Managing Information Security Risks in the Age of IoT

Abedallah Z. Abualkishik *, Rasha Almajed

American University in the Emirates, Dubai, UAE

Emails: abedallah.abualkishik@aue.ae ; rasha.almajed@aue.ae

Abstract

The advent of the Internet of Things (IoT) has led to the proliferation of connected devices, creating numerous security challenges. With billions of devices generating vast amounts of data, managing information security risks in the age of IoT has become increasingly complex. Traditional security approaches are not sufficient to mitigate the risks posed by IoT devices. Machine learning (ML) provides a promising approach to enhance the security of IoT systems. This paper proposes a machine learning approach for managing information security risks in the age of IoT. The proposed approach utilizes ML algorithms to identify and mitigate security threats in IoT systems. The approach involves collecting and analyzing data from IoT devices, and applying ML algorithms to detect patterns and anomalies that may indicate security threats. The ML algorithms are trained using both supervised and unsupervised learning techniques to enable them to identify known and unknown threats. The paper describes a case study in which the proposed approach is applied to an IoT system for home security. The results demonstrate that the ML approach can effectively detect security threats in the IoT system and mitigate them in real-time.

Keywords: Internet of Things (IoT); Information Security and Risks; Machine Learning (ML);

1. Introduction

The Internet of Things (IoT) has revolutionized the way we interact with technology, with an estimated 35 billion IoT devices in use worldwide. This rapid expansion has created a new range of security risks, as every connected device represents a potential vulnerability. Therefore, managing information security risks in the age of IoT requires a comprehensive approach that includes identifying potential threats, assessing their likelihood and impact, implementing appropriate security controls, and monitoring for new risks and vulnerabilities.

To effectively manage security risks in the age of IoT, organizations must adopt a risk-based approach that prioritizes their most critical assets and systems. This involves conducting a thorough risk assessment to identify potential threats and vulnerabilities and assessing their likelihood and potential impact. Based on this analysis, organizations can develop a risk management plan that includes appropriate security controls and risk mitigation strategies, such as encryption, network segmentation, and regular software updates. Additionally, organizations should continuously monitor their systems for new risks and vulnerabilities, and regularly review and update their risk management plan to ensure it remains effective in the face of evolving threats.

There are several key research problems related to managing information security risks in the age of IoT that require further investigation. With such a vast array of connected devices, it can be difficult to understand the interdependencies and interactions between them, making it challenging to accurately assess risk. As the technology evolves rapidly, new vulnerabilities and threats can emerge, making it critical to develop effective and scalable security solutions that can keep up with these changes. Furthermore, given the diverse range of devices and systems involved in IoT, there is a need to develop flexible and adaptable security solutions that can work across a range of platforms and environments.

Doi : https://doi.org/10.54216/JCIM.110103
Received: October 21, 2022 Revised: December 23, 2022 Accepted: January 04, 2023

