ỦY BAN NHÂN DÂN TỈNH SÓC TRĂNG

**SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG**

🙢🙠🕮🙡🙣

**BÁO CÁO**

**KIẾN TRÚC VỀ CÔNG NGHỆ**

**HẠNG MỤC**

**XÂY DỰNG KHUNG KIẾN TRÚC CÔNG NGHỆ THÔNG TIN NGÀNH TÀI NGUYÊN VÀ MÔI TRƯỜNG**

**SÓC TRĂNG, NĂM 2019**

**MỤC LỤC**

[DANH MỤC HÌNH ẢNH 3](#_Toc24441195)

[1. ĐẶT VẤN ĐỀ 4](#_Toc24441196)

[2. CÁC CÔNG NGHỆ LIÊN QUAN ĐẾN HẠ TẦNG CÔNG NGHỆ THÔNG TIN 4](#_Toc24441197)

[2.1. Lớp hạ tầng tính toán 4](#_Toc24441198)

[2.2. Lớp hạ tầng IoT (Internet Of Things) 5](#_Toc24441199)

[2.3. Lớp mạng (NetWorking) 8](#_Toc24441200)

[3. CÁC CÔNG NGHỆ DÀNH CHO PHẦN MỀM 8](#_Toc24441201)

[3.1. Các công nghệ phần mềm hệ điều hành 8](#_Toc24441202)

[3.2. Các công nghệ phần mềm quản trị cơ sở dữ liệu 9](#_Toc24441203)

[3.3. Các công nghệ phần mềm cổng thông tin, trục tích hợp, dịch vụ Web 9](#_Toc24441204)

[3.4. Các công nghệ phần mềm hệ thống thông tin địa lý 11](#_Toc24441205)

[3.5. Các công nghệ phần mềm ứng dụng khác 13](#_Toc24441206)

[4. CÁC CÔNG NGHỆ DÀNH CHO PHÁT TRIỂN ỨNG DỤNG 13](#_Toc24441207)

[5. CÁC CÔNG NGHỆ PHẦN MỀM DÀNH CHO MÔ HÌNH HÓA TÀI NGUYÊN VÀ MÔI TRƯỜNG 14](#_Toc24441208)

[6. KIẾN TRÚC VỀ AN NINH, AN TOÀN THÔNG TIN 15](#_Toc24441209)

[6.1. An toàn thông tin 15](#_Toc24441210)

[6.2. Bảo vệ thông tin riêng tư (cá nhân, privacy) 18](#_Toc24441211)

[6.3. Quản lý định danh 19](#_Toc24441212)

[7. KẾT LUẬN 23](#_Toc24441213)

# **DANH MỤC HÌNH ẢNH**

[Hình 1. Kiến trúc hệ thống IoT dựa trên nền tảng công nghệ điện toán đám mây 6](#_Toc24441247)

[Hình 2. Các tiêu chuẩn, giao thức cho hệ thống IoT 7](#_Toc24441248)

[Hình 3. Cấu trúc của hệ thống chính sách an toàn thông tin. 16](#_Toc24441249)

[Hình 4. Khung an ninh bảo mật chung cho hệ thống thông tin quản lý ngành tài nguyên và môi trường. 17](#_Toc24441250)

[Hình 5. Khung kiến trúc về công nghệ và tiêu chuẩn áp dụng cho hệ thống thông tin quản lý tài nguyên và môi trường 22](#_Toc24441251)

# **ĐẶT VẤN ĐỀ**

Báo cáo kiến trúc về công nghệ sẽ đề cập đến các giải pháp công nghệ trong và ngoài nước, cũng như tài nguyên mã nguồn mở để đáp ứng các yêu cầu, các nguyên tắc đã được đề xuất trong kiến trúc nghiệp vụ, kiến trúc dữ liệu, kiến trúc hệ thống và ứng dụng.

Nội dung các giải pháp công nghệ được đưa ra chỉ có tính chất tham chiếu trong quá trình triển khai hiện thực hóa các ý tưởng của khung kiến trúc công nghệ thông tin ngành tài nguyên và môi trường vào thực tế vì các giải pháp công nghệ luôn luôn phát triển rất mạnh mẽ và nhanh chóng. Việc cập nhật các công nghệ mới sẽ được thực hiện trong quá trình vận hành, giám sát và cập nhật kiến trúc hàng năm.

Các giải pháp công nghệ dưới đây chỉ là các giải pháp cơ bản nhất để xây dựng hệ thống thông tin quản lý tài nguyên và môi trường. Trong quá trình triển khai, ngành tài nguyên và môi trường sẵn sàng xem xét, cân nhắc mọi giải pháp công nghệ khác do các doanh nghiệp, viện, trường đại học đề xuất để đạt được mục tiêu chung.

# **CÁC CÔNG NGHỆ LIÊN QUAN ĐẾN HẠ TẦNG CÔNG NGHỆ THÔNG TIN**

Các công nghệ liên quan đến hạ tầng công nghệ thông tin sẽ tuân theo định hướng của Kiến trúc chính quyền điện tử tỉnh Sóc Trăng - phiên bản 1.0, và Kiến trúc Chính phủ điện tử Bộ Tài nguyên và Môi trường – phiên bản 1.0. Đồng thời, các công nghệ này cũng tuân theo xu hướng phát triển công nghệ thông tin trong và ngoài nước, cụ thể như sau:

## Lớp hạ tầng tính toán

Có nhiều cách để triển khai các hạ tầng tính toán cung cấp tài nguyên máy chủ, mạng, lưu trữ nhưng theo xu thế hiện nay, phần lớn các hệ thống lớn trên thế giới đều lựa chọn hệ thống điện toán đám mây bởi tính hiệu quả và tối ưu. Hệ thống thông tin quản lý ngành tài nguyên và môi trường cần hướng tới hệ thống điện toán đám mây với mức cung cấp dịch vụ PaaS (Platform as a Service – tạm dịch là Nền tảng như một dịch vụ) và SaaS (Software as a Service – tạm dịch là Phần mềm như một dịch vụ), ở đó các môi trường, nền tảng cho ứng dụng, dịch vụ chung của tỉnh đã được xây dựng, tích hợp sẵn giúp nâng cao tính tự động hóa, tiết kiệm thời gian và chi phí triển khai cho các đơn vị. Tuy nhiên, với mô hình điện tử trao đổi dữ liệu mà kiến trúc đã đề xuất, khái niệm SaaS còn được hiểu là Service as aService, có nghĩa sẽ hình thành một đám mây bao gồm rất nhiều dịch vụ Web, chứ không chỉ là phần mềm.

