UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE GUAYAQUIL

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE:
INGENIERO DE SISTEMAS

CARRERA:
INGENIERÍA DE SISTEMAS

TEMA:
“MODELO DE SEGURIDAD INFORMÁTICA PARA RIESGOS DE ROBO DE INFORMACIÓN POR EL USO DE LAS REDES SOCIALES”

AUTOR:
Nelson Alexander Vera Navas

TUTOR:
Msg. Joe Llerena Izquierdo

Junio 2021
GUAYAQUIL-ECUADOR

DECLARATORIA DE RESPONSABILIDAD

Yo, **Nelson Alexander Vera Navas**, declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del/los autor/es.

Firma del autor
Nombre: Nelson Vera Navas
CI. 0931549489

Firma del Tutor
Nombre: Joe Llerena
CI. 0914884879

MODELO DE SEGURIDAD INFORMÁTICA PARA RIESGOS DE ROBO DE INFORMACIÓN POR EL USO DE LAS REDES SOCIALES

Nelson Vera-Navas [1[0000-0002-0505-2470]], Dario Huilcapi-Subia[1[0000-0003-4603-0566]] and Joe Llerena-Izquierdo[1[0000-0001-9907-7048]]

[1] Universidad Politécnica Salesiana, Guayaquil, Ecuador
nveran@est.ups.edu.ec, dhuilcapi@ups.edu.ec, jllerena@ups.edu.ec

Abstract. Las redes sociales, aportan a la disminución de la brecha tecnológica que se refleja en el estrechamiento de la relación entre personas, facilitando la interacción digital individual o grupal, mediante la destreza de los usuarios para coexistir unos con otros, compartiendo la proporcionalidad de la participación en ambientes tecnológicos, considerando también los nodos de que permite compartir los datos mediante instrumentos para la Análisis de Redes Sociales (ARS). El objetivo de esta investigación es de analizar el impacto de las vulnerabilidades de las redes sociales por medio de un modelo de seguridad informática para disminuir los riesgos de robo de información por el uso continuo. Se aplicará la metodología cuantitativa con un criterio deductivo y se realizará un análisis a la situación presentada por el incremento en el catálogo de aplicaciones en los sistemas operativos más comunes, así como los protocolos de intercambio de datos. Por otra parte, las aplicaciones de la Evaluación o Análisis de Redes Sociales (ARS,) permiten la anticipación para detectar ataques maliciosos a la seguridad y privacidad de los datos de los usuarios que usan las plataformas digitales sociales.

Keywords: Ciberseguridad, redes sociales, seguridad informática.

1 Introducción

Las redes sociales, presentan una constante en las medidas que se adoptan para disminuir la inseguridad de las personas, mostrando un aumento de su utilización y la exposición de los datos privados a un ambiente público digital. Las plataformas de las redes sociales están en búsqueda de ofrecer a sus usuarios por medio de la mejora continua en la experiencia durante el uso de sus productos y también procurar mantener la seguridad del sistema. En relación con la seguridad, un estudio presentado por la empresa tecnológica Shopos, evidencia la actividad realizada dentro de Facebook por parte de aquellos que la utilizan, facilita la vulneración de los datos y hurto de los datos privados. ESET, una empresa estadounidense procedió a capacitar a la ciudadanía sobre seguridad informática aplicando un modelo de ciudad segura. Por otra parte, Ecuador mediante el COIP (Código Orgánico Integral Penal), art. 178 al 234, sección tercera, se

castigan los crímenes informáticos, que vulneran los datos informáticos de índole personal y privada que perjudican la economía o su intimidad.

2 Materiales y métodos

Las redes sociales, han trascendido los niveles de aceptación, en la actualidad la necesidad de estar dentro del mundo digital es creciente e inconsciente para los usuarios, pero no para aquellos que desean sacarle provecho para adquirir ganancias. La red social se volvió el centro del marketing donde cualquiera puede ser un prospecto y futuro cliente, por otra parte, los riesgos de ser robados nuestros datos de manera sigilosa o involuntaria van creciendo y afectando a cada vez más usuarios.

