Prototipo de sistema híbrido para la portabilidad de datos médicos usando cifrado por hardware y tecnología RFID

Trabajo Terminal No. 2019-B086

*Alumnos: Hernández Castellanos César Uriel , Martínez Islas Mauricio Joel , *Reyes Valenzuela Alejandro*

Directores: Rangel González Josué, Cervantes de Anda Ismael

email: areyesv11@gmail.com

Resumen: Desde los inicios de las tecnologías de la información se ha llegado a la conclusión de que ningún sistema es infalible, lo que ha provocado que el robo de datos sea uno de los delitos más frecuentes [5]. Al igual que con los sistemas en general, el sector médico ha sufrido un ascenso en el robo de información de la salud [9]. Ésta información no se limita a lo digital, sino también engloba a los archivos médicos físicos. Para auxiliar a cubrir ésta vulnerabilidad, se propone la creación de un prototipo de sistema híbrido (hardware y software) que cuente con un módulo de hardware dedicado a la ejecución de un algoritmo de cifrado, el cual se encuentre montado en un dispositivo programable (Nexys A7 Artix-7 FPGA), en colaboraciòn con un mòdulo de software que tiene como tarea el recopilar información médica sobre el paciente, para que finalmente se realice la escritura en un sistema portátil de almacenamiento y recuperaciòn de datos remoto pasivo (Higgs 3, 512 bits). Éste archivo médico será de utilidad en ocasiones donde se requiera identificar a un paciente o conocer detalles médicos sobre él.

Palabras clave: Robo de información, Información médica, Servicios De Salud, Confidencialidad, RFID, Dispositivo programable.

1. Introducción

El robo de información se ha encontrado presente a lo largo de la historia, sin embargo al surgimiento de las tecnologías de la información éste problema se ha agravado de manera significativa [1].

Desde los inicios de las tecnologías de la información, se ha llegado a la conclusión de que no existe un sistema que presuma de ser infalible. Por lo tanto, en un mundo en el que tantas organizaciones cuentan con acceso a una gran cantidad de información personal, el riesgo del robo de información se convierte en un factor a considerar, pues entre las posibles consecuencias se encuentran las siguientes: Persuasión comercial y política, fraude cibernético y robo de identidad, discriminación a partir de datos sensibles, entre otros.

En la actualidad, el uso de la informática, es algo que se encuentra alineado con la misma vida moderna, hoy toda actividad involucra aplicaciones informáticas para compartir datos, ya sea tanto de forma privada, como pública, por eso la importancia de proteger los activos de la información.

En México durante 2017, 92% de empresas reportaron incidentes informáticos, 27% de ellos fue debido a equipos robados con datos sensibles. Durante el mismo año, 85% de empresas fueron afectadas por fraude. El tipo más común fue robo de datos con un 38%, con los principales objetivos siendo datos de empleados y de clientes [7].

En los últimos años en México, el derecho a la privacidad o a la protección de datos personales se ha consolidado como un derecho fundamental y ha sido elevado a un rango institucional [4]

Dicho derecho se ha extendido al sector salud, donde en todo momento se maneja información personal catalogada como sensible. La transgresión de dicho derecho puede ocasionar diferentes consecuencias, especialmente en el mundo moderno en el que nos encontramos.

Un ejemplo de transgresión de dichos derechos se suscitó en 2010, cuando la aseguradora Dominion National reportó un robo de información médica durante nueve años en sus servidores, que potencialmente violó los datos de 2.96 millones de pacientes.

Una alerta interna avisó de diferentes accesos no autorizados a sus sistemas, lo que provocó una investigación por parte de las autoridades. Las cuales encontraron que el acceso no autorizado comenzó el 25 de agosto de 2010, casi nueve años de que se detectara la violación en abril de 2019 [5]

Un suceso similar sucedió en enero de 2019 cuando una base de datos mal configurada expuso información médica de 1.57 millones de pacientes de Inmediata Health Group.

La base de datos comprometida se descubrió, cuando personal de la organización descubrieron que un motor de búsqueda permitía indexar páginas web internas de la organización [5].

Finalmente en febrero de 2018, UW Medicine comenzó a notificar a 974,000 pacientes que sus datos se encontraron expuestos durante tres semanas debido a un servidor mal configurado. Ésta violación de datos se descubrió en diciembre de 2018, cuando un paciente realizó una búsqueda con su propio nombre y encontró un archivo que contenia su información médica. Éste es un ejemplo en donde un solo individuo ha sido afectado [5].

Trasladando éste impacto a nivel industria se observa que en el caso de Estados Unidos, el costo total promedio de la violación de datos en el sector salud durante 2018 fue de 6.45 mdd, lo cual es 65% más que el costo total promedio de una violación de datos. De aquí podemos extraer que la implementación de medidas de seguridad al momento de estar tratando con información médica es una prioridad dentro del ámbito. Por otro lado, el costo por violación de datos de un archivo médico fue de $429 [6].