2. Related Work

The literature on Information Security contains a lot of studies highlighting the growing importance of securing interconnected devices in today's digital age. The research in this area focuses on understanding the security risks associated with IoT devices, identifying potential threats and vulnerabilities, and developing effective security controls and risk mitigation strategies. For example, Siddiqui et al [3] explored the security threats and attacks associated with the IoT and proposed possible countermeasures to mitigate them. They identified a range of security threats such as physical attacks, network attacks, and application attacks that can compromise the confidentiality, integrity, and availability of IoT devices and systems. They then developed several countermeasures, including the use of secure communication protocols, device authentication mechanisms, and intrusion detection systems. In [4], Abdel-Basset et al. developed an intrusion detection approach, named Deep-IFS, for securing information Industrial IoT traffic based on fog environment. They addressed the challenge of detecting malicious activities in industrial IoT systems, which are characterized by many interconnected devices and high-speed data transfer. They used a deep learning-based algorithm to analyze network traffic and detect anomalous behavior. The approach is implemented in a fog computing environment, which provides real-time processing of data close to the source. Hossain et al [8] analyzed and identified various security challenges associated with IoT, such as privacy, authentication, access control, and data integrity. They discussed how these challenges arise due to the large number of heterogeneous devices, the lack of standardization, and the lack of centralized management. They also proposed several potential solutions, such as the use of lightweight cryptography, secure key management, and secure data transmission protocols. Sfar et al [10] presented a roadmap for identifying a range of security challenges in IoT, and developed a framework that includes several layers of security, such as physical security, network security, and application security, to address these challenges. They also discussed the importance of trust management in IoT and propose several trust models to establish and maintain trust between IoT devices and users. Kumar et al [13] explored several security challenges in IoT, such as privacy, data protection, authentication, and authorization. They also studied several solutions to those challenges, including the use of encryption, secure communication protocols, and access control mechanisms to address these challenges. Chasaki and Mansour [15] studied the importance of security awareness and education for IoT users and stakeholders to mitigate security risks. They highlighted the need for further research to address security challenges in IoT, particularly in the areas of secure data transmission, secure data storage, and secure software development practices. Mozzaquatro et al. [18] proposed an ontology-based cybersecurity framework for the IoT, which included several layers of security, such as network security, data security, and user security, to address different security aspects in IoT. They also proposed a set of cybersecurity rules and policies to ensure the secure and trustworthy operation of IoT systems. The ontology-based approach empowered framework to automatically reason about security-related information, identify security risks, and recommend appropriate security measures. Kouzinopoulos et al [22] proposed the use of blockchain technology with a decentralized and tamper-proof platform for securing IoT communication and data management. They used a private blockchain to only authorized devices to participate in the network and ensures the integrity of the data stored on the blockchain. A consensus algorithm was presented based on proof-of-work to ensure the security and reliability of the blockchain network.

3. The Proposed methodology for managing information security in IoT applications

The research approach for this study is primarily quantitative, with a focus on data analysis and statistical modeling. The study involved collecting data from an IoT system for home security, which was used to train and test ML algorithms for detecting security threats. A case study if malware detection approach was used to demonstrate the proposed solution for managing information security risks in context of IoT. The case study involved an IoT system for home security, which was used to collect malware instances for analysis. The data included sensor readings, network traffic, and user behavior logs. Malmem-2022 dataset is public opensource dataset that is used to in our framework [31]. The CIC-MalMem-2022 dataset is a malware memory dataset that was released by the Canadian Institute for Cybersecurity (CIC) at the University of New Brunswick. The dataset contains a large collection of malware samples captured in the memory of infected systems. It includes a total of 58,596 unique malware samples, 50% malicious and 50% benign. The dataset is designed to be used for the development and evaluation of ML models for malware detection in the Information Security system. It provides researchers and practitioners with a valuable resource for testing the effectiveness of different Information security approaches for IoT systems.

The class distribution of the Malmem-2022 dataset is provided in Table 1.

Doi : https://doi.org/10.54216/JCIM.110103
Received: October 21, 2022 Revised: December 23, 2022 Accepted: January 04, 2023

Table 1: Class Distribution in Malmem-2022 Dataset.

Malware category	Malware families	Count
Trojan Horse	Emotet	196
	Reconyc	157
	Refroso	200
	scar	200
	Zeus	195
Spyware	Transponder	241
	TIBS	141
	Gator	200
	Coolwebsearch	200
	180Solutions	200
Ransomware	Ako	200
	Conti	200
	MAZE	195
	Pysa	171
	Shade	220

The data analysis methods used in our research approach included exploratory data analysis, statistical modeling, and feature analysis. The CIC-Malmem-2022 Dataset was first cleaned and pre-processed to remove any outliers and missing values. Exploratory data analysis was conducted to gain insights into the characteristics of the data and identify any patterns or anomalies that may indicate security threats (See Figure 1).

