Simulation of security protocols in a SMART GRID system communication of electric vehicle charging system

Jesus Ortiz Sandoval
Universidad Técnica Federico Santa María
Valparaíso, Chile

Abstract

The following project presents an analysis of the impact of the configuration of a secure communication for the development of transactions in an electric vehicle system, evaluating the type of encryption algorithm and the size of the key to be used to determine the correct sizing taken as a development base a mixed connection topology using computer network simulation software GNS3.

Resumen

En el siguiente proyecto se plantea un análisis del impacto de la configuración de una comunicación segura para el desarrollo de las transacciones en un sistema de vehículos eléctricos, evaluando el tipo de algoritmo de encriptación y el tamaño de la llave a utilizar para determinar el dimensionamiento correcto tomando como base de desarrollo una topología mixta de conexión utilizando software de simulación de redes de computador GNS3.

INTRODUCCIÓN

Smart grid es un proyecto que involucra muchas disciplinas y que presenta muchos desafíos económicos, políticos y legislativos de los países que han decidido implementar esta tecnología. Una de las principales implementaciones de esta tecnología está relacionada con la estabilización de la carga en la red que puede verse afectada por la inclusión de vehículos eléctricos con los picos de energía que ocurren en el momento de la carga.

Además de poder controlar el comportamiento de la energía, también hay muchos desafíos, algunos principalmente en la infraestructura, porque cuando se establecieron las redes de distribución de electricidad, nunca imaginamos que la revolución tecnológica llegaría al punto que tenemos hoy, y el Se buscará la implementación de ciudades inteligentes.

Por esta razón, se están estudiando las diferentes arquitecturas que se pueden implementar en los sistemas de distribución de energía (DAS), evaluando las topologías, los costos y, sobre todo, permitiendo una transición rápida y efectiva.

Al querer implementar este tipo de proyectos en la vida real, para llevar a producción al tener un sistema conectado a internet, es necesario asegurarnos de la integridad de la información que se va a transmitir, por esto es necesario hacer un estudio sobre la forma de encriptar la información, asi como de asegurar que la información de cada transacción sea la correcta, en este trabajo se desea estudiar el impacto de un sistema de autenticación y encriptación de la información con la arquitectura tecnológica, haciendo evaluación cualitativa para determinar cual es la mejor solución posible de un conjunto finito de propuestas.

El siguiente informe se divide primero en una búsqueda de los trabajos relacionados con el área, luego un enfoque del problema a discutir, el modelado del sistema de encriptación y autenticación, la simulación y las pruebas funcionales de las arquitecturas de red propuestas en los dos estados propuestos. , para terminar con las conclusiones del proyecto.

Trabajos Relacionados

En el primer trabajo analizamos cómo se automatiza la generación de datos de entrada en programas para simular sistemas de distribución eléctrica, este tipo de programas nos permite analizar voltaje, armónicos, comportamientos anormales, y eso puede ser de gran ayuda para aumentar y evaluar diferentes arquitecturas de distribución en nodos inteligentes.[1]

Además de que para el enfoque de estos temas, debe hacer simulaciones, también encontramos un trabajo en el que evalúa el alto rendimiento de la arquitectura de comunicaciones en un sistema de distribución de electricidad orientado a países en desarrollo, esto es muy interesante y Chile actualmente por el G20 es consideró un país en vías de desarrollo, y este artículo evalúa algunos elementos, como la calidad de servicio (QoS) y el impacto de migrogrid en el tipo de arquitectura de comunicaciones que se debe elegir. [2]

Uno de los principales factores que conducen a este tipo de estudios es la introducción de vehículos eléctricos, y la necesidad de que estos conduzcan a las comunas a cargar sus baterías, en el siguiente trabajo se proponen algunos métodos de optimización. Inclusión de vehículos eléctricos en la red (V2G) [3]

Además, es necesario analizar la configuración de los sistemas eléctricos, las novedades que se pueden implementar para enfocarse en los sistemas de comunicación y poder hacer una evaluación de los resultados obtenidos, estos sistemas deben elegirse tomando como referencia la eficiencia y estabilidad del sistema [4]