Los afectados del sector salud por estos hechos reportaron dificultad para retener clientes después de haber reportado una violación de datos. 7% de clientes se mudan a otro competidor después de que se han violado sus datos. Esto posiciona a la industria de la salud como el sector más afectado por éste tipo de siniestros [7].

Las estadísticas anteriores nos muestran el impacto económico que provoca al sector salud el robo de información, sin embargo las consecuencias también pueden afectar de manera significativa a los clientes de las organizaciones afectadas.

La revelación de información médica a entidades no autorizadas puede acarrear diferentes consecuencias a nivel personal, como la empleabilidad de una persona al solicitar empleo, ya que se sabe que existen ciertos genes que predisponen al cáncer de mama o enfermedad de Alzheimer. Si esos datos se conocen o se exigen al solicitar un trabajo, dichas condiciones médica pueden resultar desfavorables algunos candidatos.

Un caso más sobre la importancia de la confidencialidad de los datos médicos se encuentra suscitando en Alemania, donde la canciller Angela Merkel ha sido señalada por diferentes medios de comunicación respecto a su estado de salud [8], lo que de resultar ser cierto y ser revelado a la opinión pública, podría derivar en consecuencias políticas, económicas y de gobernabilidad.

Los ejemplos anteriores retratan la importancia de la confidencialidad médica de las personas. Sin embargo, la revelación de información médica se da en casos excepcionales cuando entra en juego la vida [9]. Cuando se trata de un accidente es de vital importancia que los profesionales de la salud tengan acceso a la información médica del paciente, para que este pueda recibir una atención adecuada y no comprometa aún más su estado de salud.

Con la finalidad de auxiliar a pacientes de centros médicos, se propone desarrollar un prototipo de sistema híbrido médico, donde se podrá visualizar y realizar los registros médicos por medio de la identificación del paciente.

La gestión de los registros médicos será llevada en una aplicación de software. Para la identificación de los pacientes se empleará un tag de tecnología RFID (Higgs 3, 512 bits), el cual será de utilidad en ocasiones donde se requiera identificar a un paciente o conocer detalles médicos sobre él. Dicho tag será leído por un lector RFID, el cual se encontrará en comunicación con un dispositivo programable (Nexys A7 Artix-7 FPGA) que se encontrará dedicado a la ejecución de un algoritmo de cifrado.

Para esto se pretende que la persona interesada en obtener un dispositivo RFID, acuda a un centro médico en donde sea evaluado por un profesional de la salud que tiene la tarea de recopilar sus datos médicos. Ya recopilados, estos serán ingresados a un sistema de software, para su posterior cifrado, utilizando un módulo de hardware externo, encargado de implementar un algoritmo de cifrado. Éstos datos cifrados se escriben en el dispositivo RFID para que el paciente cuente con un archivo médico cifrado portátil que podrá ser visualizado en centros médicos.

Por último en el escenario que por alguna razón los datos médicos contenidos en el dispositivo RFID requieran ser sobreescritos, se requiere la asistencia del paciente a un centro médico con dicho dispositivo, junto con su llave privada para que una persona autorizada pueda modificar sus datos médicos.

2. Objetivo

Implementar un prototipo de sistema híbrido para la portabilidad y protección de datos médicos que permita a pacientes tener su información cifrada por hardware dentro de un dispositivo RFID.

Objetivos específicos:

- Implementar una interfaz que tenga acceso al servidor de sistema de datos médicos y al módulo de cifrado y descifrado.
- Implementar un servidor de base de datos en el cual se encontrará la información médica de los pacientes.
- Implementar un módulo de cifrado y descifrado en una FPGA Nexys A7 Artix-7, para el procesamiento de la información médica del paciente y posterior transmisión a un dispositivo RFID.
- Desarrollar el módulo de software que gestione los registros médicos de los pacientes y credenciales de profesionales de la salud.

3. Justificación

La industria de la salud tiene el costo más alto por violaciones de datos y es el sector más vulnerable ante clientes que deciden irse una vez enterados de tales ataques.vi

Mundialmente durante 2017, el 75% de organizaciones de cuidado de la salud, farmacología y biotecnología reportaron alguna especie de fraude. De ésta cifra, el 23% lidiaron con casos de robo de información [6]. El siguiente año (2018), por causas de robo de información, se dieron 47 incidentes reportados los cuales afectaron 771,656 archivos de pacientes. Por razones de pérdida de información, hubo un total de 11 incidentes reportado s que afectaron 23,559 archivos de pacientes. Ésto nos da un total de 795,215 archivos afectados durante 2018 debido a robo o extravío de datos[8].