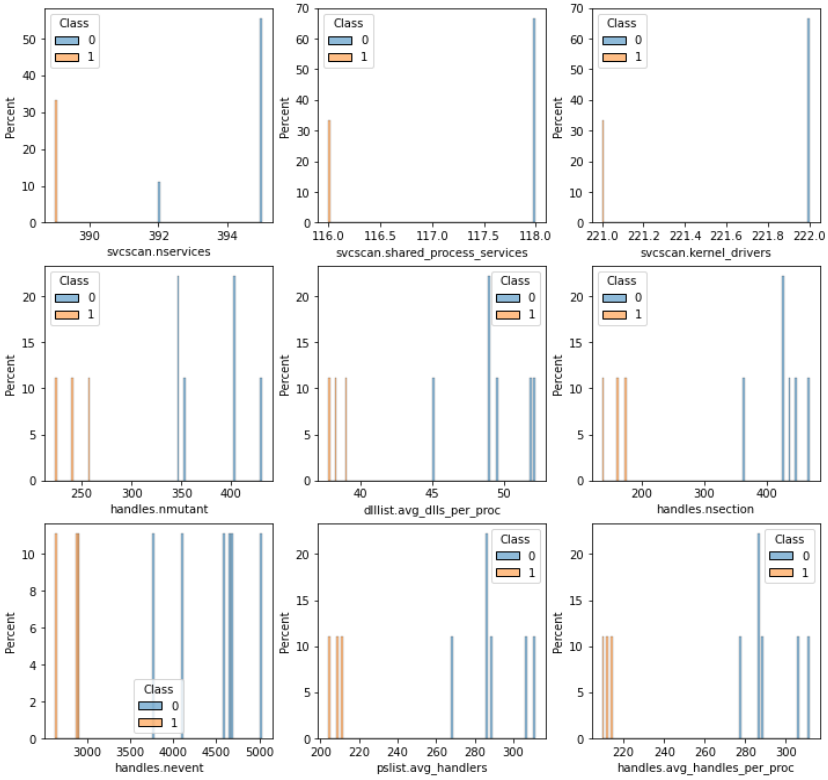

Figure 1: Visualization of feature analysis in for the

Doi : https://doi.org/10.54216/JCIM.110103
Received: October 21, 2022 Revised: December 23, 2022 Accepted: January 04, 2023

Statistical analysis is used in our framework to develop predictive models for identifying behavior of malware threats in the IoT system. The goal of statistical analysis is to extract meaningful insights from the data that can be used to improve the accuracy and effectiveness of the machine learning models used for malware detection. By analyzing the statistics of data presented in Table 2, we can identify common features and behaviors that can be used to recognize and classify malware in our information security approach.

Table 2: The descriptive statistics of the CIC-Malmem-2022 dataset are given in Table 2.

	count	mean	std	min	25%	50%	75%	max
pslist.nproc	58596	41.394771	5.777249	21	40	41	43	240
pslist.nppid	58596	14.713837	2.656748	8	12	15	16	72
pslist.avg_threads	58596	11.341655	1.588231	1.65	9.972973	11	12.861955	16.818182
pslist.nprocs64bit	58596	0	0	0	0	0	0	0
pslist.avg_handlers	58596	247.509819	111.85779	34.9625	208.725	243.96371	289.974322	24845.95122
dlllist.ndlls	58596	1810.805447	329.782639	670	1556	1735	2087	3443
dlllist.avg_dlls_per_proc	58596	43.707806	5.742023	7.333333	38.833333	42.781524	49.60528	53.170732
handles.nhandles	5.86E+04	1.03E+04	4.87E+03	3.51E+03	8.39E+03	9.29E+03	1.22E+04	1.05E+06
handles.avg_handles_per_proc	58596	249.560958	145.999866	71.139241	209.648228	247.208951	291.35505	33784.19355
handles.nport	58596	0	0	0	0	0	0	0
...	...	...	...	...	...	...	...	...
svcscan.nservices	58596	391.347549	4.529704	94	389	389	395	395
svcscan.kernel_drivers	58596	221.406581	1.991087	55	221	221	222	222
svcscan.fs_drivers	58596	25.996245	0.17079	6	26	26	26	26
svcscan.process_services	58596	25.063417	1.529628	7	24	24	27	27
svcscan.shared_process_services	58596	116.879514	1.550401	26	116	116	118	118
svcscan.interactive_process_services	58596	0	0	0	0	0	0	0
svcscan.nactive	58596	121.995546	2.822858	30	121	122	123	129
callbacks.ncallbacks	58596	86.905659	3.134117	50	87	87	88	89
callbacks.nanonymous	58596	0.000853	0.029199	0	0	0	0	1
callbacks.ngeneric	58596	7.999881	0.010929	7	8	8	8	8