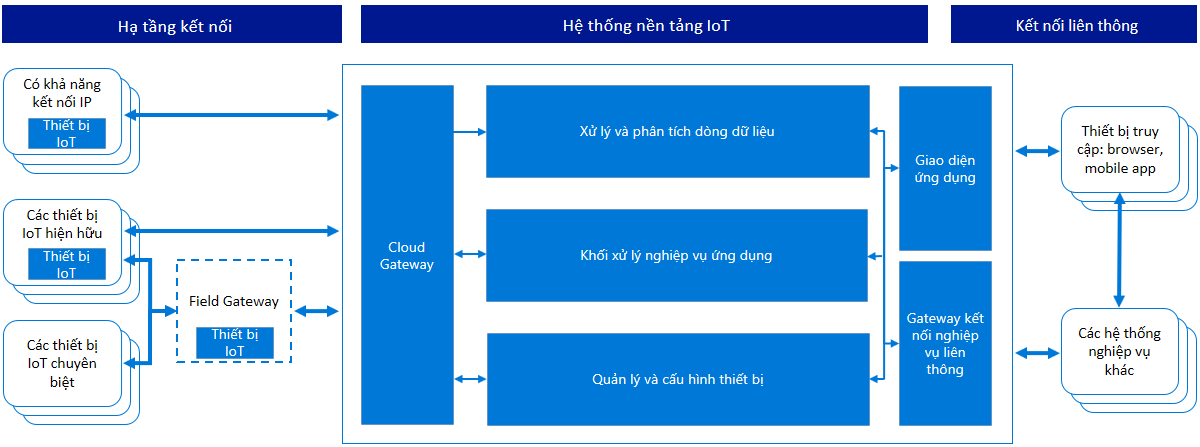
Bên cạnh đó, trong sự phát triển của công nghệ điện toán đám mây, mô hình triển khai điện toán đám mây được định nghĩa bởi phần mềm (Software-defined Cloud Computing, gọi tắt là SDC) đang được các nhà cung cấp hàng đầu trên thế giới như Google, Amazon, Microsoft,... xây dựng và phát triển bởi sự linh động, tối ưu, tiết kiệm chi phí hơn rất nhiều so với các hệ thống điện toán đám mây truyền thống. Với mô hình triển khai SDC, tất cả mọi thành phần của hệ thống bao gồm máy chủ, mạng kết nối, lưu trữ đều được định nghĩa theo phần mềm, ảo hóa và cung cấp như các dịch vụ một cách linh động, tự động cao. Đây là mô hình triển khai Điện toán đám mây mà kiến trúc cần hướng tới trong nhiều năm nữa để bắt kịp xu hướng công nghệ trên thế giới.

## Lớp hạ tầng IoT (Internet Of Things)

Đối với lớp hạ tầng, để đáp ứng nhu cầu chia sẻ và xử lý thông tin liên tục của ngành Tài nguyên và Môi trường, đặc biệt là hệ thống thông tin quan trắc của ngành. Một trong những thành phần hạ tầng chính trong khung kiến trúc công nghệ thông tin tài nguyên và môi trường là các hệ thống ứng dụng IoT trong hệ thống thông tin quan trắc tài nguyên và môi trường. Với các ứng dụng IoT, mọi sự vật, hiện tượng tại tỉnh đều được lắng nghe, tương tác thông qua các thiết bị cảm biến, camera, di động, các thiết bị đo đạc thông minh… Mọi thông tin, dữ liệu từ các thiết bị IoT phục vụ quan trắc được truyền về Trung tâm Quan trắc Tài nguyên và Môi trường để xử lý tập trung giúp tỉnh có thể hiểu rõ hiện trạng, phân tích nắm bắt xu hướng các sự thay đổi liên quan đến tài nguyên và môi trường, từ đó giúp địa phương nâng cao chất lượng các dịch vụ cung cấp cho người dân, giảm tình trạng ô nhiễm môi trường, sự cố môi trường, giám sát quy hoạch,... và đáp ứng kịp thời sự thay đổi của thế giới thực.

Kiến trúc cho hệ thống IoT phải tuân thủ các nguyên tắc:

* Tính đa dạng: Phù hợp với nhiều kịch bản, môi trường, thiết bị và các ứng dụng khác nhau.
* Khả năng bảo mật: Xem xét và đo lường khả năng bảo mật, sự riêng tư xuyên suốt từng thành phần của hệ thống.
* Khả năng mở rộng: Phải có khả năng hỗ trợ hàng triệu thiết bị kết nối.
* Tính linh hoạt: Phải có khả năng kết hợp và mở rộng linh hoạt để cho phép sử dụng nhiều công nghệ của nhiều nhà cung cấp khác nhau.



Hình . Kiến trúc hệ thống IoT dựa trên nền tảng   
công nghệ điện toán đám mây

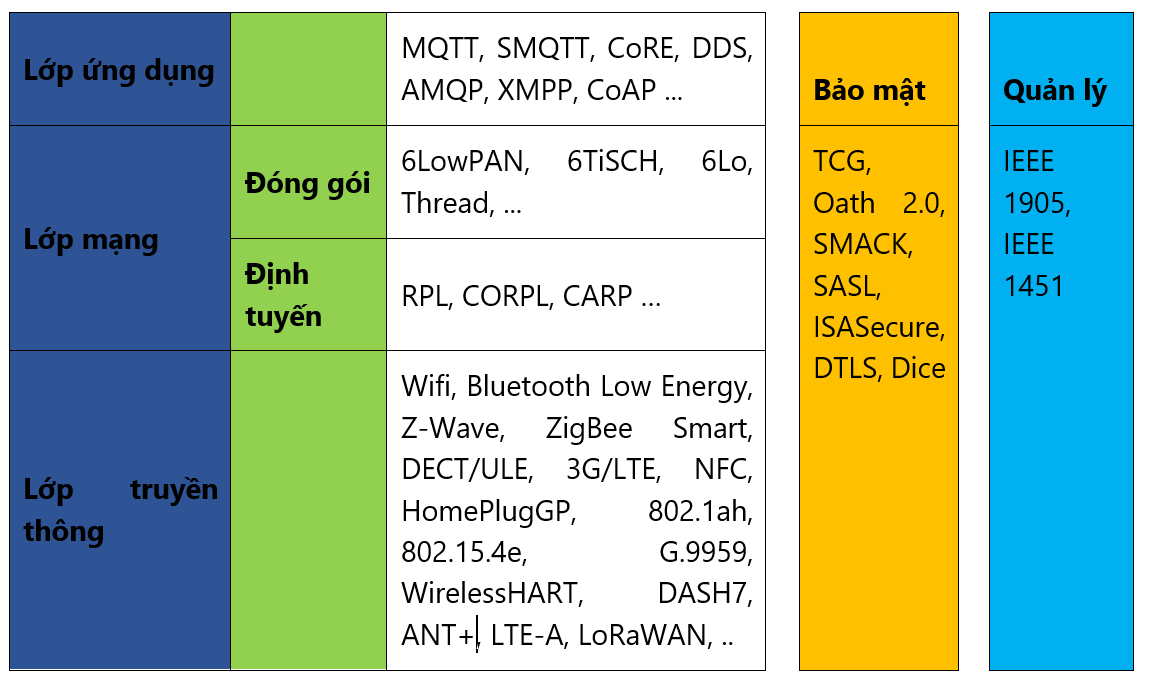
Hệ thống IoT bao gồm 3 khối chức năng chính:

* Hạ tầng kết nối: Bao gồm thiết bị IoT đa dạng chủng loại như thiết bị cảm biến, camera có thể kết nối trực tiếp hoặc gián tiếp về hệ thống nền tảng IoT thông qua trạm kết nối (Field Gateway) sử dụng nhiều giao thức truyền thông khác nhau. Kết nối từ các cổng kết nối về nền tảng IoT có thể sử dụng hệ thống mạng WAN/LAN hiện hữu hoặc sử dụng kết nối không dây (wifi, 3G/4G, ZigBee Smart, LoRaWAN...) tùy vị trí lắp đặt của nó.
* Nền tảng IoT: Hệ thống bao gồm nhiều thành phần có chức năng phát hiện, đăng ký và giám sát thiết bị; thu thập, chuyển đổi và phân tích dữ liệu; thực hiện các nghiệp vụ ứng dụng yêu cầu.
* Hiển thị và Kết nối liên thông: Đưa ra các giao diện ứng dụng và chịu trách nhiệm tích hợp với các hệ thống công nghệ thông tin khác.

