Clasificador de intrusiones para riesgos de seguridad de aplicaciones

Avance de proyecto de grado

Línea de investigación del grupo FICB-PG:

Grupo de Investigación FICB-PG

Línea de investigación del grupo FICB-PG: SEGURIDAD DE LA INFORMACIÓN

Grupo de Investigación FICB-PG

Víctor Julio Macías (1510020515)

Asesor temático:

Supervisor metodológico: **M.S.c Luis Gabriel Moreno Sandoval**

Junio 2017

Resumen

El aumento del uso de los servicios de la computación moderna presentan oportunidades para la explotación criminal y retos en términos de la seguridad de la información; ofrecer servicios en línea por medio de aplicaciones web acarrea consigo también riesgos de seguridad, así como amenazas y favorecimiento de para ataques. Ninguna de las tecnologías orientadas a la seguridad de la información garantiza una seguridad total, por consiguiente la seguridad tiene un enfoque de prevención y es aquí cuando se puede hacer uso de herramientas complementarias que apoyen las ya existentes, adoptando diferentes enfoques. Este trabajo se basa en recolectar a partir del ejecución de test de penetración que consistirá en la detección y verificación de vulnerabilidades e intento de explotación de estas para alimentar una base de intrusiones conocidas, que permitirá entrenar un clasificador de intrusiones que luego para será capaz de detectar y clasificar malversaciones sobre aplicaciones web, basado algoritmos que son capaces de hacer predicciones, tomar decisiones sin que haya existido una programación

previa y con datos que el sistema no ha visto nunca. El proyecto establecerá una herramienta de análisis de apoyo a las auditorías en busca de garantizar la protección de la información, aplicando algoritmos de reconocimiento de patrones con las técnicas de aprendizaje supervisado, generando informes con el análisis.

Palabras clave: Seguridad Información, Clasificadores, Detección de intrusiones.

Abstract

Increased use of modern computing services presents opportunities for criminal exploitation and challenges in terms of information security; offering online services through web applications also entails security risks, as well as threats and favoring of attacks. None of the information security oriented technologies guarantees total security, so security has a preventive approach and it is here that complementary tools can be used to support existing ones, adopting different approaches. This work is based on the collection of the penetration test, which will consist of detecting and verifying vulnerabilities and attempting to exploit these to feed a base of known intrusions, which will allow training of an intrusion classifier that will then be able to Detect and classify malpractices on web applications, based algorithms that are capable of making predictions, making decisions without prior programming and with data that the system has never seen. The project will establish an analysis tool to support the audits in order to guarantee the protection of the information, applying algorithms of pattern recognition with supervised learning techniques, generating reports with the analysis.

Key words: Security Information, Classifiers, Intrusion Detection.

_____

INTRODUCCIÓN

Los ataques a los sistemas siguen incrementándose día a día, el mayor conocimiento tanto de las herramientas computacionales, como de las debilidades de las mismas. La confidencialidad y la seguridad de los datos comerciales y personales así como las aplicaciones de misión crítica son parte de lo que las organizaciones no pueden permitir que estén el peligro de un fallo de seguridad. Las entidades deben tener de aplicaciones que cumplan con aspectos de seguridad, privacidad, acceso a la información de manera autorizada, en otras palabras que mitigan los riesgos asociados al manejo de la información. El objetivo de todo sistema de seguridad informática es proteger el principal valor de las organizaciones: datos e información. Cada organización tiene diferente políticas de seguridad y requerimientos dependiendo de su misión. Por ejemplo el caso de un banco, un proveedor de servicios en Internet, una universidad o una firma de consultoría. Sin embargo, todas tienen como objetivo común, de una u otra forma, mantener la confidencialidad, integridad y disponibilidad de los datos. Los sistemas de seguridad informática como firewalls, sistemas de detección de intrusos, anti-virus, y estándares para configurar sistemas operacionales y redes entre otros, conforman un sistema de apoyo que busca garantizar la protección de la información.

Justificación

Aprobar que datos confidenciales queden en manos de extraños tiene graves derivaciones para un negocio. Ya sea que esto suceda por accidente o con una intención maliciosa, una infracción de datos puede significar multas costosas por las violaciones al cumplimiento, pérdida de confianza de los clientes y una mancha en la reputación de la marca.