According to the above analysis, we decided that the data of our case study need to undergo data preparation process, to be ready to train ML model. To this end, several data preparation steps are considered in our research approach. First, data is cleaned by removing any irrelevant or duplicate data. This can include removing empty or null fields, removing duplicates, and removing irrelevant data that may not be relevant for malware detection. Next, feature

Doi : https://doi.org/10.54216/JCIM.110103
Received: October 21, 2022 Revised: December 23, 2022 Accepted: January 04, 2023

scaling is applied to normalize the features so that they have a similar range and scale. This can help to improve the accuracy of the machine learning models by reducing the impact of features that have a large scale or variance.

$$x_{in} = \frac{x_{in} - \mu}{\sigma} \quad (1)$$

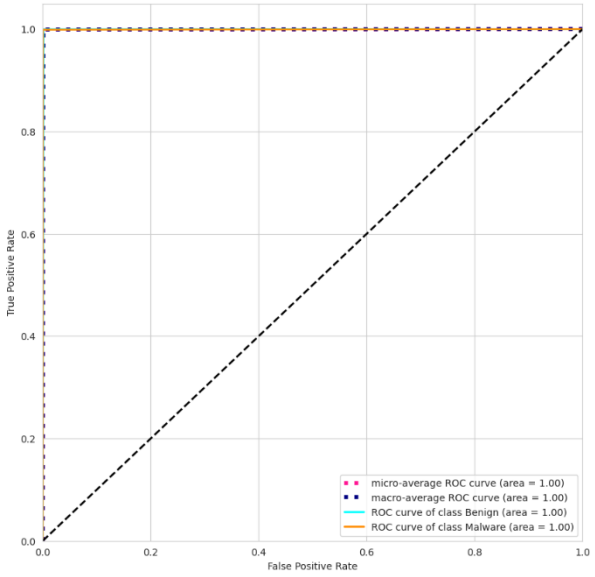

Figure 2: RoC analysis for our information security approach

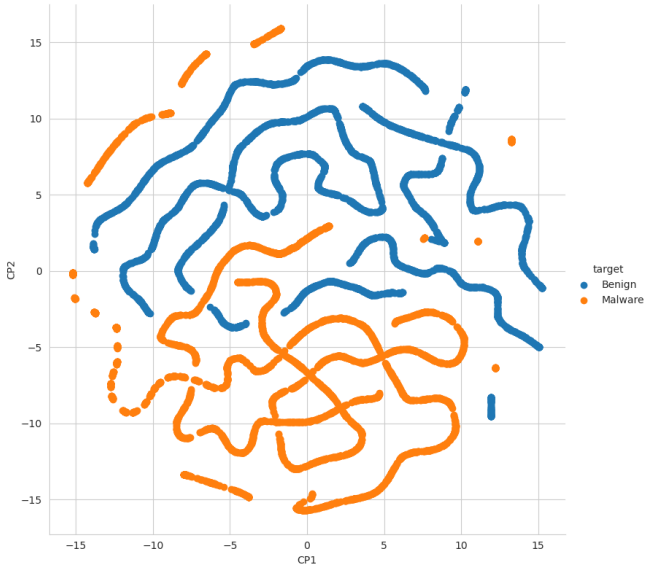

Figure 3: T-SNE analysis for our information security approach

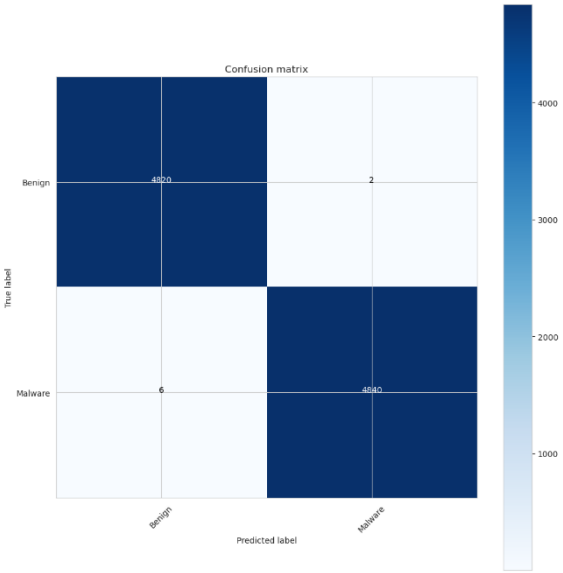

Figure 4: Confusion analysis for our information security approach

Then, feature selection is applied to select the most relevant features from the dataset, which helps to reduce the dimensionality of the dataset. The dataset is split into training, validation, and testing sets. The training set (70%) is used to train the ML models, while the validation set (10%) is used to tune the hyperparameters of the models. The testing set is used to evaluate the performance of the models on unseen data.

Doi : https://doi.org/10.54216/JCIM.110103
Received: October 21, 2022 Revised: December 23, 2022 Accepted: January 04, 2023

The training data is then fed into a simple but effective convolutional model designed to identify malware from benign samples. The input layer is simply the input data itself. We can represent it as a vector x with dimensions $(input_{shape}, 1)$.. Then, the input is fed into convolutional layer to extract important features:

