể chạy được trên tất cả các máy tính trong cụm một cách song song bởi việc phân chia toàn bộ nhiệm vụ vào các nhiệm vụ nhỏ hơn chứa trong nó. Sau đó, kết quả của nhiệm vụ nhỏ sẽ kết hợp để tạo thành kết quả cuối cùng.

Cụm máy tính giúp các tổ chức tăng khả năng tính toán của họ bằng cách sử dụng công nghệ đạt tiêu chuẩn và thường có sẵn. Những phần cứng và phần mềm này là những mặt hàng có thể mua được từ thị trường với chi phí thấp. Cụm máy tính đã nhìn thấy sự tăng trưởng to lớn trong những năm gần đây. Khoảng 80% trong top 500 trung tâm siêu máy tính trên thế giới đang sử dụng. Các cụm được sử dụng chính cho các ứng dụng về khoa học kỹ thuật, thương mại và công nghiệp đòi hỏi sẵn sàng và xử lý thông lượng cao. Sự sắp xếp thứ tự protein trong ứng dụng y sinh học, mô phỏng động đất trong xây dựng,

mô phỏng hồ chứa dầu khí trong nguồn lục trái đất và kỹ thuật dầu khí, nhân rộng và phân phối lưu trữ, máy chủ sao lưu dự phòng cho nhu cầu kinh doanh các ứng dụng web dựa trên một vài ví dụ cho các ứng dụng mà chủ yếu chạy trên các cụm. Hình 1 cho thấy sự sắp xếp của các máy tính trong cụm máy tính.



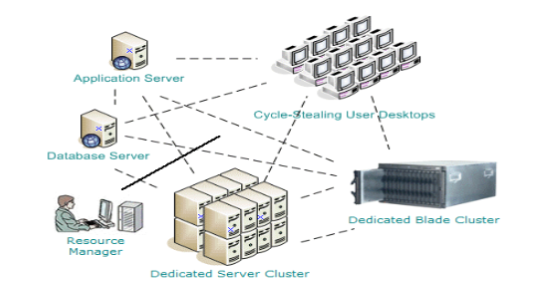
Hình 1 Cụm máy tính

1. **Lưới điều khiển máy tính**

Lưới điều khiển là một dạng của hệ thống máy tính được phân tán, một số lượng lớn các máy tính nhỏ, lỏng lẻo được hợp lại để hình thành một siêu máy tính ảo, chúng phải thực hiện những nhiệm vụ lớn đối với bất kỳ máy tính đơn để thực hiện một thời gian hợp lý.

Lưới điều khiển được định nghĩa là một hệ song song và phân tán có khả năng lựa chọn, chia sẻ các nguồn tài nguyên động được phân tán ở thời gian chạy dựa trên tính sẵn có, khả năng, hiệu suất và chi phí đấp ứng yêu cầu chất lượng dịch vụ (QoS) của người sử dụng. Mạng lưới máy tính kết hợp vớ tài nguyên máy tính được phân tán trên một khu vục địa lý rộng lớn thuộc về người tổ chức khác nhau. Mục đích chính của hệ thống lưới điều khiển là hợp tác làm việc trên nhiều hệ thống để giải quyết các nhiệm vụ của từng máy tính đơn bằng cách chia nhiệm vụ thành các nhiệm vụ nhỏ và phân tán những nhiệm vụ này ở nhiều máy tính khác nhau.

Thành phần trung gian được sử dụng trong lưới điều khiển máy tính chịu trách nhiệm phân chia và bố trí nhiệm vụ. Kích thước của hệ thống lưới điều khiển có thể khác nhau từ vài trăm máy tính trong một tổ chức cho đến hệ thống lớn bao gồm hàng nghìn nút. Lưới điều khiển nhỏ được giới hạn một tổ chức đơn thường được gọi là Intra-node corporation. Khi hệ thống rộng lớn hơn được gọi là Intra-node corporation. Hình 2 cho thấy hệ thống lưới điều khiển phân tán trên nền tảng máy tính không đồng nhất.