La necesidad de detección de intrusiones viene de la suposición de que, a pesar de la definición de políticas integrales de seguridad, y el despliegue de las medidas de seguridad apropiadas, un malintencionado todavía pueden realizar ataques y eventualmente podría tener éxito.

Toda organización basa el negocio en los datos e información. La protección de la información en las organizaciones es entonces prioritaria: mecanismos de seguridad como sistemas de detección de intrusos son una necesidad. Sin embargo, se debe tener en cuenta que la seguridad informática es sistémica y proveer de sistemas de seguridad en las organizaciones que ayuden a detectar y prevenir cualquier amenaza que pueda aprovechar una vulnerabilidad afectando la seguridad de la información y salvaguardando sus activos más valiosos, puede ser una gran inversión que no muchas empresas están dispuestas a asumir. Contar con un sistema complementario a los mecanismos de seguridad más comunes (antispam, antivirus, firewall) en organizaciones que no cuenten con los recursos suficientes para invertir en grandes plataformas de seguridad, nos brinda la necesidad de tener una visión clara sobre la efectividad de los algoritmos de reconocimiento de patrones, así como sus métodos de trabajo para la implementación en un prototipo de sistema que adopte mecanismo de defensa buscando que puedan denotar un intento de intrusión o mala utilización. Comparar sus resultados con las herramientas especializadas y obtener un porcentaje aceptable de efectividad respecto a estas herramientas, podría brindar una solución efectiva.

La protección de la información en las organizaciones es prioritaria ,ya que es un activo importante que posee valor y requiere en consecuencia una atención especial para garantizar la disponibilidad, confidencialidad e integridad de la misma. Un mecanismo de seguridad como sistemas de detección de intrusos es una necesidad, pero no todas las organizaciones están dispuestas a invertir en costosas soluciones, por lo que es necesario buscar alternativas novedosas de baja inversión que proporcionen resultados aceptables.

Pregunta de investigación

¿Cómo se relacionan las técnicas de reconocimiento de patrones con el análisis de intrusiones?

Objetivos

Objetivo general

Diseñar un clasificador de intrusiones para riesgos de seguridad de aplicaciones basado en técnicas reconocimiento de patrones

Objetivos Específicos

- Diseñar la estrategia para la adquisición de los datos que son la base en el análisis de intrusiones.
- Establecer la selección y extracción de características para el análisis de intrusiones basándose en las mejores prácticas.
- Definir la arquitectura del sistema prototipo basado en las características seleccionadas.
- Seleccionar y aplicar algoritmos de reconocimiento de patrones que se alineen con las características y arquitectura establecidas.
- Validar el prototipo de sistema de evaluando su desempeño y resultados frente a alguna herramienta de análisis de intrusiones.

Alcance

Esta investigación para profundizar en seguridad de la información está dada por proponer un clasificador de intrusiones para riesgos de seguridad de aplicaciones web basado en técnicas reconocimiento de patrones como apoyo para asegurar los servicios que estas ofrecen. Y se toman como referencia el top 10 de owasp(Williams, 2017) versiones 2013 y 2017 para la generación de intrusiones de cada tipo.

REVISIÓN DE LITERATURA

La información que ha llegado a ser considerada como el activo más valioso dentro de las empresas ya que juega un papel muy importante a la hora de la toma de decisiones ,útil para definición de nuevas estrategias de negocios, genera confianza

a clientes, organización competitiva , posicionamiento, respeto y buen nombre. Vital para cualquier organización. El aseguramiento de este activo se hace relevante. La necesidad de detección de intrusiones viene de la suposición de que, a pesar de la definición de políticas integrales de seguridad, y el despliegue de las medidas de seguridad apropiadas, un malintencionado todavía pueden realizar ataques y eventualmente podría tener éxito. Por lo que se hace necesario establecer una diversidad de barreras de seguridad, ya que una falla podría causar pérdidas incalculables que normalmente son el resultado de la ausencia o incumplimiento de las defensas o violación de las restricciones de seguridad. La seguridad de la información evolucionada considerablemente a partir de la segunda guerra mundial. Este campo ofrece muchas áreas de especialización, incluidos la auditoria de sistemas de información, seguridad operativa, detección de intrusos, computación forense, entre otros.