Para HIPAA, en el caso de ePHI (*electronic Protected Health Information)* durante 2018, se reportaron 11 violaciones de datos en los cuales los datos no estaban cifrados [9]. Si la información hubiera estado cifrada, algún tipo de protección en contra de estos ataques estaría presente.

En el caso de información de la salud dentro de México, en 2018 sucedió que Bob Diachecko, un investigador en el área de seguridad descubrió una base de datos perteneciente a Hova Health conteniendo los datos personales y médicos de 2,373,764 pacientes. Esto nos permite ver que en México existen casos de robo de información médica y el evidente descuido que lo rodea [10].

Una posible medida ante el robo de información médica que depende del paciente es el cifrado de la misma, dado que en caso de robo, los datos recolectados serían ilegibles para agentes externos que deseen hacer uso de dicha información.

Ante esto, se propone la elaboración de un prototipo de sistema híbrido médico centrado en el cifrado y descifrado de datos médicos con el propósito de brindarles a los pacientes un archivo de médico portátil.

El enfoque principal del prototipo es la protección de datos cuando se tenga un archivo médico dentro de la tarjeta. Si la tarjeta se llega a perder o clonar, el atacante solo obtendrá información cifrada, no los datos médicos del paciente. El cifrado brinda una capa de protección en estos casos, a diferencia de un dispositivo con datos visibles.

Para el desarrollo de este proyecto se propone utilizar un lenguaje de descripción de hardware VHDL y su sintetización en un FPGA (Nexys A7 Artix-7) para la implementación de un algoritmo de cifrado, además de la habilitación de periféricos para su comunicación con el lector/escritor RFID (RC522) y con el módulo de software.

4. Productos o Resultados esperados

- Prototipo de cifrador/descifrador montado en una FPGA.
- Dispositivo RFID adaptada a necesidades del sistema para el almacenamiento de datos médicos cifrados
- Aplicación de software con conexión a base de datos para el almacenamiento y manejo de datos médicos de pacientes.
- Servidor de base de datos y de llaves públicas
- Manuales de usuario para cada uno de los módulos y documento técnico.

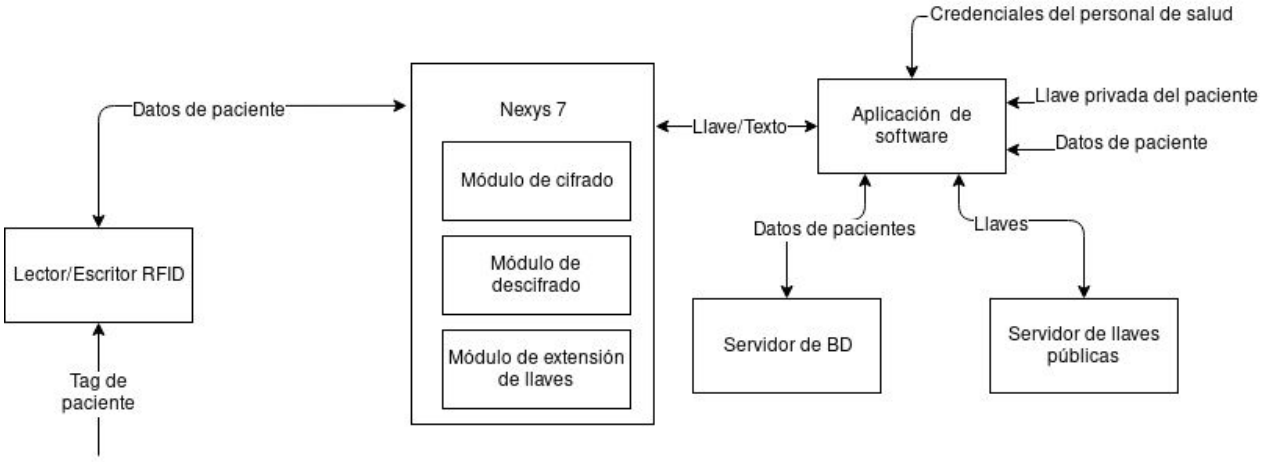

Fig. 1.0 Arquitectura del sistema

5. Metodología

Se utilizará el desarrollo iterativo e incremental para el desarrollo del trabajo terminal. La razón es que nos permite una gran flexibilidad durante el tiempo de desarrollo ya que nos brinda la posibilidad de evaluar los entregables que vayamos produciendo al final de cada iteración y decidir si se requiere cambiar drásticamente el producto de la iteración o si éste sirve como base para comenzar con la siguiente. Al ser un proyecto híbrido el que va a ser desarrollado, se adecuará la metodología para poder llevarla a cabo tanto para el hardware como para el software que se planea entregar..