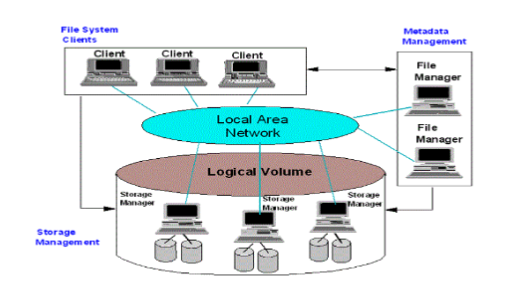


Hình 2 Hệ thống mạng lưới tính toán

Lưới điều khiển được sử dụng để thực hiện tính toán chuyên sâu các vấn đề khoa học, toán học và học tập thông qua các máy tính trung gian. Khám phá thuốc, dự báo kinh tế, phân tích địa chấn và xử lý dữ liệu văn phòng cho thương mại điện tử là một vài trong số các nhiệm vụ thường được giải quyết bằng cách sử dụng lưới điều khiển tính toán (lưới máy tính).

1. **Hệ thống lưu trữ phân tán**

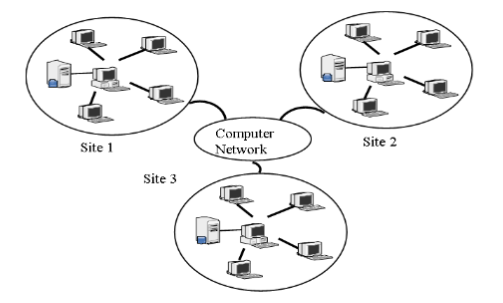
Tốc độ tăng trưởng nhanh chóng của khối lượng lưu trữ, băng thông và tài nguyên tính toán cùng với việc giảm chi phí của các thiết bị lưu trữ trở nên phổ biến đối với hệ thống lưu trữ phân tán. Mục tiêu chính của lưu trữ phân tán trên nhiều thiết bị để bảo vệ dữ liệu trong trường hợp lỗi đĩa thông qua lưu trữ dự phòng trên nhiều thiết bị để làm cho dữ liệu có sẵn gần gũi hơn với người sử dụng trong hệ thống phân tán lớn. Có bốn loại chủ yếu của hệ thống lưu trữ phân tán. Cụ thể là, server attached Redundant Array of independent Disks (RAID), centralized RAID, network attached storage (NAS) và storage Area Network (SAN). NAS và SAN là 2 kỹ thuật lưu trữ phân tán phổ biến nhất. Hình 3 cho thấy việc bố trí đặc trưng của hệ thống lưu trữ phân tán. NAS và SAN có sự khác biệt nhỏ về kỹ thuật truyền dữ liệu giữa các thiết bị và hiệu suất. NAS chủ yếu sử dụng giao thức TCP/IP và truyền dữ liệu qua nhiều thiết bị trong khi SAN sử dụng SCSI thiết lập trên các kênh cáp quang. Do đó, NAS có thể thực hiện trên bất kỳ mạng vật lý nào có sự hỗ trợ của TCP/IP như Ethenet, FDDI, ATM. Nhưng SAN chỉ có thể thực hiện được trên kênh cáp quang. SAN có hiệu suất tốt hơn NAS như TCP có chi phí cao hơn và SCSI nhanh hơn so với mạng TCP/IP.



Hình 3 Hệ thống lưu trữ phân tán

1. **Cơ sở dữ liệu phân tán**

Hệ thống cơ sở dữ liệu phân tán là một bộ sưu tập của hệ thống cơ sở dữ liệu độc lập được phân tán trên nhiều máy tính. Chúng hợp tác lưu trữ dữ liệu như vậy người sử dụng có thể truy cập dữ liệu từ nhiều nơi như thể nó được lưu trữ địa phương không phân biệt nơi mà dữ liệu được lưu trữ thực sự.



Hình 4 Sắp xếp của hệ thống cơ sở dữ liệu phân tán trên nhiều trạm mạng

# BẢO MẬT TRONG HỆ THỐNG PHÂN TÁN

Bảo mật là một trong những vấn đề quan trọng nhất của hệ phân tán. Khi dữ liệu được phân tán trên nhiều mạng hay thông tin được chuyển giao thông qua mạng công cộng, nó trở thành đối tượng để tấn công bởi các phần tử có hại. Tương tự tài nguyên máy tính khác như bộ vi xử lý, các thiết bị lưu trữ mạng… cũng có thể bị tấn công bởi các tin tặc.