Los criterios de inclusión / exclusión de artículos

1-el articulo trata temas de Information security ,Cyber security,Security Information, Intrusion Detection.

2-el artículo cumple criterio 1. y tiene relación con Classifiers, Support Vector Machine, K-NN ,Data mining ,artificial neuro fuzzy inference,Machine Learning,Naive Bayes.

Lista de artículos seleccionados ,se utilizó scopus
Anomaly-Based Intrusion Detection using Fuzzy Rough Clustering(Chimphlee, Abdullah, Sap, Srinoy, & Chimphlee, 2006)
Collaborative SVM classification in scale-free peer-to-peer networks(Khan, Schmidt-Thieme, & Nanopoulos, 2017)
Fuzziness based semi-supervised learning approach for intrusion detection system(Ashfaq, Wang, Huang, Abbas, & He, 2017)
Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system(Al-Yaseen, Othman, & Nazri, 2017)
Towards an Energy-Efficient Anomaly-Based Intrusion Detection Engine for Embedded Systems(Viegas et al., 2017)
A hybrid PSO-SVM model for network intrusion detection.(Bi, 2016)
A novel SVM-kNN-PSO ensemble method for intrusion detection system(Aburomman & Ibne Reaz, 2016)

A syllabus on data mining and machine learning with applications to cybersecurity(Epishkina & Zapechnikov, 2016)
Anomaly Detection System in Cloud Environment Using Fuzzy Clustering Based ANN(Pandeeswari & Kumar, 2016)
Automated Big Text Security Classification(Alzhrani, Rudd, Boult, & Chow, 2016)
Behavior grouping of Android malware family(Hsiao, Sun, & Chen, 2016)
Behavioral malware detection approaches for Android(Amin, Zaman, Hossain, & Atiquzzaman, 2016)
Detecting and classifying method based on similarity matching of Android malware behavior with profile(Jang, Yun, Mohaisen, Woo, & Kim, 2016)
Detection and prevention system against cyber attacks and botnet malware for information systems and Internet of Things(Indre & Lemnaru, 2016)
DroidScreening: a practical framework for real-world Android malware analysis(Yu, Huang, & Yian, 2016)
Improving Anomalous Rare Attack Detection Rate for Intrusion Detection System Using Support Vector Machine and Genetic Programming(Pozi, Sulaiman, Mustapha, & Perumal, 2016)
Machine learning classifiers for android malware analysis(Lopez & Cadavid, 2016)
Machine learning-based mobile threat monitoring and detection(Hatcher, Maloney, & Yu, 2016)
OCPAD: One class Naive Bayes classifier for payload based anomaly detection(Swarnkar & Hubballi, 2016)
A new approach to intrusion detection in databases by using artificial neuro fuzzy inference system(Brahma & Panigrahi, 2015)
A novel SVM by combining kernel principal component analysis and improved chaotic particle swarm optimization for intrusion detection(Kuang, Zhang, Jin, & Xu, 2015)
Analysis of Intelligent Classifiers and Enhancing the Detection Accuracy for Intrusion Detection System(Albayati & Issac, 2015)
Business Resilient Vulnerability Analysis for Dynamic High Security Environment(Zaerens, 2015)
Co-FQL: Anomaly detection using cooperative fuzzy Q-learning in network(Shamshirband et al., 2015)
Constructing important features from massive network traffic for lightweight intrusion detection(W. Wang, He, Liu, & Gombault, 2015)
Design and Analysis of Multimodel-Based Anomaly Intrusion Detection Systems in Industrial Process Automation(Zhou et al., 2015)
Secure software engineering requirements in cloud environment by using anticipating learning classifier system Wafa ' Slaibi Alsharafat(Transactions, 2015)
Two-tier network anomaly detection model: a machine learning approach(Pajouh, Dastghaibyfard, & Hashemi, 2015)
Fuzzy modeling for information security management issues in cloud computing(Lin, Lin, Chou, & Lee, 2014)
Multi-App Security Analysis with FUSE(Ravitch et al., 2014)
A hybrid network intrusion detection framework based on random forests and weighted k-means(Elbasiony, Sallam, Eltobely, & Fahmy, 2013)

Classification of Malignant Melanoma and Benign Nevi from Skin Lesions Based on Support Vector Machine(Mahmoud, Al-Jumaily, Maali, & Anam, 2013)
A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering(G. Wang, Hao, Ma, & Huang, 2010)
Anomaly-Based Intrusion Detection using Fuzzy Rough Clustering(Chimphlee et al., 2006)

El origen de los datos en el 45 % de los artículos proviene de una KDD-99

Que es un conjunto estándar de datos a ser auditados, que incluye una amplia variedad de intrusiones simuladas en un entorno de red militar.