$$z_i = f(W_i * x_i + bi) \quad (2)$$

where W_i is the $i-th$ filter/kernel, x_i is a subset of the input data, b_i is the bias term, and f is the activation function. The symbol $*$ indicates the convolution operation, which is designated as:

$$(W_i * x_i)_j = sum\big(W_i(k) * x_i(j+k-1)\big) \, for \, k = 0 \, to \, K-1 \quad (3)$$

where K is the kernel size, j is the index of the output feature map, and $W_i(k)$ is the $k-th$ element of the filter/kernel. To add more convolutional layers, we simply repeat the above computations with a different filter/kernel size and number of filters. We can represent the output of the $(i+1)_{th}$ convolutional layer as a vector y_i with dimensions $(n_{i+1}+1, 1)$. To flatten the output of the final convolutional layer into a 1D vector, we simply reshape it as a vector with dimensions $(n_{out}, 1)$, where n_{out} is the number of output features from the final convolutional layer. The output of the $i-th$ fully connected layer is calculated as:

$$v_i = f(W_i * y_{i-1} + b_i) \quad (4)$$

where W_i is the weight matrix, $y_{i-1}$is the output of the previous layer, b_i is the bias term, and f is the activation function. The output of the final fully connected layer is the output of the network. Since we are solving a binary classification task, a sigmoid activation function is used to produce a single output value between 0 and 1.

$$sigmod\ (v_i) = -\frac{1}{1+e^{-v_i}} \quad (5)$$

4. Information Security Results

Receiver Operating Characteristic (ROC) curves are used in this work to analyze the performance of our ML-based information security approaches. The ROC curve is a graphical representation of the trade-off between the true positive rate (TPR) and false positive rate (FPR) for different thresholds of a classification model (See Figure 2). The area under the ROC curve (AUC) is a computed as a common metric to evaluate the performance of our system.