Hay investigaciones sobre seguridad informática, las cuales refieren la importancia de garantizar el resguardo seguro y confiable de la información que se transmita por medio de alguna red social sin que esta se ponga en riesgo por la intrusión de terceras personas. Es así, que los dispositivos tecnológicos sean móviles o de escritorio con conexión a internet son mayormente expuestos [1].

En este tipo de contactos a más de seguridad se busca relaciones de negocios. Como medio de seguridad, las personas en redes sociales utilizan tarjetas de presentación para futuros encuentros reales [2][3], inclusive hay disponibilidad de reuniones online, por medio de redes sociales y que luego se vuelven reuniones cara a cara en el mundo físico. Se aplica la metodología de investigación con criterio deductivo de corte cuantitativo y se realiza un análisis documental mediante una revisión sistémica en una matriz de riesgos para contrastar la información en diferentes amenazas encontradas.

En trabajos previos, se evidencian varios tipos de amenazas presentadas en las redes sociales:

- Brechas de información: Las cuales corresponden a un hecho de alto riesgo donde se encuentra expuesto el nombre del usuario junto con algunos datos personales no solo física, sino que además digitalmente [4][5].
- Cibercrimen: Ataques cibernéticos que se llevan a cabo por medio de sitios web, obteniendo información privada para hacer mal uso de la misma [6][7][8].
- Hacktivismo: Este por lo general tiene fines políticos o sociales en los cuales se accede a la información privada con el objetivo de conocer la información interna que se desarrolla [9][10][11]. Al mismo tiempo de este elemento se derivan tres grupos fundamentales: a) Anonymous, b) Ciberocupas, c) Ciberguerreros.
- Ataques DoS: Todo tipo de amenaza que perjudica el acceso inmediato de la información [12][13].

Como un aspecto de relevancia, el software debe ser considerado, al momento de realizar análisis de las vulnerabilidades.

El acoso digital y los rumores han ido expandiéndose durante el ingreso a las redes e internet, así como surgen cambios en la manera de usarlas por parte de los usuarios de la social media, estos cambios, han ido incrementándose alrededor del mundo. Las

redes sociales (como Twitter, Facebook, Weibo) son herramientas eficientes para compartir información [14]. Los ataques, a través de las redes sociales, pueden utilizar la estrategia de desplazamiento de masas, así como la propagación de información para difundir información errónea entre los clientes [15]. Por lo tanto, es vital analizar y modelar la difusión del rumor y establecer medidas de seguridad [16]. Uno de los riesgos operativos para la empresa es el uso de cuentas de redes sociales durante el horario laboral por parte de sus empleados y por lo tanto están descuidando su trabajo, pero esta política no es efectiva hoy en día porque si los empleados quieren estar en redes sociales pueden iniciar sesión en sus cuentas a través de teléfonos inteligentes sin necesidad de computador. Además, los problemas de recolección de datos de comunicación, la privacidad y la seguridad también son desafíos que se determinan durante el análisis de la comunicación y la social media [17][18].

Al adentrarse el virus en los archivos, particularmente a aquellos que son ejecutables, este deja un código malintencionado de tal forma que dichos archivos al ser efectuados, se empieza a extender el virus, afectando a nuevos archivos. El cyber delito surgió como una nueva forma de delito y evolucionó en una industria seria, donde los atacantes especializados operan globalmente. La seguridad de cualquier sistema es una consecuencia directa de las decisiones de las partes interesadas con respecto a los requisitos de seguridad y su relativa priorización.

Las redes egocéntricas son utilizadas por grupos grandes, por medio de nodos centrales a los que también se los denomina egos, los cuales pueden ser usuarios, grupos como también organizaciones. Por otra parte, donde, la red del ego es una subgráfica centrada en un nodo (ego).