Khung bảo mật hệ thống IoT: Hiện nay các hệ thống IoT đang trở thành một mục tiêu tấn công ngày càng phổ biến. Vì vậy, song song với việc xây dựng hạ tầng nền tảng IoT thì một khung bảo mật toàn diện xuyên suốt toàn hệ thống là một vấn đề cực kỳ quan trọng. Khung bảo mật tham khảo bao gồm 04 thành phần chính:

* Hệ thống xác thực (Authentication): Cung cấp khả năng kiểm tra, xác thực định danh các thiết bị IoT truy cập vào hạ tầng dựa trên các thông tin định danh như RFID, X.509 Certificate, MAC address...
* Hệ thống cấp phép (Authorization): Cung cấp khả năng cấp phép quyền hạn truy cập của thiết bị trên hạ tầng mạng dựa trên định danh thiết bị đã được xác thực.
* Các chính sách mạng (Network Enforced Policy): Xây dựng và thực hiện các cơ chế và giao thức cho các loại lưu lượng mạng, đảm bảo mức độ an ninh cho hạ tầng.
* Hệ thống phân tích bảo mật (Security Analytic): Thực hiện thu thập và phân tích thông tin từ tất cả các phần tử trên hạ tầng mạng, từ đó đưa ra các nguy cơ và hành động cần thiết để khắc phục.

Các tiêu chuẩn về hệ thống IoT: Trong việc thiết kế, xây dựng hệ thống IoT cho tỉnh thì khả năng tương thích, mở rộng của hệ thống nền tảng IoT là vấn đề quan trọng nhất. Để làm được điều đó, các thiết bị, các phân lớp dịch vụ trong hệ thống phải tuân theo các tiêu chuẩn, giao thức phát hành bởi các tổ chức uy tín như: IEEE, IETF, ITU... và đã được khuyến nghị sử dụng bởi các liên minh lớn trên thế giới về IoT như: AllSeen Alliance, OneM2M…



Hình . Các tiêu chuẩn, giao thức cho hệ thống IoT

Một số lợi ích cho việc xây dựng hệ thống nền tảng IoT được xác định như sau:

* Việc xây dựng các tiêu chuẩn thiết kế mở xuyên suốt từng phân lớp của hệ thống hỗ trợ khả năng kết nối nhiều nền tảng IoT khác nhau, đáp ứng nhiều giải pháp, ứng dụng cũng như là các thiết bị IoT khác nhau.
* Sử dụng chung các hệ thống phân tích dữ liệu lớn, kho dữ liệu dùng chung, trục tích hợp đã được trình bày ở các lớp trước thông qua đó nâng cao hiệu quả sử dụng tài nguyên, tăng cường tính liên thông, kết nối giữa các ứng dụng, tối ưu hóa, tiết kiệm chi phí cho các hệ thống lưu trữ, xử lý, phân tích dữ liệu từ các hệ thống IoT.
* Sử dụng nền tảng điện toán đám mây giúp tiết kiệm chi phí, khả năng mở rộng nhanh chóng theo yêu cầu. Điều này đặc biệt quan trọng trong việc xây dựng từng nhóm các dịch vụ thông minh trong tầm nhìn dài hạn.
* Đảm bảo tính xuyên suốt, nhất quán trong việc quản lý bảo mật, an ninh, an toàn dữ liệu.

## Lớp mạng (NetWorking)

Khung kiến trúc chính quyền điện tử ngành tài nguyên và môi trường sử dụng hệ thống mạng diện rộng WAN của tỉnh. Theo đó, hệ thống mạng diện rộng WAN được hoàn thiện để tạo một môi trường kết nối băng thông rộng, bảo mật cao đến tất cả các cơ quan Chính quyền (từ cấp tỉnh đến cấp xã), phục vụ việc triển khai ứng dụng và quản lý nhà nước, đồng thời cung cấp dịch vụ công cho người dân và doanh nghiệp một cách thuận tiện nhất.

# **CÁC CÔNG NGHỆ DÀNH CHO PHẦN MỀM**

## Các công nghệ phần mềm hệ điều hành

**Nguyên tắc:** Hệ điều hành được sử dụng trong hệ thống thông tin quản lý ngành tài nguyên và môi trường là các hệ điều hành đáp ứng các yêu cầu sau:

* Hệ điều hành có tính thông dụng và có được sự hỗ trợ cần thiết khi cần nâng cấp và giải quyết sự cố.
* Hệ điều hành hỗ trợ tất cả các ứng dụng trong ngành tài nguyên và môi trường
* Hệ điều hành phải quen thuộc với chuyên viên công nghệ thông tin trong ngành tài nguyên và môi trường.

Đề xuất:

Có hai hệ điều hành chính dành cho các máy chủ là:

* Hệ điều hành Window Server của hãng Microsoft: Là hệ điều hành rất thông dụng tại Việt Nam và trên thế giới.
* Hệ điều hành mã mở Linux với nhiều dòng khác nhau (Ubuntu, CentOS, RedHat, Mandrake, Debian,…): Được ứng dụng nhiều trong các hệ thống máy chủ tại Việt Nam và thế giới.

Tương tự như trên, các máy trạm, máy tính làm việc sẽ ưu tiên sử dụng hệ điều hành Window và các phiên bản Linux dành cho máy tính.

Các ứng dụng trên thiết bị di động cần phải đáp ứng chạy trên các hệ điều hành như: iOS, Android và Windows phone,…

## Các công nghệ phần mềm quản trị cơ sở dữ liệu

Nguyên tắc:

* Các phần mềm quản trị cơ sở dữ liệu phải đáp ứng và minh chứng khả năng lưu trữ, quản lý, đáp ứng xử lý với khối lượng dữ liệu lớn;
* Các phần mềm quản trị cơ sở dữ liệu phải đáp ứng được khả năng quản lý và xử lý dữ liệu không gian theo chuẩn của OGC Simple Features for SQL;
* Các phần mềm quản trị cơ sở dữ liệu có khả năng lưu trữ, quản lý và xử lý các ảnh quét và đặc biệt các ảnh vệ tinh với dung lượng lớn theo chuẩn Geotiff.

Đề xuất:

* Hệ quản trị cơ sở dữ liệu Oracle của hãng Oracle.
* Hệ quản trị cơ sở dữ liệu MS SQL Server của Microsoft.
* Hệ quản trị cơ sở dữ liệu DB2 của hãng IBM.
* Hệ quản trị cơ sở dữ liệu tài nguyên và mã mở PosgeSQL với plugin PostGIS

Các phần mềm quản trị cơ sở dữ liệu cụ thể sẽ được đầu tư sau khi xem xét tổng với việc phát triển ứng dụng, cơ sở dữ liệu và dựa vào nguồn nhân lực vận hành trong thực tế triển khai.