1. **Bải mật cho các cụm máy tính**

Khi các cụm máy tính sẵn sàng cho công chúng hay các mạng được thiết lập bằng cách sử dụng các nguồn tài nguyên công cộng như internet, chúng trở thành các đối tượng để nhiều loại khác nhau tấn công. Loại phổ biến nhất tấn công vào các cụm là lấy cắp chu trình tính toán, ăn cắp sự giao tiếp giữa các nút, làm gián đoạn cụm dịch vụ. Do đó, các nhóm đã được bảo vệ bởi cơ chế bảo mật bao gồm các dịch vụ như kiểm tra tính toàn vẹn, xác thực và bảo mật. Mục đích chính của cơ chế bảo mật là bảo vệ hệ thống chống lại các tin tặc cũng như để đáp ứng các yêu cầu bảo mật của ứng dụng. Li và Vaughn đã nghiên cứu các lỗ hổng an ninh của các cụm máy tính bằng cách sử dụng đồ thị khai thác (E-graphs). Học đã mô phỏng các cuộc tấn công có thể thực hiện trên cả 3 trụ cột an ninh. Cụ thể là bảo mật, tính toàn vẹn và tính sẵn sàng. Họ chỉ ra rằng đồ thị khai thác có thể đơn giản hoá dựa trên lĩnh vực và kiến thức như các cấu hình cụm, các lỗ hổng được phát hiện… Họ phát biểu rằng kỹ thuật này có thể được sử dụng để xác nhận các cụm với sự giúp đỡ của một cơ sở kiến trúc của các lỗ hổng cụm.

Xie và Qin đã phát triển 2 chương trình phân bổ nguồn lực có tên là Deadline và Security Constraints (TAPADS) và Security Aware and Heterogeneity – Aware Resourse Allocation for Parallel jobs (SHAPH). Hai chương trình này đảm bảo rằng các ứng dụng song song được thực hiện trên các cụm máy tính trong khi đáp ứng thời hạn chót thi hành. Do đó nó có thể được nhìn thấy rằng nếu các chương trình này đảm bảo sự sẵn có của hệ thống như là thực hiện kịp thời của một ứng dụng là dấu hiệu của sự sẵn có về nguồn lực. Denial of service (DoS) là một trong các cuộc tấn công trên hệ thống phân tán. Các cuộc tấn công chủ yếu nhằm mục tiêu các nguồn lực theo cách thức các nguồn lực được ngăn chặn từ việc thực hiện các hoạt động hợp pháp của họ. Một phương pháp sử dụng dịch vụ và chuỗi Markov để giảm thiểu các tác động trên các cuộc tấn công DOS trên một cụm dựa trên mạng cảm biến không dây đã được trình bày.

Do đó nó có thể được nhìn thấy các cụm máy tính dễ bị tấn công bởi các phần tử có hại như tin tặc và crackers do tính chất mở và sử dụng tài nguyên công cộng như internet. Nghiên cứu sâu rộng đã được thực hiện bởi các nhà nghiên cứu về sự an toàn của các cụm và họ đã đề xuất một số phương pháp có thể sử dụng để bảo vệ khác cụm khỏi bị tấn công.

1. **Lưới hệ thống bảo mật**

Lưới hệ thống máy tính cung cấp một số cơ chế bảo mật để bảo vệ nguồn tài nguyên mạng lưới chống lại các cuộc tấn công. Middleware là một trong các phần mềm hệ thống quan trọng trong cơ sở hạ tầng lưới điều khiển vì nó cung cấp cơ sở hạ tầng truyền thông chung và làm cho các dịch vụ lưới điều khiển có sẵn cho các ứng dụng. Middleware cũng cho phép một cấu hình bảo mật thống nhất, xác nhậnn lưới điều khiển dựa trên cơ sở hạ tầng khoá công khai (PKI) và khả năng xử lý các loại khác nhau của thông tin người dùng như PKI, SAML, Kerberos tickets, mật khẩu… Sự uỷ quyền là một trong những cơ chế cần thiết trong mạng lưới dịch vụ phân tán và được thực hiện bằng cách sử dụng X.509 Proxy Certificate. Uỷ quyền truy cập mạng lưới tài nguyên dựa trên tổ chức ảo (VO), các thuộc tính được giao cho người sử dụng và được quản lý bởi các dịch vụ thành viên tổ chức ảo (VOMS). Sự quản lý đáng tin cậy trong hệ thống mạng lưới được xử lý bằng cách sử dụng mối quan hệ xác thực và đáng tin cậy được đại diện bởi một chuỗi các chứng nhận bao gồm mạng lưới tác quyền về văn bằng (CA) chứng chỉ và liên tiếp các giấy uỷ quyền.

