EVALUACIÓN PARA PROPUESTAS DE TRABAJO TERMINAL

NO. DE REGISTRO DEL TT: 2020-A068

TÍTULO DEL TT: SISTEMA DE ALMACENAMIENTO EN LA NUBE UTILIZANDO RECONOCIMIENTO FACIAL PARA EL CIFRADO DE LA INFORMACIÓN

FECHA DE EVALUACIÓN: VIERNES 31 DE JULIO DE 2020

NO. DE VERSIÓN 1a. [X] 2a. [ ]

PREGUNTA	SI	NO	OBSERVACIONES
1. Título del TT. ¿El título corresponde al producto esperado?	X		
2. Resumen. ¿El resumen expresa claramente la propuesta del TT, su importancia y aplicación?		X	El resumen no aporta una noción breve de las particularidades del proyecto. Por favor, consúltese los comentarios detallados.
3. Palabras clave. ¿Las palabras clave han sido clasificadas adecuadamente?	X		Sugiero que se atiendan los comentarios ya que podrían mejorarse, pero lo dejo a criterio de los autores.
4. Introducción. ¿La presentación del problema a resolver es comprensible?		X	La introducción debe mejorarse sustancialmente. Considero que es un contenido muy pobre y cuestionable. Por favor, consúltese los comentarios detallados.
5. Objetivo. ¿El objetivo es preciso y relevante?		X	
6. Planteamiento. ¿El planteamiento del problema y la tentativa solución descrita son claros?		X	
7. Justificación. ¿Sus contribuciones o beneficios están completamente justificados? Originalidad, vinculación con población usuaria potencial, utilidad de los resultados, complejidad en su elaboración a nivel ingeniería, mejoramiento de lo existente, etc.		X	Considero que la justificación urge de solidez en su argumentación. Por favor, consúltese los comentarios detallados.
8. Resultados o productos esperados. ¿Su viabilidad es adecuada? Tiempos, recursos humanos y materiales, alcances, costos y otros puntos que puedan impedir la culminación exitosa del trabajo.		X	Debido a las deficiencias en las secciones anteriores del protocolo es intrascendente considerar los resultados.
9. Metodología. ¿La propuesta metodológica es pertinente?	X		
10. Cronograma. ¿El calendario de actividades por estudiante es adecuado?	X		

DICTAMEN

APROBADO	NO APROBADO
—	X

RECOMENDACIONES ADICIONALES:

El contenido del resumen tiene el propósito de permitir que un lector obtenga una noción del documento, en este caso, del proyecto propuesto mediante este protocolo. Así entonces, sugiero realizar algunos cambios y mejorar sustancialmente el texto del resumen. Les recomiendo tomar algunos artículos científicos del tema de su preferencia y leer sus respectivos resúmenes; con ellos, tratar de hacerse una idea del contenido del artículo. Posteriormente, leer y comprender los artículos. Con este ejercicio pueden adquirir una idea inicial del contenido que los autores de esos artículos eligieron para componer sus resúmenes; luego, identificar cuáles ideas sobraron y cuáles faltaron para dar información esencial del proyecto.

El primer enunciado del resumen, “Actualmente existen… y proteger la información.”, expresa una idea de los servicios en la nube, pero no propiamente da detalles del proyecto. Sugiero prescindir de estos enunciados y elegir aquellos que sí abonen a compartir al lector una noción del proyecto.

Respecto al tercer enunciado del resumen, si bien no sugiero su remoción, sí sugiero modificarlo para ser más informativo. Es obvio que al utilizar criptografía se busca “proteger información” frente a “amenazas”, de lo contrario, no se usaría criptografía; así tal cual es irrelevante. Podrían mencionar que “clase” de ataques se busca prevenir y cuáles partes de la criptografía requieren.