Los otros artículos se basan en orígenes de datos en capturas de paquetes durante periodos de tiempo cortos, con más de 500 ordenadores y otros con muestras de intrusiones de dominio público.

TOP Clasificadores	
SVM	8
Naiye Bayes	7
Logia Difusa	6
Arboles decisión	4
Red Neuronal	4
KNN	4
Clustering	2
Mixto	2

Las tecnologías utilizadas en la implementación de los algoritmos están en Matlab y Python, pero la gran mayoría delos artículos seleccionados omiten están información.

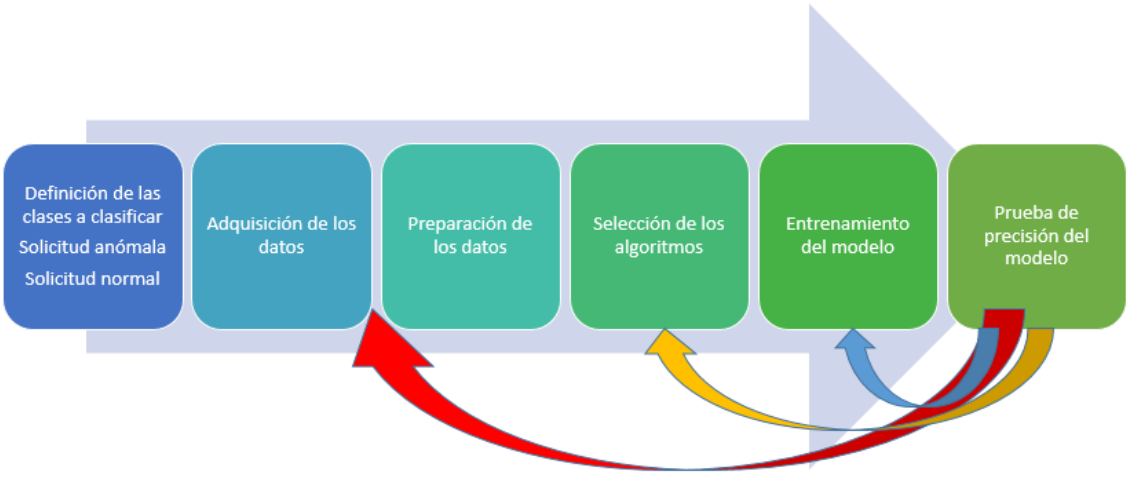
ESTRATEGIA METODOLÓGICA

Este proyecto busca crear una herramienta que realice la ejecución de modelos de clasificación supervisada del tráfico de red con el fin de rastrear intrusiones en aplicación web.

1. Adquirir la información para entrenamiento, seleccionando los sensores adecuados. Se recopilara los datos que necesitamos para responder la pregunta de investigación.
2. Transformar y procesar la información en un formato para sus procesamiento, Esto implicara realizar filtros y limpieza de la data capturada seleccionando los datos para entrenamiento
3. Seleccionamos los algoritmos a utilizar
4. Ejecutamos el entrenamiento
5. Prueba de precisión del modelo

Es posible que como resultado de la prueba de precisión del modelo si no satisface nuestra necesidad requiera ser refinado, si requiere refinamiento es volver al flujo de trabajo para modificar u obtener más datos o mejorar su preparación, mediante mejores filtros.

También es posible cambiar los algoritmos, que no dan un buen rendimiento o precisión, o ajustar los parámetros de entrenamiento.



Flujo de trabajo de aprendizaje de máquina para clasificador de intrusiones

Uso de herramientas de análisis de tráfico en internet como TCPDump/WinDump y wireshark. Serán los sensores de captura de datos.