Lưới modul xác thực (Grid Authentication Module) là một trong những thành phần quan trọng trong việc ngăn ngừa người sử dụng bên ngoài từ mạng lưới nội bộ truy cập ngẫu nhiên và bảo vệ hệ thống mạng lưới từ những người sử dụng trái phép. Module này xử lý các mối đe doạ về an ninh mạng nội bộ. Khi người dùng mạng lưới được xác nhận thực hiện những hoạt động trái phép trong mạng lưới.

Những cơ chế bảo mật mạng lưới này được thực hiện hầu như tất cả hệ thống mạng lưới có sẵn hiện nay. Một vài cụm mạng lưới đầu tiên tiếp tục phát triển trong vùng mạng lưới trung gian tương tác. Điều này cuối cùng thống nhất mạng lưới an ninh như là một hệ thống bảo mật chặt chẽ độc lập.

1. **Bảo mật hệ thống lưu trữ phân tán**

Một số nghiên cứu hoạ động thực hiện trong mô hình đe doạ và phát triển mô hình an ninh để bảo vệ hệ thống lưu trữ phân tán. Tài nguyên quan trọng nhất trong hệ thống lưu trữ phân tán là dữ liệu được lưu trữ trong thiết bị lưu trữ của hệ thống. Dữ liệu này cần được dán nhãn và bảo vệ. Ngoài ra bất kỳ hệ thống bảo vệ được giới thiệu phải tương thích ngược. Nói cách khác, nó không những bảo vệ các dữ liệu được lưu trữ sau khi chương trình bảo mật được cài đặt mà dữ liệu đó được ưu tiên đối với hệ thống.

Hasan và cộng sự của ông ta đã giới thiệu một mô hình đe doạ có tên là mô hình đe doạ CIAA. Mô hình này đã giải quyết tất cả các vấn đề về an ninh. Cụ thể là bảo mật, toàn vẹn, tính sẵn có và xác thực. Đến mô hình này các tác giả đã tổ chức các mối đe doạ trên hệ thống lưu trữ phân tán dưới mỗi thể loại của trụ cột CIAA của kỹ thuật an ninh và được cung cấp có thể được sử dụng để phá vỡ các mối đe doạ. Mô hình bảo mật khác được thảo luận bởi các tác giả là mô hình vòng đời dữ liệu. Nó kiểm tra các mối đe doạ có thể xảy ra ở các giai đoạn khác nhau của trạng thái dữ liệu từ nguy cơ tuyệt chủng. Theo mô hình này, mối đe doạ được tổ chức dưới dạng 6 nhóm và các giải pháp được đề xuất.

Dikaliotis, Dimakis và Ho đã đề xuất một kỹ thuật băm tuyến tính đơn giản, nó có thể phát hiện ra lỗi trong các nút lưu trữ trong hệ thống lưu trữ phân tán mã hoá. Cơ chế phục hồi hợp tác lẫn nhau (MCR) cho phép hệ thống khôi phục dữ liệu trong tình huống nhiều nút thất bại. Sơ đồ truyền và thiết kế một mạng tuyến tính mã hoá chương trình dựa trên (n, k) strong-MDS code đề nghị giúp hệ thống hồi phục từ thất bại với một các tương đối dễ dàng.

Do đó có thể thấy vấn đề an ninh trong hệ thống lưu trữ phân tán chủ yếu tập trung vào việc bảo mật dữ liệu trong giới hạn toàn vẹn và quản lý thất thoát nếu có.