El segundo enunciado, “El presente trabajo… utilizando reconocimiento facial.”, es el que aporta la mayor información: “busca desarrollar un sistema de almacenamiento”, utilizará criptografía asimétrica y tomará como entrada datos de reconocimiento facial. Sin embargo, sugiero especificar a cuál tipo de almacenamiento se enfocará, qué clase de datos almacenará, y las particularidades que caracterizan su proyecto. Podrían considerar la existencia hipotética de otro proyecto similar al de ustedes y elegir esas particularidades que los diferencian del otro proyecto para identificar características a incluir en esta descripción.

En general, considero que el resumen es poco informativo y debe mejorarse sustancialmente.

Las palabras clave me dejan una impresión muy general. Les recomiendo consultar las revistas científicas especializadas en las áreas relacionadas con su proyecto para tener una idea de aquellas que podrían permitir identificar mejor su proyecto. Por ejemplo, dado que su proyecto involucra la criptografía, bien podrían tomar algunas revistas especializadas en criptografía, revisar sus listas de palabras clave y elegir aquellas que ajustan a lo que estará relacionado con su proyecto; de la misma manera con revistas sobre cómputo en la nube (*cloud computing*) y las demás áreas que intervienen en el proyecto.

El texto de la introducción consta de exactamente un párrafo y una tabla. Definitivamente, esta sección debe contener una introducción con más información. Invito a los autores a cuestionarse sensatamente la suficiencia del contenido de esta sección.

Sean cuidadosos con las deficiencias en el uso de signos de puntuación. Préstenles la atención necesaria, ya que no se esperan de un estudiante de nivel superior. Menciono un par de ejemplos. El primero se ubica en el primer enunciado de único párrafo de la Introducción. Falta una coma en "En los últimos años el almacenamiento", la frase "en los últimos años" tiene una función de aposición explicativa y va delimitada por una coma. El segundo es "De esta forma", ubicado en el último enunciado del resumen.

Sugiero se apoyen de un manual de estilo y, complementariamente, consulten las normas de los usos de los signos de puntuación. Adicionalmente, les recomiendo optar por construcciones de enunciados cortos o medianos, en lugar de largos. Esto les permite expresar ideas más claras y sintéticas que se complementan entre sí construyendo un párrafo.

Consideren modificar la Tabla 1 para que destaque las diferencias entre su proyecto y los trabajos existentes. Desafortunadamente, la plantilla del formato de protocolo tiene una tabla de ejemplo que poco ayuda destacar estas diferencias. Sin embargo, dado que no existe una prohibición explícita que les impida modificarla, sugiero adaptarla para que sea un instrumento más didáctico que exhiba estas diferencias.

La tabla actual considera dos aspectos a comparar: las características del software y su precio en el mercado. Considero que el precio en el mercado es un aspecto irrelevante para el contexto de este protocolo. Dado que su proyecto no tiene una intención de comercialización inmediata, entonces es irrelevante este dato.

El segundo aspecto, las características del software, sí son de interés, y precisamente por esto, deberían expresarse de forma más clara y no sólo narrativa. Por citar algunos posibles ejemplos, se podría resaltar el tipo de archivos compatibles en los sistemas, el tipo de cifrado, servicios de seguridad que consideran, la disponibilidad de archivos, etc.

En este mismo sentido sobre importancia de una comparación clara entre la propuesta y el estado del arte, tomo como ejemplo el primer proyecto presentado en la tabla es "AceroDocs". De sus características me surgen varias preguntas, entre ellas: ¿qué es un "sistema de protección documental" y cómo es comparable con un "sistema de almacenamiento en la nube"?, ¿qué significado relevante tiene que esté "dirigido a grandes empresas y pequeños negocios"?, ¿qué se debe entender por "protección remota de documento"?, ¿qué diferencia tiene un documento ordinario, por ejemplo, un DOC o un PDF, con un "documento especialmente sensible"?, ¿por qué se considera una "función innovadora" la protección remota para documento, existiendo muchas técnicas de cifrado de documentos que no se encuentran en la computadora local?