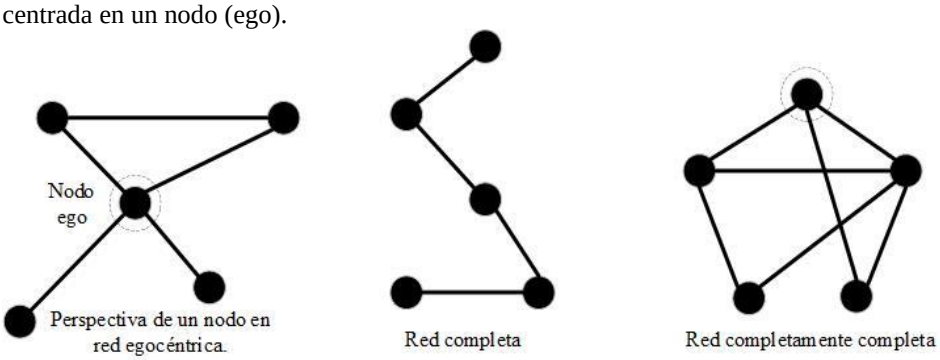

Fig. 1. Nodos en las redes sociales

En las redes sociales se evidencia un incremento de los vínculos débiles, que poseen los usuarios, lazos que se encuentran en una dinámica constante, pero con la posibilidad de comprometer cada vez más la información personal de cada participante. Esto produce un incremento de inseguridad y vulnerabilidad.

Existen riesgos de seguridad de la social media, entre ellos:

- Disminución del pensamiento crítico
- Incremento en el uso por parte de la aplicación sin petición del usuario
- Ocupación de gran potencia con consecuencias indeterminadas a corto plazo

- Condensan de manera general los vínculos de manera acelerada.
- Almacenan datos imprescindibles tanto explícita como no explicita
- Se presenta al usuario las opciones de forma tan llamativa, lo que compromete muchas veces la privacidad.

Las redes funcionan normalmente, las personas se comunican y se cumplen algunas metas. Estas posibilitan que la red se desarrolle, del mismo modo que impulsa la plataforma por medio de herramientas de comunicación. Cuando es utilizada la ingeniería social por los invasores, éstos adoptan un procedimiento para su ejecución y, en primer lugar, identifican a la víctima que tenga las características de interés como puede ser personal o por intereses financieros, para luego proceder a hacer mal uso de su información. Estos ataques se basan en la influencia manipuladora sobre las personas.
El uso de las redes sociales conforma gran parte de las actividades diarias; utilizadas no solo mediante una computadora o portátil, sino además de otros dispositivos tecnológicos. los delincuentes a menudo toman medidas para ocultar sus identidades, ya sea mediante un patrón complejo de ofuscación o, como en los delitos de identidad, utilizando la identidad de otra persona para cometer fraude.
Cada individuo tiene interacciones que se observan en las redes sociales, esto produce un producto que será llamado gráfica de interacción social. La gráfica tiene como eje central el kernel del sistema utilizado por usuario. La capacidad de controlar los intrusos se ven disminuidas por la intromisión en los procesos a los cuales se les autoriza manipular, estos datos pueden ser una un conjunto de datos organizados en una Data Base. Las redes sociales esperan honestidad, pero no todas las personas son honestas.
La información encontrada y comparada en la matriz, orientada a sistematizar los datos, analizando la documentación y mapearla por etapas que responden 1) Preguntas de Investigación, 2) Medio en que se Desenvuelve, 3) Satisfacer el Proceso de Búsqueda. 4) Encontrar los datos relevantes, 5) Filtrado Investigativo, 6) Gráfica de Datos, 7) Plan de Estudio Investigativo, 8) Elección de Información.

Table 1. Datos y Preguntas Para Investigación Sistémica

Interrogativas	Razón
Question 1 - Q1. ¿Qué tipo de datos documentales satisfacen el proceso de búsqueda investigativa?	Contrastar el conjunto de datos publicados en revistas indexadas que permitan mostrar datos relevantes.
Question 2 - Q2. ¿Es posible que la documentación facilite información referente a la autoridad de la Social Media en la inseguridad de las personas que las usan?	Establecer la influencia de la autoridad de la Social Media en la inseguridad de las personas que las usan.
Question 3 - Q3. ¿Aporta a la investiga-	Analizar la documentación para sostener

ción la información encontrada en las publicaciones de investigación para elaborar una matriz sistémica?	una matriz sistémica de la temática estudiada.