PROBLEMA Y MARCO TEORICO

Esta área del conocimiento actualmente desarrolla muchos trabajos de investigación, referentes a tecnologías, arquitecturas, protocolos, distribución, etc. Pero también es relevante los estudios que se están haciendo para llevar a cabo una correcta distribución de esta tecnología referente a lo que son los sistemas de seguridad en la red, es importante determinar que lo que se desea es un sistema que no afecte la estabilidad del sistema, que permita tener una eficiencia en la comunicación y que asegure la integridad de la información en las transacciones, para esto nosotros con una arquitectura que ya ha sido evaluada y que tiene un correcto desempeño en términos de latencia en las estaciones se va a implementar un sistema de autenticación y encripta miento con dos tecnologías diferentes AES, RCA, además de diseñar el envió de un hash en cada transacción al usuario y a la empresa fuente del servicio , y vamos a cuantificar cuanto es el incremento de latencia, y si se mantiene en niveles adecuados de eficiencia de prestación del servicio.

EPON diseño y simulación

Utilizando un sistema basado en el protocolo Ethernet industrial junto con una red PON (red óptica pasiva), en esta arquitectura tenemos un OTL que es un transmisor óptico, cableado de fibra óptica, divisores de fibra óptica y unidades de recepción óptica de la ONU como se muestra en la figura 1. Para diseñar nuestra red, primero realizaremos el modelado de la red tomando como referencia la tabla 1 con los valores asociados con la atenuación de los componentes

y la pérdida de señal insertada en los divisores.

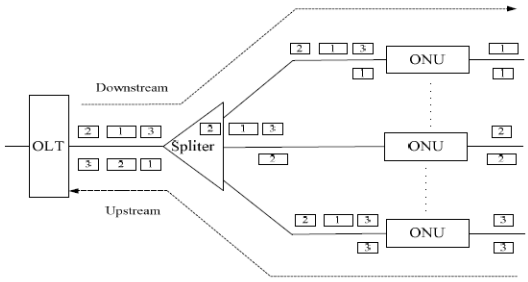

Figure 1. Arquitectura EPON [1]

Para poder realizar el modelado correcto, primero analizamos los tipos de arquitectura que se pueden implementar, lo que se desea en este caso es resolver uno de los principales problemas que ocurren en la transición de la red a una red inteligente, que son costos de implementación e infraestructura, para tal caso debemos aprovechar la misma arquitectura de distribución eléctrica, tomando para tal caso la infraestructura tipo bus como podemos analizar en la figura 2.

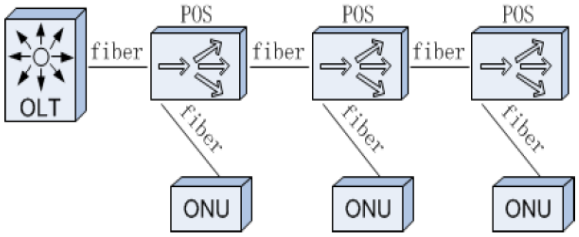

Figura 2. Arquitectura tipo BUS EPON [1]

Componente	**Atenuación**	Perdida insertada
Fiber	0.4 dB/Km	N/A
Connector	0.2 dB	N/A
Splitter 1x2	N/A	(5%-95%) (0.4dB -11dB)
Splitter 1x4	N/A	(25%-25%-25%-25%)(6dB-6dB-6dB-6dB-)

Tabla 1. Perdidas asociadas con cada elemento de la red

Para este estudio de caso, tomaremos como referencia un hipotético sistema de carga de vehículos eléctricos implementado en la Universidad Técnica Federico santa María, con referencia únicamente al alimentador 1 de la línea que tiene 11 unidades de carga, la idea principal de este diseño es que si el funcionamiento correcto del modelo y la simulación puede proceder a una implementación adecuada. En la figura 3 podemos ver el diagrama general de la arquitectura EPON propuesta, y la sección que se va a estudiar.