Revisé la referencia 1, dirige a una "nota periodística" [3] del Instituto Nacional de Ciberseguridad de España. El texto que se puso como características de AceroDocs es una copia truncada del sexto párrafo de esa nota. Les sugiero evitar este tipo prácticas cuestionables. Esta acción me lleva a dudar de la calidad de la investigación del estado del arte para este proyecto. Profundizando un poco más en esta referencia, se puede llegar a la página oficial de AceroDocs [4]. Ahí no se dan detalles sobre el tipo de cifrado que se utiliza, como tampoco da indicios para pensar que usan información de reconocimiento facial, por lo tanto, pongo en duda, cuán comparable es este proyecto con su propuesta y si acaso es válido como parte de estado del arte.

Considero que esta misma falta de información ocurre con los otros proyectos.

Los proyectos MEGA, Face ID Lock Screen, Vault, AppLock Face, Railer y Luxand Face Recognition no tienen una referencia para ser consultados, por lo tanto, no hay forma de verificar su validez como estado del arte. Si bien MEGA [5] es un proyecto popular y fácil de encontrar, procuren no omitir sus referencias. Encontré una aplicación con la palabra "Vault" [1] que se ajusta a la descripción de características pero sin la certeza de que esta sea a la que se refieren. El mismo caso con AppLock Face [2], Railer [6] y Luxand Face Recongnition [7].

Como ejemplo sobre formatos que puedan ayudar a comparar características en el estado del arte sugiero consultar la tabla que se presenta en la página de AceroDocs bajo el encabezado "*Elige el plan que más se ajuste a tí*". Como podrán ver aquí se comparan los planes del servicio y es posible ver con claridad que diferencias hay entre cada uno. Una idea similar les sugiero que tengan en mente cuando realicen esa comparación. El proyecto K-Rax 3D tiene una referencia equivocada: la de la nota del INCIBE. Por último, el proyecto que refieren como "Apps de entretenimientos" tiene una referencia al "Sistema Generador y Modelador de Retratos Hablados K-Rax 3D".

El objetivo general considero que sí es claro, pero mejorable. En cambio, los objetivos específicos lucen más como un listado de componentes del sistema que como una lista de objetivos. No se deben confundir los conceptos. En esta sección son objetivos y estos pueden tener una dimensión tecnológica, técnica, práctica, social, etc.

La justificación tiene una solidez argumental pobre y debe mejorarse. Carece también de la "motivación del proyecto" y del "planteamiento del problema"; dicho sea, dos conceptos que con frecuencia se confunden.

Esta sección expone texto poco informativo, incluso incurre en obviedades. El primer enunciado del primer párrafo de esta sección menciona "En la nube, cualquier vulnerabilidad en el software puede suponer un gran impacto para la información". ¿Qué se entiende por "vulnerabilidad"?, es obvio que riesgo en el

resguardo de información puede representar algún agravio a alguien, ¿por qué mencionar lo obvio?, ¿qué debemos entender por "impacto para la información"?, ¿acaso que "se corrompe la integridad de los datos"? El segundo enunciado menciona "Se han encontrado vulnerabilidades en muchos sistemas de almacenamiento… y que requieren mejoras en su estructura y nuevas implementaciones de seguridad". ¿Cuáles sistemas y que vulnerabilidades han reportado?, ¿acaso el reconocimiento facial atiende las vulnerabilidades a las que se refiere implícitamente el texto?. Del tercer enunciado, ¿Por qué sería "ideal" implementar el reconocimiento facial para el manejo seguro de la información?, ¿qué se entiende por "manejo seguro de la información"?