## Các công nghệ phần mềm cổng thông tin, trục tích hợp, dịch vụ Web

Nguyên tắc cho các giải pháp cổng thông tin

* Các giải pháp cổng thông tin tham gia vào hệ thống thông tin quản lý ngành tài nguyên và môi trường phải đáp ứng được các yêu cầu đối với nghiệp vụ, dữ liệu và ứng dụng đã trình bày ở các chương trước.
* Các giải pháp cổng thông tin có hỗ trợ BPMN hoặc BPEL.
* Các giải pháp cổng thông tin phải minh chứng được tính thông dụng, phổ cập và đã triển khai thành công tại Việt Nam và trên thế giới.
* Các giải pháp cổng thông tin phải đảm bảo nguồn lực hỗ trợ khi cần nâng cấp, phát triển và xử lý sự cố.

Đề xuất:

* Giải pháp cổng thông tin IBM WebSphere Portal của hãng IBM.
* Giải pháp cổng thông tin SharePoint của hãng Microsoft.
* Giải pháp cổng thông tin tài nguyên mã mở Liferay.
* Giải pháp tài nguyên mã mở Geonetwork để phát triển hệ thống đăng ký và công bố dịch vụ và dữ liệu tài nguyên và môi trường.

Các giải pháp cổng thông tin khác sẽ được xem xét trong quá trình triển khai hệ thống thông tin tài nguyên và môi trường.

Nguyên tắc cho các giải pháp trục tích hợp (Enterprise Service Bus)

* Các giải pháp công nghệ trục tích hợp cần đáp ứng các yêu cầu về kiến trúc nghiệp vụ, dữ liệu và ứng dụng đã đề xuất.
* Các giải pháp công nghệ trục tích hợp phải minh chứng được khả năng vận hành ổn định, chịu tải cao và khả năng quản lý, đảm bảo hiệu năng của các giao dịch.

Đề xuất:

* Tham khảo các giải pháp trục tích hợp trên thế giới hiện nay theo bảng sau:

<https://en.wikipedia.org/wiki/Comparison_of_business_integration_software>

* Ưu tiên sử dụng giải pháp trục tích hợp IBM Integration Bus của IBM
* Ưu tiên sử dụng giải pháp trục tích hợp tài nguyên mã mở WSO2 ESB
* Ưu tiên sử dụng giải pháp Biztalk Server của Microsoft

Các giải pháp công nghệ trục tích hợp sẽ được xem xét tổng thể nhiều khía cạnh trong quá trình triển khai hệ thống thông tin tài nguyên và môi trường.

Nguyên tắc cho các giải pháp xây dựng dịch vụ Web:

**Nguyên tắc:** Các giải pháp xây dựng dịch vụ Web phải đáp ứng yêu cầu đối với các tiêu chuẩn, các chuẩn đề ra với từng loại dịch vụ Web theo chuẩn của W3C và OGC.

Đề xuất:

* Sử dụng các framework của các hãng nổi tiếng để phát triển các dịch vụ Web như Microsoft Visual Studio, Eclipse,…
* Sử dụng các gói có sẵn như Apache Axis, WSO2 Data Service,…
* Sử dụng các phần mềm máy chủ đã hỗ trợ tạo ra các dịch vụ Web như: Geoserver, ArcGIS Server, Deegree Server,…

## Các công nghệ phần mềm hệ thống thông tin địa lý

Nguyên tắc đối với các phần mềm GIS phía máy chủ (GIS Server)

* Các phần mềm GIS phía máy chủ phải đảm bảo kết nối với các hệ quản trị cơ sở dữ liệu để truy cập, truy vấn và xử lý dữ liệu.
* Các phần mềm GIS phía máy chủ phải đáp ứng các yêu cầu về chuẩn dịch vụ Web như đã đề xuất và đảm bảo hiệu năng vận hành khi phải đáp ứng nhiều yêu cầu.
* Các phần mềm GIS phía máy chủ phải tương thích với cả hai hệ điều hành là Linux và Windows.

Đề xuất:

* Phần mềm ArcGIS Server của hãng ESRI
* Phần mềm Bentley System của hãng Bentley
* Phần mềm tài nguyên mã mở GeoServer
* Phần mềm tài nguyên mã mở UMN Mapserver
* Phần mềm APOLO ERDRAS SERVER của hãng Hexagon Geospatial.

Tất cả các giải pháp công nghệ khác dành cho GIS phía máy chủ đều được cân nhắc, xem xét trong quá trình triển khai hệ thống thông tin quản lý ngành tài nguyên và môi trường.

Nguyên tắc đối với các phần mềm GIS phía ứng dụng (Desktop)

* Các ứng dụng GIS phía ứng dụng phải kết nối với các phần mềm GIS phía máy chủ hoặc với các hệ quản trị cơ sở dữ liệu để truy cập, truy vấn và xử lý dữ liệu.
* Các ứng dụng GIS phía ứng dụng phải đảm bảo cung cấp các chức năng cần thiết để phục vụ các nghiệp vụ chuyên môn của ngành.
* Các ứng dụng phải bảo đảm các giao tiếp truy cập dữ liệu theo chuẩn mở của OGC.
* Các ứng dụng GIS phía máy chủ phải đảm bảo hoạt động ổn định trên nền tảng hệ điều hành và hạ tầng công nghệ thông tin như đã đề xuất.

Đề xuất:

* Bộ ứng dụng ArcMap, ArcToolBox, ArcCatalogue và các ứng dụng plugin khác của hãng ESRI là được ưu tiên.
* Bộ ứng dụng Bentley Map của hãng Bentley.
* Ứng dụng tài nguyên mã mở Quantum GIS (QGIS).
* Ứng dụng tài nguyên mã mở gvSIG Desktop.
* Các ứng dụng tự phát triển đáp ứng được các nguyên tắc trên.

Nhu cầu ứng dụng GIS trong công tác quản lý là rất cao trong ngành tài nguyên và môi trường và luôn thay đổi nên các ứng dụng nói trên chỉ mang tính chất bắt buộc cần phải có. Ngoài ra quan điểm của khung kiến trúc công nghệ thông tin ngành tài nguyên và môi trường là khuyến khích và tạo điều kiện cho các giải pháp khác tiếp cận và tham gia ứng dụng trong ngành tài nguyên và môi trường. Tất cả các giải pháp khác đều được cân nhắc và xem xét trong quá trình triển khai xây dựng hệ thống thông tin ngành tài nguyên và môi trường.