Kali Linux es una distribución de Linux avanzada para pruebas de penetración y auditorías de seguridad y hherramientas

- Owasp Zed Attack Proxy
- JSQL Injection
- OpenVAS

Permitirán la generación de solicitudes o trafico malicioso. Siguiendo cada una de las siguientes fases para el ethical hacking.

DESARROLLO E IMPLEMENTACIÓN (AVANCES)

Adquisición de los datos

Para esta fase se estableció el montaje de máquinas virtuales para elaborar un laboratorio, donde se despliegan aplicaciones web desarrolladas sobre la tecnología de .net sobre el servidor de aplicaciones IIS; estas aplicaciones son tomadas de repositorios de las entidades en la que he trabajado incluye (web services, web site, web API) son versiones anteriores que hoy día utilizan en producción.

La máquina que es atacada es un Windows server 2012, con los últimos parches y aplicando una lista de chequeo de hardenning del CIS Center for Internet Security [https://www.cisecurity.org/cis-benchmarks/],para reducir la superficie de ataque. Adicionalmente se prepara una maquina Linux kali con las herramientas necesarias para la auditoria. En la maquina Windows server se instala un IDS (Sistema de detección de intrusiones basado en red) basado en expresiones regulares, configurado con todas las alertas, con el fin de registrar, los eventos de intrusión, con este IDS nos servirá con filtro para la preparación de los datos de entrenamiento y como sensor.

Preparación de los Datos

La captura de los paquetes de red realizada en formato binario logs sea en modo binario, es registrada en disco y contienen request sobre el protocolo http, de trafico normal como de trafico anómalo, generado en hacking ético realizo, le aplicamos filtros para depurar, protocolos que no son del interés de estudio.

Selección de los algoritmos y entrenamiento

En paralelo y basados en la consulta de los artículos, seleccionamos algunos algoritmos a utilizar en este proyecto Naive bayes, Arboles de decisión y SVM.

Aplicamos Naive bayes, obteniendo los siguientes resultados

Se tomaran los dados de HTTP DATASET CSIC 2010 [http://www.isi.csic.es/dataset/],este conjunto de datos contiene el tráfico generado dirigido a una aplicación web de comercio electrónico, contiene 36.000 solicitudes normales y más de 25.000 solicitudes anómalas.

Las solicitudes HTTP se etiquetan como normales o anómalas y el conjunto de datos incluye ataques tales como inyección de SQL, desbordamiento de búfer, recopilación de información, revelación de archivos, inyección XSS.

Extracción y selección de características

Se estos archivos se tomaron 20000 solicitudes de cada clase. Equivalente al 80%.

Entrenamiento -

Clasificador Naive bayes

Definición del vocabulario (Características)

Solicitudes HTTP etiquetados como [Solicitud anómala].ver Tabla 1.

Palabra	Cantidad
SCRIPT	1544
ALERT	242
VAR	221
SELECT	128
FROM	210
WHERE	124
OR	31338

TABLE	7
AND	557
DATABASE	3
.GIF	836
.JPG	118
LOGIN	1273
HOST	41439
COOKIE	16039
HTTP	15497
LINUX	15497
XML	46491
LINUX	15497
XML	46491

Tabla 1

Solicitudes HTTP etiquetados como [Solicitud normal].ver Tabla 2

Palabra	Cantidad
VAR	104
OR	25218
AND	142
.GIF	2235
.JPG	1788
LOGIN	772
HOST	42281
COOKIE	16097
HTTP	16098
LINUX	16098
XML	48294

Tabla 2

Vocabulario

Definición del vocabulario. Ver Tabla 3. Tamaño total del vocabulario: 340691

171564 de Solicitud anómala (y) ,169127 de Solicitud Normal: (x)

Palabra	Normal	Anómala
SCRIPT	0	1544
ALERT	0	242
VAR	104	221
SELECT	0	128
FROM	0	210
WHERE	0	124
OR	25218	31338
TABLE	0	7
AND	142	557
DATABASE	0	3
.GIF	2235	836
.JPG	1788	118
LOGIN	772	1273
HOST	42281	41439
COOKIE	16097	16039
HTTP	16098	15497
LINUX	16098	15497
XML	48294	46491