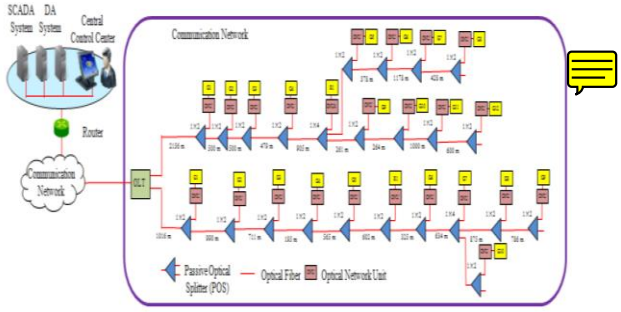

Figura 3. EPON for case of study.

Tomando como referencia el trabajo realizado por (Ahmed y Kim, 2019), evaluaremos su comportamiento, pero con una métrica diferente a la evaluada en el documento en cuestión. Dado que nos enfocamos en considerar la estabilidad de la red como un proceso crítico y queremos analizar la latencia de los dispositivos que pertenecen a la red inteligente y qué sucede con la latencia en el momento en que solo unos pocos vehículos están transmitiendo, o qué sucede cuando varios o incluso todos los vehículos están transmitiendo

Tabla 2. Resultados con arquitectura funcionando

	1-3 stations	4-10 stations	>10 stations
Charger 3-1-20	42 ms	42 ms	42 ms
Charger 3-1-18	40 ms	40 ms	40 ms
Charger 3-1-17	47 ms	47 ms	47 ms
Charger 3-1-16	36 ms	36 ms	36 ms
Charger 6-1-5	38 ms	38 ms	38 ms
Charger 5-1	22 ms	22 ms	22 ms
Charger 6-1-15	36ms	36ms	36ms
Charger 4-1-7	34 ms	34 ms	34 ms

Una vez implementada la arquitectura se hacen mediciones de latencias, con distancias entre 1 y 3 estaciones, 4 y 10 estaciones y más de 10 estaciones, lo que encontramos es que la latencia al estar conectados en una arquitectura estrella es la misma sin importar cuantas estaciones están en el medio de la comunicación.

Autenticación y cifrado

Es importante determinar que en un sistema adecuado de autenticación y cifrado de información entre un host y un usuario se tiene que cumplir unos ítems básicos como lo son, integridad de la información que se va a compartir, disponibilidad de los datos, y no repudio de la transacción.

Con estos preceptos claros, nosotros vamos a estudiar dos métodos de autenticación que será implementados en paralelo, para ver primero que ambos cumplan con los requisitos expuestos, además de ver cuál es el impacto en los resultados alcanzados en la simulación sin sistema de seguridad que se observan en la tabla 2.

AES

Advanced Encryption Standard (AES), es un esquema de cifrado por bloques creado en Bélgica. Este sistema está basado en una red de sustitución, AES es rápido tanto en software como en hardware, es bastante fácil de implementar, además actualmente es tan seguro que no ha sufrido ataques exitosos, solo en 2002 un posible ataque, pero en el que al parecer los autores cometieron errores en la matemática, por lo que el éxito de ese ataque se disolvió. AES tiene un tamaño de bloque fijo de 128 bits y diferentes tamaños de llave que van desde 128 hasta los 256 bits.

RSA (Rivest, Shamir, Adleman)

Es un sistema criptográfico de clave publica desarrollado en 1979, la seguridad de este algoritmo se encuentra en la factorización de numero enteros. La gran ventaja de este sistema es que su capacidad de computo aumenta con el crecimiento exponencial de la capacidad de calcula de las computadoras. El único problema que puede enfrentar este sistema de encripta miento serían los avances en computación cuántica, que sería capaz de descomponer rápidamente un numero grande, lo que volvería completamente obsoleto a este algoritmo.

METODOLOGIA PROPUESTA

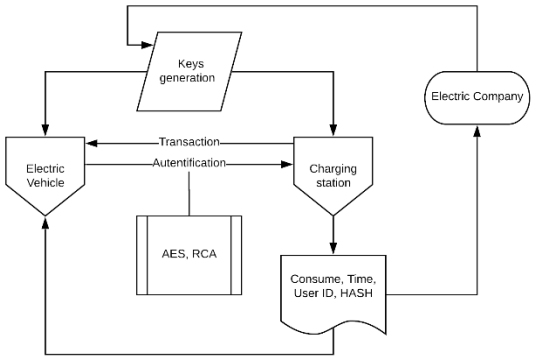

Figura 4. Metodologia de desarrollo propuesta.