Moreover, t-SNE (t-distributed Stochastic Neighbor Embedding) plots are a applied in our experiments as powerful visualization tool for analyzing the performance of our information security approaches. As shown in Figure 3, t-SNE is a non-linear dimensionality reduction algorithm that is used to visualize high-dimensional data in two or three dimensions. It works by preserving the local structure of the data while also reducing the dimensionality of the data. The resulting t-SNE plot shows the clustering of the samples in the reduced dimensional space. Confusion matrix is also used to visually illustrate the performance of our approach, where the rows of the table correspond to the true class labels, while the columns correspond to the predicted class labels (See Figure 4). By examining the confusion matrix plot, we can gain insight into the efficiency of our system to discriminate between benign software and malware in IoT environments.

5. conclusion

This paper proposed a ML approach for managing information security risks in the age of IoT. The proposed approach involved collecting and analyzing data from IoT devices, and applying ML algorithms to detect patterns and anomalies that may indicate security threats. The approach was demonstrated in a case study of an IoT system for home security, which showed that the approach can effectively detect and mitigate security threats in real-time. The results of this research suggest that ML is a promising approach for enhancing the security of IoT systems. By using ML techniques, organizations can better manage information security risks in the aera of IoT and protect against potential security threats. However, further research is needed to explore the full potential of ML for IoT security and to develop more advanced ML algorithms for this purpose.

Doi : https://doi.org/10.54216/JCIM.110103
Received: October 21, 2022 Revised: December 23, 2022 Accepted: January 04, 2023

References

[1] Chen, K., Zhang, S., Li, Z., Zhang, Y., Deng, Q., Ray, S., & Jin, Y. (2018). Internet-of-Things security and vulnerabilities: Taxonomy, challenges, and practice. *Journal of Hardware and Systems Security*, *2*, 97-110.

[2] Razzaq, M. A., Gill, S. H., Qureshi, M. A., & Ullah, S. (2017). Security issues in the Internet of Things (IoT): A comprehensive study. *International Journal of Advanced Computer Science and Applications*, *8*(6).

[3] Siddiqui, S. T., Alam, S., Ahmad, R., & Shuaib, M. (2020). Security threats, attacks, and possible countermeasures in internet of things. In *Advances in Data and Information Sciences: Proceedings of ICDIS 2019* (pp. 35-46). Springer Singapore.

[4] Abdel-Basset, M., Chang, V., Hawash, H., Chakrabortty, R. K., & Ryan, M. (2020). Deep-IFS: Intrusion detection approach for industrial internet of things traffic in fog environment. *IEEE Transactions on Industrial Informatics*, *17*(11), 7704-7715.

[5] Li, S., Xu, L. D., & Zhao, S. (2015). The internet of things: a survey. *Information systems frontiers*, *17*, 243-259.

[6] Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. *The internet society (ISOC)*, *80*, 1-50.

[7] Abdel-Basset, M., Moustafa, N., Hawash, H., Ding, W. (2022). Internet of Things Security Requirements, Threats, Attacks, and Countermeasures. *Deep Learning Techniques for IoT Security and Privacy*, 67-112.

[8] Hossain, M. M., Fotouhi, M., & Hasan, R. (2015, June). Towards an analysis of security issues, challenges, and open problems in the internet of things. In *2015 ieee world congress on services* (pp. 21-28). IEEE.

[9] Masoodi, F., Alam, S., & Siddiqui, S. T. (2019). Security & privacy threats, attacks and countermeasures in Internet of Things. *International Journal of Network Security & Its Applications (IJNSA) Vol*, *11*.

[10] Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks*, *4*(2), 118-137.

[11] Jurcut, A., Niculcea, T., Ranaweera, P., & Le-Khac, N. A. (2020). Security considerations for Internet of Things: A survey. *SN Computer Science*, *1*, 1-19.

[12] Abdel-Basset, M., Moustafa, N., & Hawash, H. (2022). *Deep Learning Approaches for Security Threats in IoT Environments*. John Wiley & Sons.