Nguyên tắc đối với các phần mềm GIS trên nền tảng Web

* Các phần mềm GIS trên nền tảng Web phải hỗ trợ các giao tiếp chuẩn của dịch vụ Web theo các tiêu chuẩn đã yêu cầu.
* Các phần mềm GIS trên nền tảng Web phải đáp ứng được các yêu cầu khai thác và sử dụng dữ liệu tài nguyên và môi trường như đã quy định.
* Các phần mềm GIS trên nền tảng Web phải vận hành trên nhiều trình duyệt khác nhau như: Edge Browser, Chrome, Opera, Firefox,… và đảm bảo chạy được trên các thiết bị di động như Smartphone, Tablet, iPad,…

Đề xuất:

* Sử dụng các tài nguyên mã mở có sẵn dưới dạng Framework dành cho ứng dụng WebGIS để phát triển các ứng dụng đáp ứng nhu cầu sử dụng của ngành tài nguyên và môi trường và phục vụ nhân dân, cộng đồng.
* Ưu tiên sử dụng các framework tài nguyên mã mở như: Openlayer, Leaflet,…

Các ứng dụng GIS trên nền tảng Web rất thuận tiện cho việc phổ biến, cung cấp thông tin đến nhân dân và cộng đồng nói chung. Mỗi một ứng dụng Web trên nền tảng GIS thường chỉ phục vụ cho một số yêu cầu cụ thể nào đó nên nhu cầu ứng dụng GIS trên nền tảng Web là rất lớn và phong phú.

Các giải pháp xây dựng GIS trên nền tảng GIS luôn được cập nhật theo xu hướng công nghệ thế giới trong quá trình triển khai xây dựng hệ thống thông tin quản lý ngành tài nguyên và môi trường.

Nguyên tắc đối với các phần mềm GIS phục vụ tích hợp, chuyển đổi dữ liệu.

* Đáp ứng chuyển đổi dữ liệu CAD, GIS, Remote Sensing với tất cả các khuôn dạng khác nhau.
* Hỗ trợ tác nghiệp và dịch vụ trực tuyến và không trực tuyến.
* Hỗ trợ tích hợp, trích xuất dữ liệu, xử lý dữ liệu theo WorkFlow và đáp ứng các chuẩn đã đề xuất.
* Đáp ứng khả năng kết nối với các hệ quản trị cơ sở dữ liệu đã đề xuất (PostgreSQL, Orcale, MS SQL Server,…).
* Đáp ứng chuẩn OGC WPS (Web Processing Service)

Đề xuất:

* Sử dụng phần mềm FME ([Feature Manipulation Engine](https://www.google.com.vn/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&ved=0ahUKEwjKw7zSt9bVAhVBNrwKHduMCegQFgg5MAc&url=http%3A%2F%2Fgisgeography.com%2Ffme-software%2F&usg=AFQjCNHhmkvJ1TWsDA2YOTGJWxO6h3qWOw)) của hãng Safe Software (<https://www.safe.com/>).
* Tham khảo sử dụng các phần mềm mã nguồn mở khác như North 52 WPS.

## Các công nghệ phần mềm ứng dụng khác

Ngoài các phần mềm cơ bản nói trên, ngành tài nguyên và môi trường cũng rất cần trang bị nhiều phần mềm ứng dụng chuyên biệt khác để phục vụ công tác tạo lập, xử lý và phân tích số liệu và mô hình hóa dữ liệu.

* Các phần mềm ứng dụng liên quan đến thiết kế như Microstation, AutoCAD, Bình sai lưới tọa độ và độ cao, chuyển đổi tọa độ,…
* Các phần mềm liên quan đến xử lý và phân tích ảnh viễn thám như: ENVI, ERDAS IMAGINE, PCI Geomatica,…
* Các phần mềm ứng dụng liên quan đến mô hình hóa tài nguyên và môi trường như MIKE, SWAT,… và các phần mềm khác của các nhà khoa học Việt Nam.

# **CÁC CÔNG NGHỆ DÀNH CHO PHÁT TRIỂN ỨNG DỤNG**

**Nguyên tắc:** Các nền tảng phát triển ứng dụng (IDE) phải thông dụng và ổn định nhằm tận dụng được các nguồn lực trong và ngoài ngành tài nguyên và môi trường. Đồng thời sẵn sàng nhận được sự hỗ trợ khi cần hiệu chỉnh, nâng cấp và phát triển các ứng dụng.

Đề xuất:

* Sử dụng nền tảng môi trường phát triển ứng dụng của Microsoft .Net Framework, trong đó C# là ngôn ngữ lập trình chính.
* Sử dụng nền tảng môi trường lập trình Java J2EE của Sun Oracle.
* Sử dụng môi trường phát triển bằng PHP.

Các ngôn ngữ lập trình và các môi trường phát triển ứng dụng có thể thay đổi tùy thuộc và từng ứng dụng cụ thể nhưng các môi trường phát triển nói trên là sự lựa chọn ưu tiên cho mọi ứng dụng trong ngành tài nguyên và môi trường.

Ngoài ra, trong quá trình phát triển các ứng dụng có thể các sử dụng các thư viện lập trình và các gói javascript để tạo ra các ứng dụng Web hoặc ứng dụng Desktop. Một số thư viện cần tham khảo như sau:

* Các thư viện lập trình GIS của nền tảng ESRI API, ESRI ArcEngine,…
* Các thư viện mã mở như Geotools, GDAL/OGR, …

Các ngôn ngữ lập trình như R, Python cũng cần nghiên cứu và áp dụng trong các hệ thống liên quan đến GIS, đặc biệt trong các bài toán xử lý, phân tích và mô hình hóa dữ liệu không gian.

# **CÁC CÔNG NGHỆ PHẦN MỀM DÀNH CHO MÔ HÌNH HÓA TÀI NGUYÊN VÀ MÔI TRƯỜNG**

Có thể liệt kê một số phần mềm mô hình hóa như sau:

| **Các mô hình** | **Chức năng** |
| --- | --- |
| SWAT, HEC-RAS, LINGO, LINDO, MARKOV CHAIN, AHP, MODFLOW | Đánh giá chất lượng đất, nước, mô hình thủy lực – lũ, xử lý đa thứ bậc, chuỗi thay đổi Markov, tối ưu đơn và đa biến, Dòng chảy ngầm |
| SWAT, HEC-RAS, CLUMondo, MARKOV CHAIN, AHP | Đánh giá chất lượng đất, nước, mô hình thủy lực – lũ, xử lý đa thứ bậc, chuỗi thay đổi Markov, Mô phỏng biến động sử dụng đất |
| Gauss, Berliand, Isc3, Qual2k | Mô phỏng diễn tiến chất lượng không khí và nước |
| SWAT, HEC-RAS, MIKE 11, MARKOV CHAIN, AHP | Đánh giá chất lượng đất, nước, mô hình thủy lực – lũ, xử lý đa thứ bậc, chuỗi thay đổi Markov |
| CLUMondo | Mô phỏng biến động sử dụng đất |
| Gauss, MIKE, Qual2k | Mô phỏng diễn tiến chất lượng không khí và nước |
| MIKE 11 | Mô phỏng nước mặt |
| SWAT, MODFLOW | Mô phỏng nước ngầm |
|  | Các mô hình về khí, cháy nổ và phát thải chất hữu cơ từ thực vật |
| SWAT, MARKOV CHAIN, AHP | Đánh giá chất lượng đất, nước, mô hình thủy lực – lũ, xử lý đa thứ bậc, chuỗi thay đổi Markov |
| SWAT, MARKOV CHAIN, AHP | Đánh giá chất lượng đất, nước, mô hình thủy lực – lũ, xử lý đa thứ bậc, chuỗi thay đổi Markov |
| TOPON | Mô hình khí |

Ngoài ra còn nhiều phần mềm khác do các nhà khoa học trong nước nghiên cứu và xây dựng cũng cần phải ưu tiên quan tâm và tạo môi trường cộng tác để phát triển.