, En la figura 4 encontramos nuestra propuesta de desarrollo de proyecto, utilizando la misma simulación para la arquitectura EPON lo que vamos a realizar es la implementación de este sistema de autenticación y cifrado, entre el servidor que se encarga de la administración de las estaciones de carga, y los vehículos que llegan

a hacer su respectiva transacción, en primer lugar, vamos a correr dos experimentos diferentes con los sistemas de encriptación AES y RSA, la generación de la llave estará a cargo del servidor central, por cada transacción vamos a crear un ticket que debe contener la información de consumo, tiempo, ID del usuario y un HASH que le será entregada al usuario y será almacenado en el servidor para verificar la integridad de las transacciones. En el momento que se esté desplegando el sistema y que se estén llevando a cabo transacciones, se ejecutaran las mismas pruebas de latencia, para ver si este sistema tiene algún impacto en la calidad de la comunicación, así como aleatoriamente se elegirán HASH para verificar la integridad de algunas transacciones realizadas.

RESULTADOS

LATENCIA	
ESTACION	**SERVIDOR**
EV1	1.0106 ms
EV2	1.0088 ms
EV13	3.8738 ms
EV15	3.2172 ms
EV20	4.2 ms
EV22	3.3624 ms
EV24	3.8118 ms
EV25	7.2036 ms
EV26	5.116 ms
EV27	4.8322 ms
EV32	5.2814 ms
EV33	5.1567 ms
EV35	5.757 ms

Tabla 3. Resultados con arquitectura funcionando

Debido a la incompatibilidad de Cisco Packet Tracer donde se realizo la primera parte del proyecto, se decide pasar a trabajar en GNS3. Packet Tracer no maneja sistemas operativos en sus servidores, lo que imposibilita la instalación de servicios o sistemas que son necesarios para el desarrollo de nuestro proyecto, es necesario instalar los siguientes servicios:

- Apache 2 servidor Web
- Servidor DNS usando BIND9
- Servidor FTP usando BIND9
- Generación de claves mediante OpenSSL

Con los elementos que cuenta Cisco PT, no se puede garantizar la configuración ni testing de 3 de los 4 servicios nombrados anteriormente, mientras que en GNS3 mediante el uso de una maquina virtual con Lubuntu y configuración de cloud para uso de internet podemos garantizar la instalación y configuración de todos los sistemas que fueron enumerados.

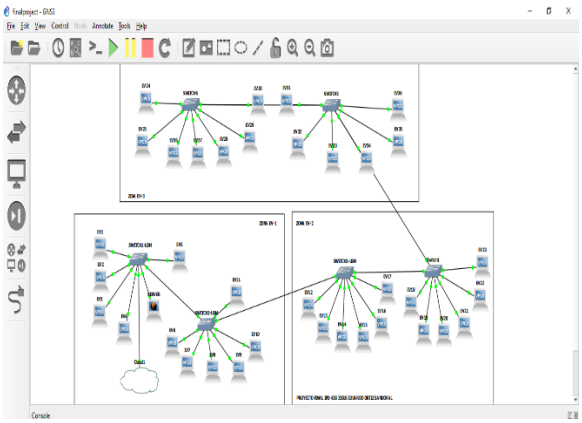

Figura 5. Diseño de propuesta de EV en USM

En la figura 5 encontramos la implementación que se hizo de las 3 zonas de carga de vehículos eléctricos en una topología mixta, utilizando bus en la conexión en los switches y una conexión en este alrededor de los elementos de red, con la conexión de un servidor principal en la Zona 1 de la configuración, utilizamos VPCs usando el servidor DHCP que provee la configuración cloud con router externo, además que se remplazaban en algunas estaciones por Lubuntu para hacer las pruebas de conexión con los servicios instalados. En la tabla 3 repetimos las mediciones que se hicieron con Packet Tracer para comprobar que los resultados tengan lógica antes de realizar la evaluación de los tiempos en el sistema desplegado completamente, y se puede garantizar que los tiempos aumentan a medida que la distancia aumenta desde el servidor central a las ultimas estaciones ubicadas en la zona 3 de carga del proyecto.