Tabla 3

Probabilidades a-priori

$$\begin{aligned} \mathrm{N}_i &= 20000 \\ p(\Theta_s) &= N_i / \textstyle\sum_{j=1}^{k} N_j \\ p(\Theta_x) &= 20000/(20000+20000) = 0,5 \\ p(\Theta_y) &= 20000/(20000+20000) = 0,5 \end{aligned}$$

Probabilidades condicionadas

Palabra	Probabilidad
p(SCRIPT |Solicitudnormal)=	0,0000059
p(SCRIPT |Solicitudanomala)=	0,0090054
p(ALERT |Solicitudnormal)=	0,0000059
p(ALERT |Solicitudanomala)=	0,0014164
p(VAR |Solicitudnormal)=	0,0006208
p(VAR |Solicitudanomala)=	0,0012940
p(SELECT |Solicitudnormal)=	0,0000059
p(SELECT|Solicitudanomala)=	0,0007519

p(FROM|Solicitudnormal)=	0,0000059
p(FROM|Solicitudanomala)=	0,0012299
p(WHERE|Solicitudnormal)=	0,0000059
p(WHERE|Solicitudanomala)=	0,0007286
p(OR|Solicitudnormal)=	0,1491128
p(OR|Solicitudanomala)=	0,1826665
p(TABLE|Solicitudnormal)=	0,0000059
p(TABLE|Solicitudanomala)=	0,0000466
p(AND|Solicitudnormal)=	0,0008455
p(AND|Solicitudanomala)=	0,0032524
p(DATABASE|Solicitudnormal)=	0,0000059
p(DATABASE|Solicitudanomala)=	0,0000233
p(.GIF|Solicitudnormal)=	0,0132208
p(.GIF|Solicitudanomala)=	0,0048786
p(.JPG|Solicitudnormal)=	0,0105779
p(.JPG|Solicitudanomala)=	0,0006936
p(LOGIN|Solicitudnormal)=	0,0045705
p(LOGIN|Solicitudanomala)=	0,0074258
p(HOST|Solicitudnormal)=	0,2500015
p(HOST|Solicitudanomala)=	0,2415425
p(COOKIE|Solicitudnormal)=	0,0951829
p(COOKIE|Solicitudanomala)=	0,0934928
p(HTTP|Solicitudnormal)=	0,0951888
p(HTTP|Solicitudanomala)=	0,0903336
p(LINUX|Solicitudnormal)=	0,0951888
p(LINUX|Solicitudanomala)=	0,0903336
p(XML|Solicitudnormal)=	0,2855546
p(XML|Solicitudanomala)=	0,2709892

Score 0.2273

RESULTADOS PRELIMINARES

Matriz Confusión de Naive Bayes

		Real	
		A	N
Estimada	A	30	8
	N	8	34
	Tot	38	42

Tot	TP	TP%	FP	FP%	FN	FN%	TN	TN%
38	30	78,9%	8	19,0%	8	21,1%	34	-89,5%
42	34	81,0%	8	21,1%	8	19,0%	30	-71,4%
80	64	80,0%	16	20,1%	16	20,0%	64	-80,0%

Sensibilidad	TP/(TP+FN)		80,0%
Especificidad	TN/(TN+FP)		80,0%

El algoritmo de clasificación que se utilizó para el experimento Naive Bayes, Los resultados de la fase de pruebas se encuentran 80 %

REFERENCIAS

Aburomman, A. A., & Ibne Reaz, M. Bin. (2016). A novel SVM-kNN-PSO ensemble method for intrusion detection system. *Applied Soft Computing Journal*, *38*, 360–372. https://doi.org/10.1016/j.asoc.2015.10.011

Al-Yaseen, W. L., Othman, Z. A., & Nazri, M. Z. A. (2017). Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system. *Expert Systems with Applications*, *67*, 296–303. https://doi.org/10.1016/j.eswa.2016.09.041

Albayati, M., & Issac, B. (2015). Analysis of Intelligent Classifiers and Enhancing the Detection Accuracy for Intrusion Detection System. *International Journal of Computational Intelligence Systems*, *8*(5), 841–853. https://doi.org/10.1080/18756891.2015.1084705

Alzhrani, K., Rudd, E. M., Boult, T. E., & Chow, C. E. (2016). Automated Big Text Security Classification, 103–108.