La tabla 1, muestra cómo las preguntas con las que se interactúa, la actividad de investigación gira entorno de las respuestas de los cuestionamientos presentados en el estudio, la sistematización con la información convirtiendo la información encontrada en un medio para la toma de decisiones. Así también, son también parte importante en el aporte para entender los procesos que influyen en la vulnerabilidad de las redes sociales.

Por otra parte, cada red social, tiene el compromiso de mejorar las seguridades de sus redes sin interferir en las decisiones de cada usuario. Cada pregunta de investigación tiene una respuesta mostrada en la tabla 2, los datos son correspondientes según las posibles alternativas propuestas.

Table 2. Respuestas a preguntas de investigación

Interrogativas	**Razón**
Question 1 - Q1. ¿Qué tipo de datos documentales satisfacen el proceso de búsqueda investigativa?	a. Herramientas sociales media b. Diagnóstico de vulnerabilidad c. Protección de datos privados d. Innovación tecnológica
Question 2 - Q2. ¿Es posible que la documentación facilite información referente a la autoridad de la Social Media en la inseguridad de las personas que las usan?	a. Credibilidad en la red social b. Distorsión de los perfiles c. Zonificación de los tics d. Tiempo de respuestas de los nodos
Question 3 - Q3. ¿Aporta a la investigación la información encontrada en las publicaciones de investigación para elaborar una matriz sistémica?	a. Revisión periódica de seguridades b. Actualización de políticas de seguridad c. Fortalecimiento de seguridades digitales d. Consulta de estudio indexado

Por otra parte, la figura 2 muestra, un número de 42 revistas consultadas de las cuales 16 se utilizaron para fundamentar la Matriz de Riesgos referente al tema de la seguridad informática y el robo de información en las redes sociales.

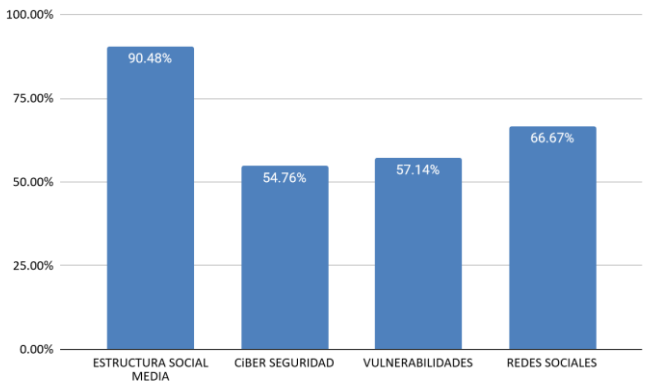

Fig. 2. Matriz Sistémica de Temáticas de investigación

De los cuatro temas atendidos, se obtienen 90,48% de las referencias aportan a la temática de Estructura social, 54,76% a Ciberseguridad, 57,14% a las vulnerabilidades, 66,67% a las redes sociales, lo que implica una relevancia y un alto grado de pertinencia de los documentos expuestos en la investigación.

Table 3. Matriz Sistémica de Riesgos

MATRIZ DE RIESGOS						
	Categoría	**Subcategoría**	**Área temática sobre riesgo en o por**	**ID**	**% Riesgo**	**Artículos**
1	Organizacional	Recursos	Estructura social media	R1	90.48%	38
2		Financiación	Ciber seguridad	R2	54.76%	23
3		Priorización	Vulnerabilidades	R3	57.14%	24
4			Redes sociales	R4	66.67%	28
5	Técnico	Requisitos	Herramientas sociales media	R5	71.43%	30
6		Tecnología	Diagnóstico de vulnerabilidad	R6	59.52%	25
7		Complejidad	Protección de datos privados	R7	57.14%	24
8		Fiabilidad	Innovación tecnológica	R8	69.05%	29
9	Externo	Mercado	Credibilidad en la red social	R9	73.81%	31

10		Condiciones de seguridad	Distorsión de los perfiles	R10	54.76%	23
11		Cliente	Zonificación de los tics	R11	64.29%	27
12		Proveedores	Tiempo de respuestas de los nodos	R12	78.57%	33
13	Interno	Estimación	Revisión periódica de seguridades	R13	50.00%	21
14		Planificación	Actualización de políticas de seguridad	R14	47.62%	20
15		Control	Fortalecimiento de seguridades digitales	R15	54.76%	23
16		Comunicación	Consulta de estudio indexado	R16	73.81%	31
			Número de artículos			**42**