[13] Kumar, S. A., Vealey, T., & Srivastava, H. (2016, January). Security in internet of things: Challenges, solutions and future directions. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 5772-5781). IEEE.

[14] Adat, V., & Gupta, B. B. (2018). Security in Internet of Things: issues, challenges, taxonomy, and architecture. *Telecommunication Systems*, *67*, 423-441.

[15] Chasaki, D., & Mansour, C. (2020, February). Improving Efficiency in Attack Detection through Real-time Processing Monitoring and Machine Learning. In 2020 International Conference on Computing, Networking and Communications (ICNC) (pp. 145-151). IEEE.

[16] Ahmad, M., Younis, T., Habib, M. A., Ashraf, R., & Ahmed, S. H. (2019). A review of current security issues in Internet of Things. *Recent trends and advances in wireless and IoT-enabled networks*, 11-23.

[17] Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. Digital Communications and Networks, 4(2), 118-137.

[18] Mozzaquatro, B. A., Agostinho, C., Goncalves, D., Martins, J., & Jardim-Goncalves, R. (2018). An ontology-based cybersecurity framework for the internet of things. *Sensors*, *18*(9), 3053.

[19] Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, *22*(2), 1191-1221.

[20] Vashi, S., Ram, J., Modi, J., Verma, S., & Prakash, C. (2017, February). Internet of Things (IoT): A vision, architectural elements, and security issues. In 2017 international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 492-496). IEEE.

[21] Radanliev, P., De Roure, D. C., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S., & Burnap, P. (2018). Future developments in cyber risk assessment for the internet of things. *Computers in industry*, *102*, 14-22.

[22] Kouzinopoulos, C. S., Spathoulas, G., Giannoutakis, K. M., Votis, K., Pandey, P., Tzovaras, D., ... & Nijdam, N. A. (2018). Using blockchains to strengthen the security of internet of things. In *Security in Computer and Information Sciences: First International ISCIS Security Workshop 2018, Euro-CYBERSEC 2018, London, UK, February 26-27, 2018, Revised Selected Papers 1* (pp. 90-100). Springer International Publishing.

Doi : https://doi.org/10.54216/JCIM.110103
Received: October 21, 2022 Revised: December 23, 2022 Accepted: January 04, 2023

[23] Weber, M., & Boban, M. (2016, May). Security challenges of the internet of things. In *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 638-643). IEEE.
[24] Perera, C., Ranjan, R., Wang, L., Khan, S. U., & Zomaya, A. Y. (2015). Big data privacy in the internet of things era. *IT Professional*, *17*(3), 32-39.
[25] Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks*, *141*, 199-221.
[26] Azrour, M., Mabrouki, J., Guezzaz, A., & Kanwal, A. (2021). Internet of things security: challenges and key issues. *Security and Communication Networks*, *2021*, 1-11.
[27] Arias, O., Wurm, J., Hoang, K., & Jin, Y. (2015). Privacy and security in internet of things and wearable devices. *IEEE Transactions on Multi-Scale Computing Systems*, *1*(2), 99-109.
[28] Mishra, S., Sahoo, S., & Mishra, B. K. (2019). Addressing security issues and standards in Internet of things. In *Emerging trends and applications in cognitive computing* (pp. 224-257). IGI Global.
[29] Li, S., Tryfonas, T., & Li, H. (2016). The Internet of Things: a security point of view. *Internet Research*.
[30] Mugarza, I., Flores, J. L., & Montero, J. L. (2020). Security issues and software updates management in the industrial internet of things (iiot) era. *Sensors*, *20*(24), 7160.
[31] Carrier, T., Victor, P., Tekeoglu, A., & Lashkari, A. H. (2022, February). Detecting Obfuscated Malware using Memory Feature Engineering. In *ICISSP* (pp. 177-188).

Doi : https://doi.org/10.54216/JCIM.110103
Received: October 21, 2022 Revised: December 23, 2022 Accepted: January 04, 2023