Amin, M. R., Zaman, M., Hossain, M. S., & Atiquzzaman, M. (2016). Behavioral malware detection approaches for Android. In I. I. 2016-M. and W. N. Symposium & Behavioral (Eds.), *2016 IEEE International Conference on Communications (ICC)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICC.2016.7511573

Ashfaq, R. A. R., Wang, X.-Z., Huang, J. Z., Abbas, H., & He, Y.-L. (2017). Fuzziness based semi-supervised learning approach for intrusion detection system. *Information Sciences*, *378*, 484–497. https://doi.org/10.1016/j.ins.2016.04.019

Bi, Y. (2016). A hybrid PSO-SVM model for network intrusion detection. *Ijsn*, *11*(4), 196–203. https://doi.org/10.1504/IJSN.2016.079258

Brahma, A., & Panigrahi, S. (2015). A new approach to intrusion detection in databases by using artificial neuro fuzzy inference system. *International Journal of Reasoning-Based Intelligent Systems*, *7*(3/4), 254. https://doi.org/10.1504/IJRIS.2015.072952

Chimphlee, W., Abdullah, A. H., Sap, M. N. M., Srinoy, S., & Chimphlee, S. (2006). Anomaly-Based Intrusion Detection using Fuzzy Rough Clustering. *2006 International Conference on Hybrid Information Technology*, *1*, 329–334. https://doi.org/10.1109/ICHIT.2006.253508

Elbasiony, R. M., Sallam, E. A., Eltobely, T. E., & Fahmy, M. M. (2013). A hybrid network intrusion detection framework based on random forests and weighted k-means. *Ain Shams Engineering Journal*, *4*(4), 753–762. https://doi.org/10.1016/j.asej.2013.01.003

Epishkina, A., & Zapechnikov, S. (2016). A syllabus on data mining and machine learning with applications to cybersecurity. In *2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC)* (pp. 194–199). IEEE.

https://doi.org/10.1109/DIPDMWC.2016.7529388

Hatcher, W. G., Maloney, D., & Yu, W. (2016). Machine learning-based mobile threat monitoring and detection. *2016 IEEE/ACIS 14th International Conference on Software Engineering Research, Management and Applications, SERA 2016*, 67–73. https://doi.org/10.1109/SERA.2016.7516130

Hsiao, S.-W., Sun, Y. S., & Chen, M. C. (2016). Behavior grouping of Android malware family. In *2016 IEEE International Conference on Communications (ICC)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICC.2016.7511424

Indre, I., & Lemnaru, C. (2016). Detection and prevention system against cyber attacks and botnet malware for information systems and Internet of Things. *2016 IEEE 12th International Conference on Intelligent Computer Communication and Processing (ICCP)*, 175–182. https://doi.org/10.1109/ICCP.2016.7737142

Jang, J. wook, Yun, J., Mohaisen, A., Woo, J., & Kim, H. K. (2016). Detecting and classifying method based on similarity matching of Android malware behavior with profile, *5*(1). https://doi.org/10.1186/s40064-016-1861-x

Khan, U., Schmidt-Thieme, L., & Nanopoulos, A. (2017). Collaborative SVM classification in scale-free peer-to-peer networks. *Expert Systems with Applications*, *69*, 74–86. https://doi.org/10.1016/j.eswa.2016.10.008

Kuang, F., Zhang, S., Jin, Z., & Xu, W. (2015). A novel SVM by combining kernel principal component analysis and improved chaotic particle swarm optimization for intrusion detection. *Soft Computing*, *19*(5), 1187–1199. https://doi.org/10.1007/s00500-014-1332-7

Lin, G. T. R., Lin, C. C., Chou, C. J., & Lee, Y. C. (2014). Fuzzy modeling for information security management issues in cloud computing. *International Journal of Fuzzy Systems*, *16*(4), 529–540. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84920682189&partnerID=tZOtx3y1

Lopez, C. C. U., & Cadavid, A. N. (2016). Machine learning classifiers for android malware analysis. In *2016 IEEE Colombian Conference on Communications and Computing (COLCOM)* (pp. 1–6). IEEE. https://doi.org/10.1109/ColComCon.2016.7516385