La tabla 3, muestra como de los 42 artículos usados para la investigación, un número importante de artículos, de manera sistemática se relacionan, teniendo enfoques sobre temáticas específicas, las cuales sirven para describir el control y responsabilidad dentro de las redes sociales, así como el riesgo porcentual que se ha mencionado en cada temática mencionada en la sistematización de la matriz. Al describir el criterio de exclusión se discrimina la información relacionada al riesgo y el conjunto de los datos encontrados en la sistematización, discriminando los datos que orienten al buen uso de los recursos y herramientas informáticas que beneficien a la disminución de las vulnerabilidades y que mediante los documentos aportan a conocer acerca del robo de información en las redes sociales, Las preguntas de investigación son parte de este proceso como se muestra en la pregunta Q2. ¿Es posible que la documentación facilite información acerca del poder que tiene la Social media en la inseguridad de las personas que las usen?

3 Resultados y discusión

Las redes sociales han logrado introducir el interés por las conexiones entre usuarios, pero también se muestran las nocivas formas en que se pueden presentar un rompimiento de la reserva en la información privada. la información contenida dentro de bóvedas virtuales, convierten los datos en tesoros cada vez más atractivos que si son mal utilizados pueden perjudicar la vida e identidad digital de quienes son víctimas, para lo cual se emplean diferentes maneras de protegerse.

Al respecto de las preguntas de investigación, Question 1 - Q1. ¿Qué tipo de datos documentales satisfacen el proceso de búsqueda investigativa? Las bibliografías consultadas, aportan al buen uso de los recursos tecnológicos, con supervisión cuidadosa de lo que se comparte. Question 2 - Q2. ¿Es posible que la documentación facilite información referente a la autoridad de la Social Media en la inseguridad de las personas que las usan? Detrás de cada usuario hay un mundo y hay la intencionalidad de influenciar para acercar a los usuarios a llevar a cabo acciones no percibidas por el usuario, pero que persiguen la intencionalidad de quien influyo. Question 3 - Q3. ¿Aporta a la investigación la información encontrada en las publicaciones de investigación para elaborar una matriz sistémica? La matriz sistémica permitió encontrar de manera documental, las consecuencias de la Social Media durante el proceso de acciones de los usuarios cuando no se tienen los cuidados respectivos.

En las preguntas de investigación, se logró mostrar cómo los diferentes documentos atienden áreas técnicas, organizaciones, externas e internas, en la relación al tratamiento de las vulnerabilidades, estos puntos son mostrados en la figura 3 de porcentajes sistémico de la Matriz de Riesgos.

Las plataformas usadas en las redes sociales son mostradas como un medio de exposición vulnerable, los usuarios corren constantemente el riesgo de robo de información, siempre y cuando esta sea introducida dentro de las bases de datos de los sitios donde se alojan las redes sociales. Confiar en que las imágenes, videos, datos personales sensibles como cuentas bancarias o tarjetas de débito, son solo una parte de los datos que son constantemente buscados para ser usados ilegalmente.

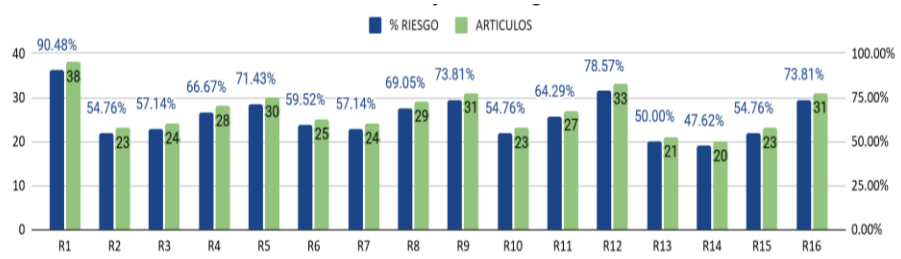

Fig. 3. Porcentaje Sistémico de la Matriz de riesgos

Según la figura 3, el porcentaje de riesgo ubica los Id con un número de incidencia que se calcula de acuerdo con el número total de los 16 riesgo que se muestran de acuerdo a los códigos del R1 al R16 y que corresponde a los 42 documentos analizado, al fin de prevenir, controlar, evitar, retener, transferir el riesgo. Al describir las acciones de las áreas vulnerables que podrían identificar a los responsables. la disminución del impacto de las vulnerabilidades va de la mano con los datos de riesgo.