1. **Bảo mật cơ sở dữ liệu phân tán**

Hệ thống quản lý cơ sở dữ liệu phân tán đối mặt với nhiều nguy cơ về an ninh hơn so với cơ sở dữ liệu tập trung. Sự phát triển về bảo mật cho hệ thống cơ sở dữ liệu phân tán trở nên phức tạp hơn so với việc giới thiệu các mô hình cơ sở dữ liệu mới như mô hình cơ sở dữ liệu hướng đối tượng, mô hình cơ sở dữ liệu thời gian và mô hình cơ sở dữ liệu quan hệ đối tượng…

Trong mô hình bảo mật truyền thống, tất cả các dữ liệu được lưu trữ trong cơ sở dữ liệu và người truy cập dữ liệu thuộc cùng mức độ bảo mật. Một hệ thống cơ sở dữ liệu an toàn gán mức độ bảo mật cho mỗi giao dịch và dữ liệu. mức độ giải phóng một giao dịch được thể hiện bằng mức độ bảo mật được giao và mức độ phân loại của dữ liệu được đưa ra bởi mức độ phân loại. Một hệ thống quản lý cơ sở dữ liệu an toàn (MLS/DBMS) hạn chế các hoạt động của cơ sở dữ liệu dựa trên mức độ bảo mật. Từ các cuộc thảo luận cho thấy bằng các giới thiệu phân loại lượng thông tin và điều khiển truy cập, an ninh của cơ sở dữ liệu phân tán được tăng cường.

Zubi đã giới thiệu một thiết kế mà cải thiện tính chuyển đổi, tính dễ tiếp cận và tính linh hoạt trong khi truy cập các loại dữ liệu đa dạng trong hệ thống cơ sở dữ liệu phân tán. Ông cũng đề xướng mức độ đa dạng về sự điều khiển truy nhập, tính bí mật, sự tin cậy, sự toàn vẹn và sự khôi phục để quản lý an ninh của một hệ thống cơ sở dữ liệu phân tán.

# KẾT LUẬN

Từ thảo luận trên có thể nhìn thấy rằng bảo mật trở nên cấp thiết hơn khi hệ thống được phân tán trên khắp các vị trí địa lý. Mỗi loại hệ thống phân tán có yêu cầu bảo mật riêng của nó. Nhưng tất cả các hệ thống có chung bộ ba CIA (Central Intelligence Agency) như là trung tâm của việc bảo mật. Trong các cụm máy tính và mạng lưới an ninh chủ yếu tập trung bảo vệ dữ liệu trong việc truyền dẫn với sự truy nhập tới tài nguyên phân tán. An ninh trong các cụm đơn giản hơn so với mạng lưới do tính đồng nhất của các cụm. Một vài cuộc tấn công chính đã được thực hiện trên các cụm là cuộc tấn công Denial of Service (DoS). Các nhà nghiên cứu đã đề xuất các phương pháp mới dựa trên chuỗi Markov nhằm giảm thiểu những tác động của các cuộc tấn công DoS.

Trong mạng lưới các lớp trung gian cung cấp nền tảng cho việc thực hiện bảo mật trên hệ thống mạng lưới toàn diện. Hệ thống mạng lưới sử dụng an ninh vững chắc dựa trên PKI và chứng chỉ X.509. Mô hình chứng thực người sử dụng trong mạng lưới cung cấp sự an toàn chống lại sự đe doạ bởi những nguồn và những hoạt động bất hợp pháp bởi những người sử dụng nội tại.

An ninh của hệ thống lưu trữ phân tán chủ yếu tập trung vào bảo mật dữ liệu. Các lĩnh vực chủ yếu tập trung vào lưu trữ phân tán được bảo vệ chống lại sự mục nát dữ liệu và bảo vệ dữ liệu trong tình huống các nút bị lỗi. Các nhà nghiên cứu đã đề xuất nhiều mô hình khác nhau và các chương trình để bảo vệ hệ thống lưu trữ chống lại các cuộc tấn công và hư hỏng ở các nút.

Trong hệ thống cơ sở dữ liệu phân tán, an ninh được thực hiện phức tạp hơn do sự có sẵn nhiều mô hình cơ sở dữ liệu khác nhau. Như các nhà nghiên cứu chỉ ra bằng cách áp dụng nhiều mức độ bảo mật dựa vào việc phân loại lượng thông tin và kiểm soát truy cập. Bảo mật cơ sở dữ liệu có thể được tăng cường.