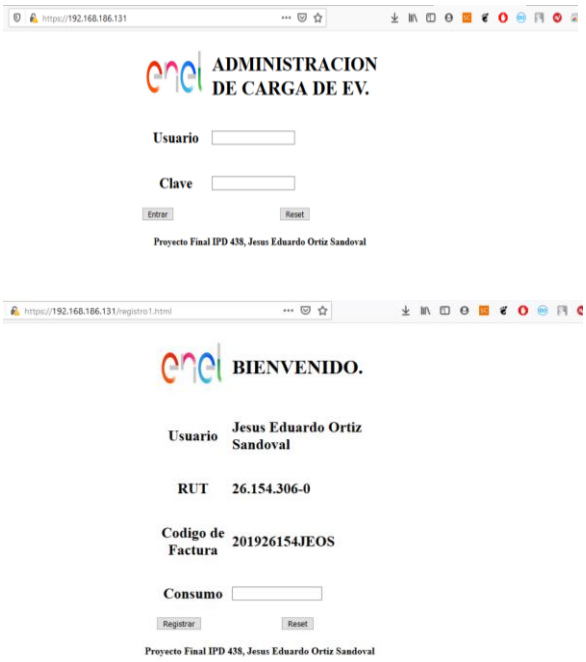

Figura 6. Página web para realizar las transacciones

Luego el primer servicio que configuramos es el servidor Apache2 para almacenar la pagina web que construimos básicamente en HTML junto con SQL para almacenar la información correspondiente de los usuarios, en este servidor es donde se instalan las llaves de autenticación utilizando AES con diferentes tamaño de llave que es la evaluación que se realiza de capacidad del servidor, en este apartado se instala también un servicio OpenSSL para poder generar las llaves que generan la comunicación segura entre el usuario y el servidor, cabe la pena resaltar que este proceso debe ser automático, nosotros simulamos de esta forma es para poder ver a la pagina que estamos accediendo y poder estar seguros de que al momento de automatizar todo el procesos efectivamente funciona como debe ser. Para garantizar que el certificado cumple con las especificaciones del algoritmo en el momento que se realiza la comunicación podemos dar clic en el candado que indica la comunicación segura y ver la información del certificado y de las llaves que fueron generadas para encriptar la comunicación, en la figura 7 podemos observar la información con la que se generaron las llaves.

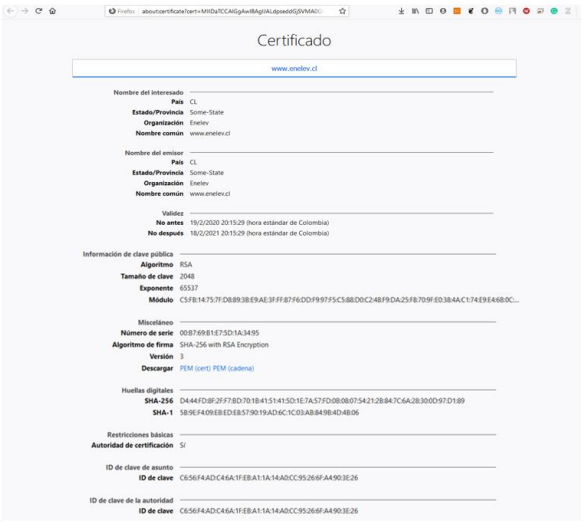

Figura 7. Certificado usando OpenSSL con tamaño de clave de 2048 bytes.

Con todo el sistema desplegado diseñamos la forma de evaluar el servidor y acercarnos a encontrar los resultados de este proyecto, obviamente no es relevante medir el ping desde los PC hasta el servidor, por que ellos solo miden el tiempo de respuesta lo que era necesario era poder medir los tiempos que se generaban al ingresar al sistema, tiempos de conexión y de espera, para este fin encontramos que el servidor Apache2 trae una herramienta llamada Apache Bench, con esta herramienta el procedimiento a realizar es cargar los certificados OpenSSl con diferente tamaño de llave, se reinicia el servidor Apache2 y realizar la medición del servidor, en las figura 8 y 9 encontramos el resultado de la medición del servidor, las llaves que se generan son de tamaño 2048 y 4096 utilizando algoritmo AES, acá lo interesante en los resultados es que se podría pensar es que el resultado seria lineal, pero por la capacidad de computo del algoritmo es exponencial.