Iteración 0 o Iteración Inicial

- Plática con directores
- Planeación inicial
- Delimitación de requerimientos de los módulos del sistema
- Planificación de actividades

1° Iteración (Desarrollo de terminal con conexión a sistema de datos médicos)

- Análisis
- Diseño
- Desarrollo y codificación del módulo de cifrado
- Pruebas
- Evaluación del entregable

2° Iteración (Desarrollo del módulo de cifrado de información)

- Análisis
- Diseño
- Desarrollo y codificación del módulo de cifrado
- Pruebas
- Evaluación del entregable

3° Iteración (Adaptación de dispositivo RFID)

- Análisis
- Diseño
- Adaptación de dispositivo RFID de acuerdo a las necesidades del sistema
- Pruebas
- Evaluación del entregable

4° Iteración (Establecimiento de conexión entre el módulo de cifrado y el módulo de almacenamiento)

- Desarrollo y establecimiento de comunicación entre módulos
- Pruebas
- Evaluación del entregable

5° Iteración (Desarrollo del módulo de descifrado de información)

- Análisis
- Diseño
- Desarrollo y codificación del módulo de descifrado
- Pruebas
- Evaluación del entregable

6° Iteración (Desarrollo de terminal con módulo de autenticación)

- Análisis
- Diseño

- Desarrollo y codificación de la terminal
- Pruebas
- Evaluación del entregable

7° Iteración (Integración de módulos).

- Desarrollo y establecimiento de comunicación entre todos los módulos desarrollados
- Pruebas finales con los tres módulos en conjunto
- Entrega final con manuales de usuario para cada módulo

7. Referencias

[1]"Robo de Identidad y Consecuencias Sociales | Documentos - CSI -", *Cert.org.mx*, 2019, Disponible: https://www.cert.org.mx/historico/documento/index.html-id=16.

[2] "Ley Federal de Protección de Datos Personales", *Es.wikipedia.org*, 2019, Disponible: https://es.wikipedia.org/wiki/Ley_Federal_de_Protecci%C3%B3n_de_Datos_Personales.

[3] "The 10 Biggest Healthcare Data Breaches of 2019, So Far", *HealthITSecurity*, 2019, Disponible: https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2019-so-far

[4] IBM Security, Cost of a Data Breach Report, pp.16, 26, 27,42,76, 2019

[5] Kroll, *Global Fraud & Risk Report*, p.66, 2018

[6] K. Bennhold, "La salud de Angela Merkel intensifica el debate sobre su sucesión", *Nytimes.com*, 2019. Disponible: https://www.nytimes.com/es/2019/07/04/merkel-temblores-salud-temblando/.

[7] *Código de ética para el ejercicio profesional del médico colegiado en México*, 2019, Disponible: http://www.comego.org.mx/reglamentos/codigo_etica.pdf.

[8] Protenus, 2019 Annual Breach Barometer Report, p.10-11, 2019

[9] HIPAA Journal, Healthcare Data Breach Statistics, Disponible: https://www.hipaajournal.com/healthcare-data-breach-statistics/

[10] HealthcareITNews, Telemedicine vendor breaches the data of 2.4 million patients in Mexico, Disponible: https://www.healthcareitnews.com/news/telemedicine-vendor-breaches-data-24-million-patients-mexico

8. Alumnos y Directores

César Uriel Hernández Castellanos.- Alumno
de la carrera de Ing. en Sistemas Computacionales en
ESCOM, Especialidad Sistemas, Boleta: 2016602860 , Tel.
5577497900 , email uuriel12009u@gmail.com
Firma:_____

Mauricio Joel Martínez Islas.- Alumno
de la carrera de Ing. en Sistemas Computacionales en
ESCOM, Especialidad Sistemas, Boleta: 2014090412 , Tel.
5586136841 , email maumartinez1297@gmail.com
Firma:_____

Alejandro Reyes Valenzuela.- Alumno
de la carrera de Ing. en Sistemas Computacionales en
ESCOM, Especialidad Sistemas, Boleta: 2014090587 , Tel.
5532819601 , email areyesv11@gmail.com
Firma:_____

Cervantes de Anda Ismael..- M. en C. en Ingeniería en Sistemas,
SEPI ESIME 2003, Ing. en Comunicaciones y Electrónica
en 1997, Profesor de ESCOM/IPN (Dpto C. I. C.) desde 1998,
Áreas de Interés: Control y Automatización, Microcontroladores, Instrumentación.
Ext. 52055, email icervantesd@ipn.mx**.**

Firma:_____

Josué Rangel González.- M. en C. en Ingeniería en Ciencias de la Computación,
CIC - IPN, Ing. en Computación
en 2007, Profesor de ESCOM/IPN (Dpto I. S. C.) desde 2009,
Áreas de Interés: Sistemas web, Cómputo paralelo y distribuido, Machine learning.
Ext. 52055, email josuergmx@gmail.com**.**

Firma:_____