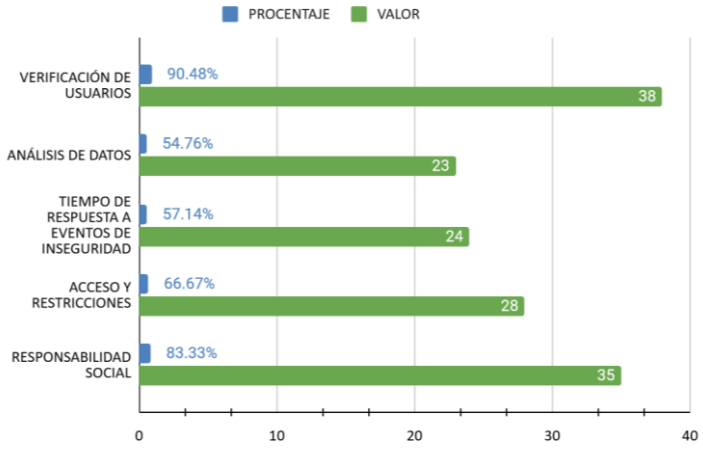

Fig. 4. Solución

La figura 4, muestra como la verificación de usuarios es parte importante en la disminución de las incidencias de robo de información, es necesario, que los datos ingresados sean analizados, así como el tiempo de respuesta de cada evento de inseguridad. Por otra parte, el acceso y restricción de al momento de ingresar a servicios y configuraciones es necesario protegerlo por medio de verificación de identidad. Todos estos procedimientos deben ser dirigidos por medio de un trato con responsabilidad social, cuidando de los usuarios que la usan.

4 Conclusiones

Los datos recopilados en las diferentes fuentes permiten concluir que son constantes los ataques dentro de las redes sociales, los usuarios son víctimas por el uso sin autocontrol de las redes sociales, así como el ingreso de información privada no precautelando las posibilidades de pérdida o robo de datos, los robos pueden darse por parte de delincuentes virtuales.

Las redes sociales, se introdujo con el surgimiento de la tecnología y los dispositivos móviles, tuvo un impulso, es necesario manejar los accesos, tanto para que las imágenes, videos o datos sean cuidados, el descontrol de la información facilita el mal uso de las herramientas virtuales; Es necesario, contar con políticas o buenas prácticas para disminuir dichas incidencias.