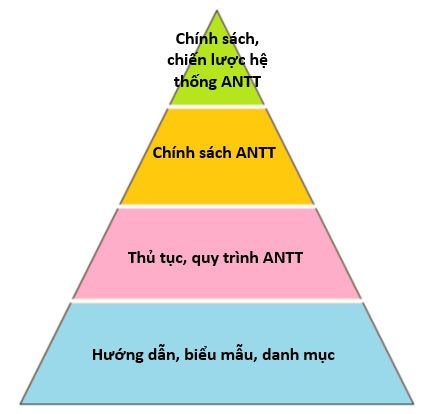
# **KIẾN TRÚC VỀ AN NINH, AN TOÀN THÔNG TIN**

## An toàn thông tin

Sự phát triển hệ thống thông tin quản lý ngành tài nguyên và môi trường theo kiến trúc đã đề xuất (kiến trúc hướng dịch vụ) sẽ đối mặt với thách thức và tiềm ẩn nguy cơ tấn công lớn hơn rất nhiều đối với hệ thống an toàn bảo mật thông tin. Cụ thể một số thách thức và rủi ro cho hệ thống an toàn bảo mật thông tin như:

* Các thiết bị IoT, điện toán đám mây thường được đặt tại các khu vực công cộng, do đó tiềm ẩn nguy cơ bị truy nhập trái phép.
* Nền tảng dịch vụ Web với việc cung cấp các cổng giao tiếp ngoài công cộng, là mục tiêu dễ bị tấn công mạng.
* Việc phát triển các trục liên thông kết nối ứng dụng tăng nguy cơ lây lan các phần mềm mã độc (malware, spyware).

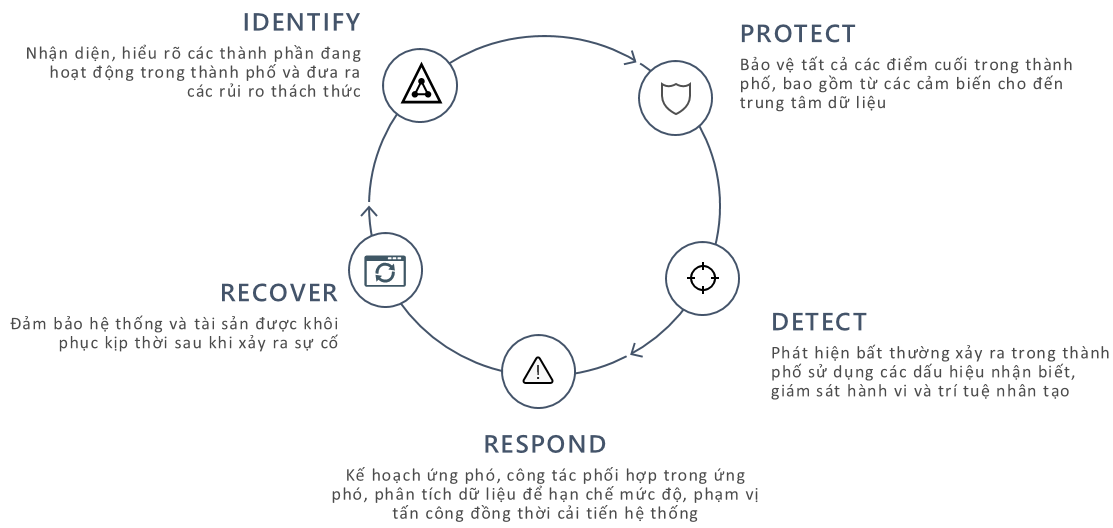
Các chính sách chiến lược, khung và các nguyên tắc triển khai an ninh thông tin cần tuân theo chuẩn ISO 27001



Hình . Cấu trúc của hệ thống chính sách an toàn thông tin.

* Mức 1: Chính sách, chiến lược hệ thống quản lý an ninh thông tin – Là chính sách ở mức cao nhất, mang tính chiến lược, quy định các nguyên tắc, các bên liên quan và liệt kê các chính sách cần được tuân thủ, thực thi của Tỉnh
* Mức 2: Bộ chính sách an toàn thông tin của Tỉnh
* Mức 3: Các thủ tục và quy trình được yêu cầu cho việc thực hiện, điều hành và giám sát
* Mức 4: Các hướng dẫn thực hiện và các biểu mẫu áp dụng trong quá trình tác nghiệp

Khung an ninh thông tin chung cho tỉnh được đề ra theo viện tiêu chuẩn và kỹ thuật quốc gia Mỹ (NIST) và theo tiêu chuẩn ISO 27001 về hệ thống quản lý an toàn bảo mật thông tin:



Hình . Khung an ninh bảo mật chung cho hệ thống thông tin quản lý ngành tài nguyên và môi trường.

Khung an toàn thông tin của NIST được sắp xếp theo dạng tiến trình với các thành phần chính như sau:

* Nhận diện – Identify (ID)
* Bảo vệ - Protect (PR)
* Phát hiện – Detect (DE)
* Ứng phó – Respond (RS)
* Khôi phục – Recover (RC)

Xác định các nguyên tắc triển khai an ninh thông tin:

* Xây dựng cách tiếp cận an ninh mạng (ANTT) dưới dạng quản lý rủi ro
* Xác định rõ ràng các mức độ ưu tiên
* Định nghĩa hệ thống an ninh ICT mức tiêu chuẩn (cơ bản)
* Sắp xếp và chia sẻ thông tin về các mối đe dọa cũng như các lỗ hổng của hệ thống
* Xây dựng năng lực đối phó với sự cố
* Tăng cường nhận thức xã hội, đào tạo, phát triển nguồn nhân lực
* Tăng cường hợp tác với xã hội, doanh nghiệp, tư nhân và các trường, viện

Đề xuất ngành tài nguyên và môi trường cần thực hiện xây dựng hệ thống an ninh thông tin hệ thống thông tin quản lý ngành tài nguyên và môi trường theo các bước cụ thể như sau:

* Xây dựng cơ chế chính sách trong đó phân chia thành các cấp:
* Xác định Khung an ninh thông tin và các giải pháp công nghệ cần thực hiện
* Xác định nguyên tắc triển khai an ninh thông tin

Triển khai an toàn thông tin theo lộ trình và mức ưu tiên được xây dựng dựa trên 3 bước trên.

## Bảo vệ thông tin riêng tư (cá nhân, privacy)

Sự phát triển bùng nổ của Internet cùng với các thiết bị di động kéo theo sự tăng lên nhanh chóng việc tương tác của người dân, doanh nghiệp với các dữ liệu của hệ thống thông tin quản lý tài nguyên và môi trường trên Internet. Kết quả của quá trình này là việc các công dân, doanh nghiệp khó kiểm soát được các thông tin riêng tư của mình, dẫn đến việc rò rỉ thông tin và sẽ xuất hiện nhiều “cạm bẫy” để lấy cắp thông tin riêng tư. Do đó nhiệm vụ của các hệ thống thông tin quản lý ngành tài nguyên và môi trường là phải đảm bảo sự riêng tư dữ liệu, đem lại sự yên tâm cho mỗi công dân, mỗi doanh nghiệp, tổ chức khai thác và sử dụng các dịch vụ thông tin, dữ liệu của hệ thống.