Más adelante se exponen "problemas a mitigar". ¿Acaso con el reconocimiento facial se evita la pérdida de datos debido al olvido de claves de cifrado?, ¿cómo se considera las fallas del reconocimiento facial, como los falsos positivos o falsos negativos?, si se conside que los cifradores son esencialmente deterministas ¿cómo garantizar que el reconocimiento facial tiene una salida constante, tal que sea una entrada válida para los cifradores?, ¿con que fundamento técnico se opta por elegir criptografía asimétrica para cifrar datos?

Las secciones revisadas hasta este punto deben mejorar. Se puede ver que la propuesta carece de información básica que dé suficiencia técnica a este proyecto. Sugiero al estudiante revisar con seriedad literatura básica sobre criptografía, a fin de evitar que este proyecto sea un ejercicio ocioso, como baticino basado en este protocolo. Me permito sugerir los libros "CryptoSchool" [8] e "Introduction to Applied Cryptography" [9], como dos referencias introductorias. Desconozco si el estudiante cursó alguna materia de criptografía, en caso de no haberlo hecho, le recomiendo enfáticamente tomar un curso, ya que le permitirá tener los conocimientos básicos para proponer un proyecto con viabilidad ingenieril en esta área.

Sin estas secciones bien planteadas, considero que es intrascendente considerar los resultados esperados.

Respecto a la metodología y al cronograma, no tengo comentarios o aportaciones que hacerles. Confío en el criterio de su director para organizar y dirigir el equipo de trabajo de la mejor forma que las circunstancias lo permitan.

Finalmente, termino con una crítica e invitación para reflexionar. En este protocolo no vi expresadas las contribuciones académicas, tecnológicas, pero sobre todo sociales. No las encontré ni en la introducción, ni en la justificación; quizá este último el lugar más adecuado para expresarlo. Esta institución es una de educación pública y en el artículo primero de su ley orgánica expresa motivaciones de independencia, en varias dimensiones; además es financiada por recursos públicos a través de impuestos. Por lo tanto, sugiero considerar las contribuciones que como estudiante se deja a la sociedad, que no forzosamente a la institución, con este proyecto.

Espero que estos comentarios, resulten una retroalimentación constructiva. Cualquier duda o comentario, por favor, no duden en contactarme y con todo gusto los atenderé.

[1]: https://play.google.com/store/apps/details?id=com.netqin.ps
[2]: https://play.google.com/store/apps/details?id=com.sensory.tsapplock
[3]: https://www.incibe.es/sala-prensa/notas-prensa/cinco-proyectos-lideres-ciberseguridad-apoyados-el-ministerio-energia
[4]: https://www.acerodocs.com/
[5]: https://mega.nz/
[6]: https://play.google.com/store/apps/details?id=com.railer.face
[7]: https://www.luxand.com/
[8]: https://link.springer.com/book/10.1007/978-3-662-48425-8
[9]: https://link.springer.com/book/10.1007/3-540-49244-5

NOMBRE Y FIRMA DEL SINODAL:	Israel Buitrón Dámaso
ACADEMIA:	Ciencias Básicas
DEPARTAMENTO:	Formación Básica
CONTACTO:	ibuitron@ipn.mx, www.comunidad.escom.ipn.mx/ibuitron/contacto.html

Nombre de archivo: 2020A068-protocolo-evaluacion-1.0.docx
Directorio: /Users/israel/Box Sync/Escom/Trabajos Terminales/2020-A068/protocolo/1.0
Plantilla: /Users/israel/Library/Group Containers/UBF8T346G9.Office/User Content.localized/Templates.localized/Normal.dotm
Título:
Asunto:
Autor: UTEyCV-E
Palabras clave:
Comentarios:
Fecha de creación: 05/08/20 4:40:00
Cambio número: 2
Guardado el: 05/08/20 4:40:00
Guardado por: Israel Buitrón Dámaso
Tiempo de edición: 0 minutos
Impreso el: 05/08/20 4:40:00
Última impresión completa
Número de páginas: 3
Número de palabras: 2,164
Número de caracteres: 13,324 (aprox.)