Mahmoud, M. K. A., Al-Jumaily, A., Maali, Y., & Anam, K. (2013). Classification of Malignant Melanoma and Benign Nevi from Skin Lesions Based on Support Vector Machine. In *2013 Fifth International Conference on Computational Intelligence, Modelling and Simulation* (pp. 236–241). IEEE. https://doi.org/10.1109/CIMSim.2013.45

Pajouh, H. H., Dastghaibyfard, G., & Hashemi, S. (2015). Two-tier network anomaly detection model: a machine learning approach. *Journal of Intelligent Information Systems*, (2), 1–14. https://doi.org/10.1007/s10844-015-0388-x

Pandeeswari, N., & Kumar, G. (2016). Anomaly Detection System in Cloud Environment Using Fuzzy Clustering Based ANN. *Mobile Networks and*

Applications, *21*(3), 494–505. https://doi.org/10.1007/s11036-015-0644-x

Pozi, M. S. M., Sulaiman, M. N., Mustapha, N., & Perumal, T. (2016). Improving Anomalous Rare Attack Detection Rate for Intrusion Detection System Using Support Vector Machine and Genetic Programming. *Neural Processing Letters*, *44*(2), 279–290. https://doi.org/10.1007/s11063-015-9457-y

Ravitch, T., Creswick, E. R., Tomb, A., Foltzer, A., Elliott, T., & Casburn, L. (2014). Multi-App Security Analysis with FUSE. In *Proceedings of the 4th Program Protection and Reverse Engineering Workshop on 4th Program Protection and Reverse Engineering Workshop - PPREW-4* (pp. 1–10). New York, New York, USA: ACM Press. https://doi.org/10.1145/2689702.2689705

Shamshirband, S., Daghighi, B., Anuar, N. B., Kiah, M. L. M., Patel, A., & Abraham, A. (2015). Co-FQL: Anomaly detection using cooperative fuzzy Q-learning in network. *Journal of Intelligent and Fuzzy Systems*, *28*(3), 1345–1357. https://doi.org/10.3233/IFS-141419

Swarnkar, M., & Hubballi, N. (2016). OCPAD: One class Naive Bayes classifier for payload based anomaly detection. *Expert Systems with Applications*, *64*, 330–339. https://doi.org/10.1016/j.eswa.2016.07.036

Transactions, S. (2015). Secure software engineering requirements in cloud environment by using anticipating learning classifier system Wafa ' Slaibi Alsharafat, *6*(1).

Viegas, E., Santin, A. O., Franca, A., Jasinski, R., Pedroni, V. A., & Oliveira, L. S. (2017). Towards an Energy-Efficient Anomaly-Based Intrusion Detection Engine for Embedded Systems. *IEEE Transactions on Computers*, *66*(1), 163–177. https://doi.org/10.1109/TC.2016.2560839

Wang, G., Hao, J., Ma, J., & Huang, L. (2010). A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering. *Expert Systems with Applications*, *37*(9), 6225–6232. https://doi.org/10.1016/j.eswa.2010.02.102

Wang, W., He, Y., Liu, J., & Gombault, S. (2015). Constructing important features from massive network traffic for lightweight intrusion detection. *IET Information Security*, *9*(6), 374–379. https://doi.org/10.1049/iet-ifs.2014.0353

Williams, J. (2017). *OWASP Top 10 - 2017 RC1*.

Yu, J., Huang, Q., & Yian, C. (2016). DroidScreening: A practical framework for real-world Android malware analysis. John Wiley and Sons Inc. https://doi.org/10.1002/sec.1430

Zaerens, K. (2015). Business Resilient Vulnerability Analysis for Dynamic High Security Environment. In *2015 18th International Conference on Network-Based Information Systems* (pp. 242–249). IEEE. https://doi.org/10.1109/NBiS.2015.39

Zhou, C., Huang, S., Xiong, N., Yang, S.-H., Li, H., Qin, Y., & Li, X. (2015). Design and Analysis of Multimodel-Based Anomaly Intrusion Detection Systems in Industrial Process Automation. *IEEE Transactions on Systems, Man, and*

Cybernetics: Systems, *45*(10), 1345–1360.
https://doi.org/10.1109/TSMC.2015.2415763