Đề xuất: Ngành tài nguyên và môi trường cần xây dựng các chính sách về bảo mật thông tin riêng tư cho người dân và doanh nghiệp. Ngành tài nguyên và môi trường cần phối hợp với Sở Thông tin và Truyền thông tổ chức rà soát các công tác triển khai chấp hành bảo vệ an ninh thông tin cá nhân theo mục 2, chương II của Luật an toàn thông tin mạng năm 2015 và ban hành các quy trình kiểm soát, quy định rõ mục đích và trách nhiệm sử dụng các dữ liệu cá nhân và doanh nghiệp trong hệ thống thông tin quản lý tài nguyên và môi trường, yêu cầu các giải pháp công nghệ được cung cấp cho hệ thống thông tin quản lý ngành tài nguyên và môi trường phải tuân thủ Luật và thực hiện kiểm định, đánh giá các giải pháp đảm bảo an ninh thông tin cá nhân trước khi cho phép triển khai, và ban hành những cơ chế chế tài, xử phạt nghiêm mang tính răn đe cao đối với các trường hợp cố ý vi phạm. Các chính sách được đưa ra phải đảm bảo cân bằng giữa yếu tố riêng tư và khả năng truy cập/phân tích dữ liệu nhằm cung cấp cho người dân/doanh nghiệp những dịch vụ ngày một tốt hơn. Các chính sách đề xuất cần quy định:

* Các tổ chức/cá nhân được sở hữu các tập dữ liệu nào.
* Quyền sở hữu bao gồm các quyền hạn và cơ chế bảo vệ nào.
* Các dữ liệu nào là riêng tư (phải được cho phép, xác thực mới được truy cập).
* Các dữ liệu nào có thể chia sẻ với tỉnh hay với các tổ chức bên thứ ba.
* Các dữ liệu được chia sẻ bằng cách nào.
* Các chính sách công khai về tính riêng tư giúp tiết kiệm thời gian, tiền bạc và khuyến khích các sáng tạo đột phá. Các tổ chức/doanh nghiệp sẽ dễ dàng hơn để phát triển sản phẩm, dịch vụ cho người dùng khi họ nắm rõ các chính sách này.

## Quản lý định danh

Hệ thống quản lý định danh được mô tả là sự quản lý riêng từng cá nhân trong việc xác thực, cấp quyền, vai trò, sự ưu tiên cho mỗi cá nhân trong phạm vi một hệ thống công nghệ thông tin hay giữa nhiều hệ thống công nghệ thông tin. Hiện nay trên thế giới các tổ chức doanh nghiệp thường sử dụng cơ chế đăng nhập một lần, xác thực qua nhiều bước (single sign on – SSO) cho phép truy cập nhiều dịch vụ trong cùng một hệ thống của doanh nghiệp hay nhiều hệ thống.

Một khi nhu cầu khai thác và sử dụng dữ liệu tài nguyên và môi trường của người dân, doanh nghiệp và các tổ chức là tương đối lớn thì việc kiểm soát quyền truy cập và thống nhất định danh, tránh thủ tục rườm rà cho mọi thành phần tham gia hệ thống trong tỉnh là điều cần thiết. Việc triển khai hệ thống định danh còn giúp các lãnh đạo, chuyên viên, viên chức trong ngành tài nguyên và môi trường giảm thiểu thời gian truy cập, đơn giản hóa khi truy cập các ứng dụng khác nhau trong hệ thống thông tin quản lý tài nguyên và môi trường. Vì vậy việc triển khai hệ thống SSO cho các ứng dụng thông minh trở nên rất thiết thực.

Vai trò quan trọng của việc quản lý định danh trong hệ thống thông tin:

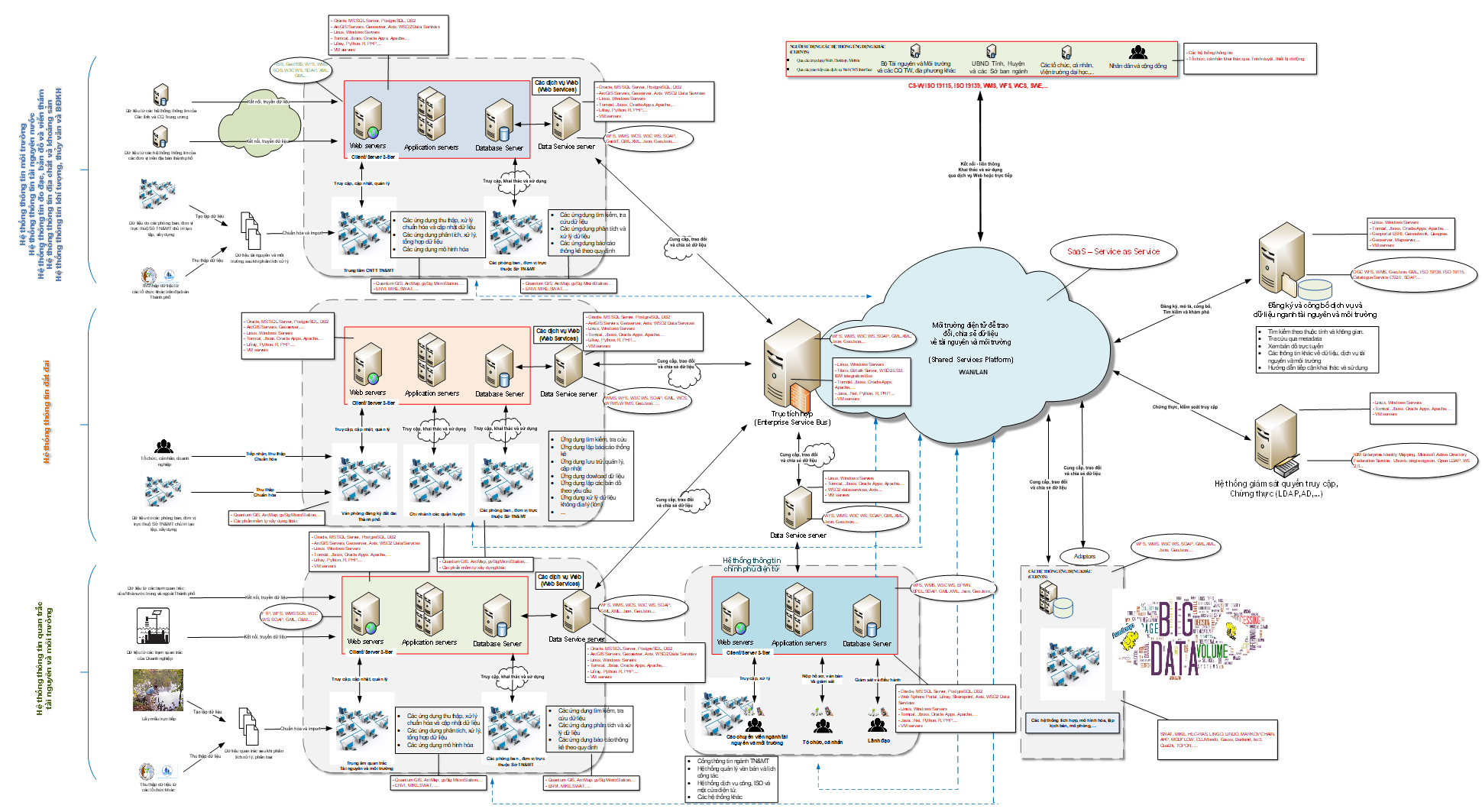
* Giúp minh bạch việc truy xuất hệ thống dữ liệu bằng cách gán cho mỗi người dùng theo vai trò trong tổ chức hiện hành, cấp quyền truy cập tài nguyên theo vai trò đó đồng thời có ghi log theo dõi từng hoạt động của mỗi người dùng trong hệ thống.
* Lợi ích của việc đăng nhập một lần (SSO) là giúp quản lý việc xác thực cũng như phân quyền dễ hơn, một cách thống nhất và minh bạch hơn khi người dùng chỉ cần một username và password là có thể đăng nhập vào các hệ thống thông tin trong cùng đơn vị hoặc giữa các đơn vị. Với hệ thống định danh hiện tại tồn tại rất nhiều hệ thống con với nhiều username và password khác nhau khiến cho việc giám sát, ghi log các hoạt động người dùng trở nên khó khăn và tốn nhiều tài nguyên hệ thống và nhân lực.
* Việc quản lý định danh cũng bao gồm sự mã hóa dữ liệu trao đổi trên toàn bộ hệ thống lớn (bao gồm tất cả các hệ thống nhỏ bên trong nó) theo quy trình khép kín bắt đầu từ lúc đăng nhập hệ thống cho đến lúc đăng xuất. Vì vậy dữ liệu sẽ được an toàn trao đổi bên trong hệ thống lớn mà không cần lo đến công đoạn hay hệ thống con nào sẽ phải mã hóa dữ liệu.
* Việc xác thực cấp quyền theo vai trò sẽ được quản lý tập trung vào một phòng ban duy nhất vì vậy sẽ dễ dàng hơn cho việc phân chia tập trung sử dụng tài nguyên con người, hệ thống quản lý định danh sẽ được tập trung đầu tư bảo vệ hơn là tách rời từng phòng ban một nhóm quản lý định danh riêng.
* Việc xác thực qua nhiều bước giảm thiểu tối đa nhiều lỗ hổng bảo mật khi người dân chỉ cần đăng nhập một lần mà vào được nhiều hệ thống.