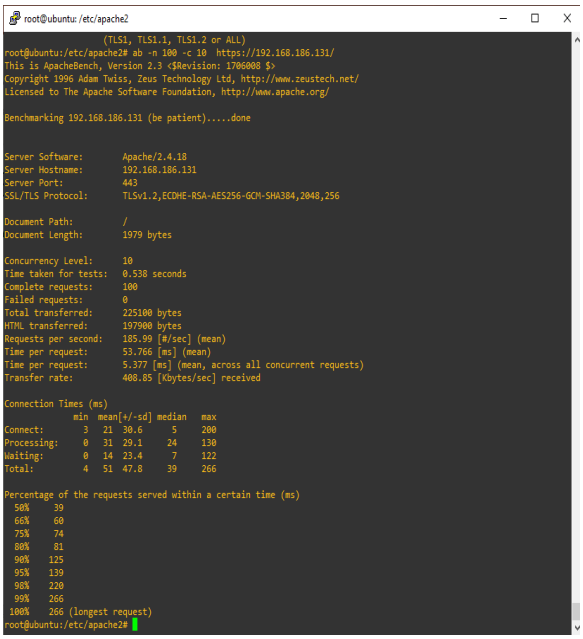

Figura 8. Metodología de desarrollo propuesta

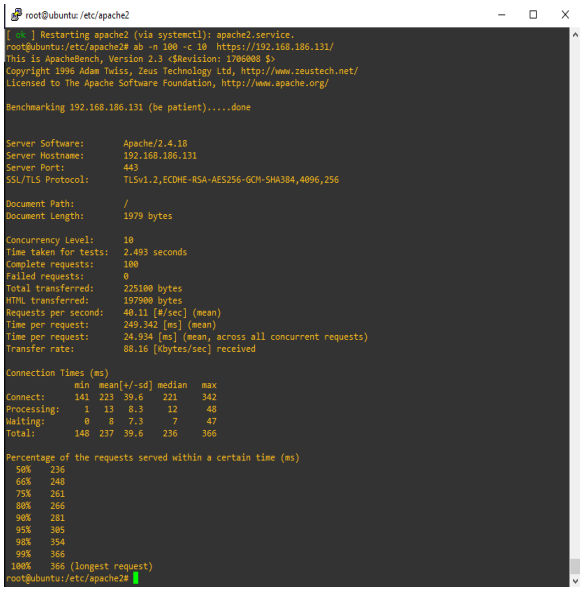

Figura 9. Metodología de desarrollo propuesta

Tamaño Llave	Conexión	Procesamiento	Espera
AES 2048	5 ms	24 ms	7 ms
AES 4096	221 ms	12 ms	47 ms

Tabla 4. Evaluación del servidor usando Apache Bench

Los resultados son bien claros, el tamaño de clave influye en la capacidad de computo del servidor de establecer la comunicación, sobre todo en la parte de conexión, pues es en el momento en que se intercambian las llaves, pero que de una llave a otra aumenta considerablemente, en tiempos de procesamiento y espera, los tiempos disminuyen pues los cálculos son tan pesados al inicio de la comunicación que luego esos tiempo disminuyen radicalmente, pero que si se evalúa el total de los tiempos la diferencia nos muestra que no es el doble como se esperaba, es una diferencia que radica en la capacidad de computo de la maquina donde se aloja el servicio HTTPS.

CONCLUSIONES

Aunque el trabajo se planteó originalmente como un estudio de seguridad en sistemas de grilla inteligente, debido al poco tiempo a la complejidad de realizar simulaciones a profundidad de sistemas completos solo pudimos estudiar el impacto de un espacio de comunicación segura bajo una pagina web donde se intercambia la información y se genera el reporte de la transacción que es almacenado en el servidor.