5 Referencias

1. Gencoglu, O.: Cyberbullying Detection with Fairness Constraints. IEEE Internet Comput. (2020). https://doi.org/10.1109/MIC.2020.3032461.
2. Nkuna, G., Coetzee, M.: Social Event Invitation and Recommendation for Event based Social Networks. In: 2020 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems, icABCD 2020 - Proceedings. Institute of Electrical and Electronics Engineers Inc. (2020). https://doi.org/10.1109/icABCD49160.2020.9183860.
3. Hou, Q., Han, M., Cai, Z.: Survey on data analysis in social media: A practical application aspect, (2020). https://doi.org/10.26599/BDMA.2020.9020006.
4. Putra, A.P.G., Humani, F., Zakiy, F.W., Shihab, M.R., Ranti, B.: Maturity Assessment of Cyber Security in The Workforce Management Domain: A Case Study in Bank Indonesia. Presented at the November 25 (2020). https://doi.org/10.1109/icitsi50517.2020.9264982.
5. White, G.R.T., Allen, R.A., Samuel, A., Abdullah, A., Thomas, R.J.: Antecedents of Cybersecurity Implementation: A Study of the Cyber-Preparedness of U.K. Social Enterprises. IEEE Trans. Eng. Manag. 1–12 (2020). https://doi.org/10.1109/tem.2020.2994981.
6. Al-Khater, W.A., Al-Maadeed, S., Ahmed, A.A., Sadiq, A.S., Khan, M.K.: Comprehensive review of cybercrime detection techniques. IEEE Access. 8, 137293–137311 (2020). https://doi.org/10.1109/ACCESS.2020.3011259.
7. Batra, S., Gupta, M., Singh, J., Srivastava, D., Aggarwal, I.: An Empirical Study of Cybercrime and Its Preventions. Presented at the January 15 (2021). https://doi.org/10.1109/pdgc50313.2020.9315785.
8. Chitrey, A., Singh, D., Singh, V.: A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model. Int. J. Inf. Netw. Secur. 1, (2012). https://doi.org/10.11591/ijins.v1i2.426.
9. Allodi, L., Hutchings, A., Massacci, F., Pastrana, S., Vasek, M.: WACCO 2020: The 2nd Workshop on Attackers and Cybercrime Operations Co-held with IEEE European Symposium on Security and Privacy 2020, (2020). https://doi.org/10.1109/EuroSPW51379.2020.00063.
10. Maisikeli, S.: UAE cybersecurity perception and risk assessments compared to other developed nations. In: Proceedings - 3rd International Conference on Information and Computer Technologies, ICICT 2020. pp. 432–439. Institute of Electrical and Electronics Engineers Inc. (2020). https://doi.org/10.1109/ICICT50521.2020.00075.
11. Wiafe, I., Koranteng, F.N., Obeng, E.N., Assyne, N., Wiafe, A., Gulliver, S.R.: Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. IEEE Access. 8, 146598–146612 (2020). https://doi.org/10.1109/ACCESS.2020.3013145.
12. Mazepa, S., Dostalek, L., Sharmar, O., Banakh, S.: Cybercrime and Vulnerability of Ukrainian Critical Information Infrastructure. In: 2020 10th International Conference on Advanced Computer Information Technologies, ACIT 2020 - Proceedings. pp. 783–786. Institute of Electrical and Electronics Engineers Inc. (2020). https://doi.org/10.1109/ACIT49673.2020.9208965.
13. Kao, D.Y., Chen, Y.Y., Tsai, F.: Hacking Tool Identification in Penetration

Testing. In: International Conference on Advanced Communication Technology, ICACT. pp. 256–261. Institute of Electrical and Electronics Engineers Inc. (2020). https://doi.org/10.23919/ICACT48636.2020.9061401.
14. Liu, Y., Yang, R.: Rumor detection of sina weibo based on MCF algorithm. In: Proceedings - 2020 International Conference on Computing and Data Science, CDS 2020. pp. 411–414. Institute of Electrical and Electronics Engineers Inc. (2020). https://doi.org/10.1109/CDS49703.2020.00086.
15. Alorini, D.S., Rawat, D.B., Alorini, G.S.: On the Influence Blocking Maximization for Minimizing the Spreading of Fake information in Social Media. In: Proceedings of the 2020 Spring Simulation Conference, SpringSim 2020. Institute of Electrical and Electronics Engineers Inc. (2020). https://doi.org/10.22360/SpringSim.2020.CSE.005.
16. Muhlmeyer, M., Agarwal, S., Huang, J.: Modeling Social Contagion and Information Diffusion in Complex Socio-Technical Systems. IEEE Syst. J. 14, 5187–5198 (2020). https://doi.org/10.1109/JSYST.2020.2993542.
17. Gao, H., Gao, T.: Prevention of Rumor Spreading Based on Blockchain. Presented at the December 24 (2020). https://doi.org/10.1109/icct50939.2020.9295764.
18. Llerena-Izquierdo, J., Viera-Sanchez, N., Rodriguez-Moreira, B.: Portable Device and Mobile Application for the Detection of Ultraviolet Radiation in Real Time with a Low Cost Sensor in Arduino. In: Communications in Computer and Information Science. pp. 301–312. Springer (2020). https://doi.org/10.1007/978-3-030-42517-3_23.