Mô hình cơ chế đăng nhập một lần cho hệ thống thông tin quản lý ngành tài nguyên và môi trường (Enterprise SSO system): Hệ thống SSO bao gồm một cơ sở dữ liệu về chứng thư người dùng (credential database), các ứng dụng liên kết (affiliate applications – là các thực thể logic đại diện cho một hệ thống con trên hệ thống lớn ví dụ một host, một hệ thống back-end hay một ứng dụng phục vụ công việc mà sử dụng Enterprise SSO), một server khóa bảo mật cấp cao nhất (master secret server), và các server thành viên đăng nhập một lần (SSO server) có sử dụng đến khóa bảo mật của master secret server:

* Credential Database: Là một cơ sở dữ liệu lưu trữ thông tin về các Affiliate applications, cũng như là thông tin người dùng đã được mã hóa cho tất cả các affiliate applications đó.
* Affiliate Application: Các affiliate applications có cơ chế lưu trữ việc ánh xạ xác thực quyền người dùng cho các hệ thống con mà nó đại diện cho. Ví dụ nó sẽ ánh xạ người dùng trong các server quản lý tập trung user cho toàn bộ hệ thống lớn (LDAP, Active Directory…) với người dùng đã tồn tại trước khi có SSO trong hệ thống con. Cơ chế này cho phép phân quyền cho từng hệ thống con rõ ràng, đặc biệt giúp nâng cấp hệ thống cũ lên hệ thống SSO mới dễ dàng hơn rất nhiều như ví dụ nêu ở trên => Điều này rất thích hợp cho tỉnh khi muốn nâng cấp lên hệ thống SSO cho toàn tỉnh mà vẫn giữ được nguyên cấu trúc từng hệ thống ứng dụng nhỏ trong nó.
* Master secret Server: Là Enterprise SSO server chứa khóa bảo mật cấp cao nhất. Tất cả các SSO servers khác đều phải xác thực trước và lấy khóa bảo mật này khi muốn xác thực một người dùng hay một affiliate application.
* SSO servers system: Là một hệ thống server có cấu trúc phần mềm tương tự master secret server nhưng ở cấp thấp hơn, chúng sử dụng affiliate applications ánh xạ user được quản lý tập trung theo LDAP, Active Directory… với user có trong từng hệ thống con, đồng thời sẽ làm công việc tìm kiếm chứng thư trong Credential database để xác thực người dùng đăng nhập cũng như hoạt động trong hệ thống. SSO servers được các admin sử dụng để duy trì cũng như mở rộng hệ thống SSO.

Một số giải pháp tiêu biểu của các nhà cung cấp hàng đầu thế giới như IBM Enterprise Identity Mapping, Microsoft Active Directory Federation Service, Facebook connect, Ubuntu single sign on, Open LDAP, …

Hệ thống thông tin quản lý ngành tài nguyên và môi trường cần xây dựng hệ thống quản lý định danh tập trung của nhóm các ứng dụng thông minh với mô hình đăng nhập một lần (SSO).



Hình . Khung kiến trúc về công nghệ và tiêu chuẩn áp dụng cho hệ thống thông tin quản lý tài nguyên và môi trường

# **KẾT LUẬN**

Kiến trúc an ninh và công nghệ đã điểm ra những vấn đề mấu chốt về an ninh và đề ra nhưng nguyên tắc cơ bản, các công nghệ cơ bản từ hạ tầng đến phát triển ứng dụng, tạo lập và xây dựng cơ sở dữ liệu nhằm thỏa mãn các nguyên tắc chung của nghiệp vụ, dữ liệu và hệ thống ứng dụng.

Tất cả các công nghệ được giới thiệu trong chương này có tính chất tham khảo chính và được ưu tiên áp dụng trong quá trình xây dựng hệ thống thông tin tài nguyên và môi trường dựa trên cơ sở bám sát thực trạng công nghệ hiện này trên thế giới và Việt Nam và dựa trên khả năng đáp ứng của thị trường, của ngành tài nguyên và môi trường đối với việc làm chủ công nghệ hiện đại.

Công nghệ và khoa học kỹ thuật luôn luôn phát triển với tốc độ cao, đặc biệt trong thời kỳ của cuộc cách mạng 4.0 hiện nay nên cần luôn theo dõi và tăng cường nghiên cứu để áp dụng các công nghệ tiên tiến nhất nhằm triển khai hiệu quả hệ thống thông tin quản lý ngành tài nguyên và môi trường như tầm nhìn và mục tiêu đã đề ra.