Este trabajo de estudio de sistemas seguros utilizando certificado OPENSSL, nos permite establecer cuanto es el costo en tiempo de escoger diferente tamaño de llaves para el intercambio de información, teniendo en cuenta las capacidades del servidor elegido, con esta información se puede determinar el nivel de escalabilidad de la implementación de un sistema SMART GRID teniendo en cuenta tecnología, arquitectura, configuración lógica y física de la red.

Debido a las limitaciones de configuraciones que entrega CISCO en su software de análisis de redes PACKET TRACER no se pudo desarrollar el proyecto como se planteo en un comienzo debido a que el servidor no permitía la configuración adecuada de los sistemas que iban a ser necesario para la evaluación del impacto de la seguridad en los sistemas eléctricos inteligentes, esto se debe a que Packet Tracer no maneja sistemas operativos reales Ubuntu, Windows, etc, si no maneja un OS básico sin

ninguna posibilidad de hacer configuraciones de instalación de llaves, paquetes, servicios o tampoco permitir la comunicación con el exterior mediante una maquina virtual, con todo lo que se encontró se tuvo que determinar que el software GNS3 es necesario para realizar el proyecto, pues tiene la escalabilidad necesaria para la implementación del proyecto, no se puede desconocer que Packet Tracer es bueno para analizar la arquitectura o topología de la red, pero este tipo de simulación no se puede evaluar en este programa.

Es interesante la forma en la que se puede configurar todo tipo de servicios en una máquina virtual pequeña Lubuntu que fue entregada en el ramo IPD438, se pudo desplegar un servidor Apache2, DNS, FTP además de que se instalo el servicio OpenSSL, para generar las llaves de encriptación usando AES con diferentes tamaños de claves que fueron herramienta para la evaluación del servidor en sus tiempos de ejecución para determinar cuál sería el tamaño ideal de encriptación en el que aun se mantengan los tiempo por debajo de 1s para manejar una fluidez con el usuario garantizando la máxima seguridad, esto también es bien interesante por que determina una forma de evaluar los servidores para este tipo de aplicaciones en los que se pueda asegurar con datos reales la capacidad de un servidor en torno a todos los servicios que puede ofrecer.

TRABAJOS FUTUROS

Se pueden diseñar otras pruebas con mas tipos de algoritmo de encriptación, que podrían ser evaluados no solo con latencia, si no con disponibilidad, no repudio, estabilidad del sistema y que también son elementos importantes para la implementación de estos proyectos.

Aunque en el servidor se desplego el algoritmo en JavaScript para generar un hash con string usando MD5 y que permita generar la seguridad en cada transacción, hizo falta fue la implementación con HTML, con Php ya se encuentra el código listo, entonces se pueden hacer muchas mas pruebas de seguridad para determinar un protocolo de análisis de sistemas de seguridad en Smart grid.

BIBLIOGRAFIA

[1] X. He, M. O. Pun, and C. C. J. Kuo, “Secure and efficient cryptosystem for smart grid using homomorphic encryption,” 2012 IEEE PES Innov. Smart Grid Technol. ISGT 2012, 2012, doi: 10.1109/ISGT.2012.6175676.

[2] F. Li, B. Luo, and P. Liu, “Secure Information Aggregation for Smart Grids Using Homomorphic Encryption,” pp. 327–332, 2010, doi: 10.1109/smartgrid.2010.5622064.

[3] Z. Zhang, K. T. Chau, C. Qiu, and C. Liu, “Energy encryption for wireless power transfer,” IEEE Trans. Power Electron., vol. 30, no. 9, pp. 5237–5246, 2015, doi: 10.1109/TPEL.2014.2363686.

[4] J. H. Im, H. Y. Kwon, S. Y. Jeon, and M. K. Lee, “Privacy-preserving electricity billing system using functional encryption†,” Energies, vol. 12, no. 7, pp. 1–15, 2019, doi: 10.3390/en12071237.

[5] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, “Smart-grid security issues,” IEEE Secur. Priv., vol. 8, no. 1, pp. 81–85, 2010, doi: 10.1109/MSP.2010.49.

[6] M. A. Ahmed and Young-Chon Kim, “System Architecture based on IoT for Smart Campus Parking Lots” International conference on Computer Applications & Information Security, ICCAIS'2019. 01-03 May, 2019.