20th International Conference on Renewable Energies and Power Quality (ICREPQ'22)
Vigo (Spain), 27th to 29th July 2022
Renewable Energy and Power Quality Journal (RE&PQJ)
ISSN 2172-038 X, Volume No.20, September 2022

The relevance of IT Security awareness in Renewable Energy facilities

Justino Lourenço[1], Eric Zanghi[2], José Morais[1] Nelson Neves[2], César Vasques[3] e Fernando Figueiredo[3].

[1] Department of Computer Science Engineering
[2] Department of Electronics and Automation Engineering
[3] Department of Mechanical Engineering
ISPGAYA – Instituto Superior Politécnico Gaya
Avenida dos Descobrimentos, 333, Vila Nova de Gaia, Portugal
Phone/Fax number:+351 223745730, e-mail: jml@ispgaya.pt

Abstract. In recent years several efforts have being made in bringing smart network connectivity to the Renewable Energy Plant (REP) environment. On the other hand, REP is extending in scale from specialized points where the energy provider acts as a supplier to home REP (self-energy producers). This enables new important features such as: process automation, monitoring, control and optimizations. On the other hand, and in particular during and after the Covid19 pandemics the cybersecurity menace is a massive concern. The digital literacy of a worker of such an infrastructure is relevant to the correct implementation of adequate security policies. This article describes the threats and challenges on the field and conducts an enquire for perceiving the awareness of Automation and Mechanics Engineering students for this relevant problem, as future player in the field.

Key words. Renewable energies, Cybersecurity, Digital Literacy.

1. Introduction

Avoiding environment abuse is nowadays a top priority concern, along with the current -2022 energy crisis has also pushed the industry for REP solutions. The followed path of car electrification is also raising the delicate issue of producing efficient and clean electric energy.

The innovation in the sector is a constant evolutionary path. Powering a facility or even a single machine recurring to renewable energy strategies is an achieved goal **[1]**.

In the field of renewable energies several relevant research state-of-the-art projects have being conducted to improve efficiency and to rationalize installation costs by introducing several innovative approaches **[2]**, **[3]**, **[4]** **[5]**, **[6]**, **[7]**, **[8]**, **[9]** and **[10]**.

All the described goals and innovation achievements supported by data networks for data flow brought along the new introduction of concepts such as Big Data **[11]**, **[12]** and **[13]**, Artificial Intelligence (AI) **[14]**, **[15]**, **[16]**, **[17]**, **[18]**, Internet of Things (IoT) **[19]**, **[20]**, **[21]**, **[22]** and **[23]** and many others.

All these new technologies open the hot topic of cybersecurity into the REP world. Several state-of-the-art research bibliography describe a strong correlation between digital literacy and the cybersecurity risks increase **[24]**, **[25]**, **[26]** and **[27]**. The digital literacy among with a set of rules (security policies) and good IT practices will contract the security risk.

The purpose of this article is to understand the degree of cybersecurity literacy of Engineering students that have a high probability of leading a future project in the field of renewable energies.

2. Cybersecurity issues

This section will detail the most common risks in IT infrastructures. In particular, the increase cybersecurity attack during the Covid19 pandemic brought several new procedures to promote IT resilience in the organizations **[28]**, **[29]**, **[30]**.

A. Login and Password security

The authentication threw a login and a password is still the most common procedure to access IT services. This dependency is a strong point-of-failure in the cybersecurity chain.

A combination of a week password, without an aging mechanism implementation or even the access credentials shared with a coworker present a serious risk. Also of strong relevance the risk of a remote access without the support of a secured connection.

A multiple step authentication is an important step introduced to bypass these vulnerabilities.

Several proposals are presented as strategical countermeasures for this topic, with the support of machine learning techniques **[31]**, **[32]** using of secure logins protocols **[33]** and bringing Blockchain (BC) as a solution **[34]**.

B. *Phishing*

Establishing a contact from someone posing as a legitimate entity to lure a user into providing sensitivity data to gain access to a service of infrastructure is another cyberattack form.

The most common methodology to avoid this form of attack is supported by Web Crawling detection **[35]**, user training **[36]** and most recently with the support of machine learning models **[37]**.

C. *Ransomware*

This form of cyberattack explores a malware that employs encryption methodologies in order to hold a victim's information in a ransom.

The state-of-the art points to the support of AI tools as best tactics against this form of attack **[38]**, **[39]** and **[40]**.

D. *Software vulnerabilities and updates*

The layer of software has an increasing relevance in all the REP solutions. The interface with the user, all the data input, processing and output are the result of a secure code execution. Any coding flaw may be the open door for a security issue and it is an important point of research [41]. In particular, over the communication management software module – where all the information flows from and into a channel.

There are several forms of diluting this issue over the scientific literature: the development of software vulnerability prediction model. This solution enables to forecast whether a software module is vulnerable or not, this way bringing a relevant tool for the security improvement **[42]**. Automated vulnerabilities detection is also a proposal. With a new approach, a compressive experimental setup is created for accessing the methodology and report the vulnerabilities found **[43]**, **[44]**. The Static Code Analysis (SCA) has, also, a good detection rate and is the central technique for improving the effectiveness of vulnerability detection **[45]**. As a last bibliographic reference is from the support of machine learning solutions as relevant tool for the analysis of software vulnerabilities **[46]**.

A regular practice of constant software updating is also a simple form to improve software productivity and reduce the menace of software vulnerabilities.

E. *Wireless access*

The universal connection of devices in the wireless form was a relevant form of accessing corporate data all over the facilities and in remote work scenarios.

The data exposition increases during the radio frequency trip from one network hop to the next hop. Old classical methodologies such as the “man in the middle attack”, where a (illegitimate) node masked as a (falsely) certified network device intrudes a network, this way intercepting - On the other hand there are several hacking strategies to explore the intrinsic WLAN vulnerabilities described over t several state-of-the-art literature **[50]**, **[51]**, **[52]** and **[53]**.

3. Renewable Energy Facilities

As described in previous sections the increasing pressure of the fossil energy along with the demand for a greener environment is the perfect lever to increase the number of renewable energy facilities around the globe. Iceland is a relevant case of study. Its massive adoption of green energy around the country is an worldwide good example **[54]**, **[55]**, **[56]**, **[57]** and **[58]**.

The quest, as also previously described, for the full adoption of new and trendy IT approaches in order to provide remote full access to energy production data, secure connections for telemetry and control, autonomous and intelligent tuning of the resources collected in the green energy production (with the goal of maximization of the production and minor ambient impact), overall management of the network of energy production, fault autonomous / human response and facility security management – will be the key innovation (already in motion) in the current decade.

So technical issues related to data networks, such as cryptography, BC, AI or Cloud storage and processing will be relevant topics.

4. Methodology

The study methodology –an enquiry -implemented was conducted in two Higher Education Institutions (HEI) in Northern Portugal The enquiry population was shared engineering with the students (Electronics and Mechanical Engineering), The General objective were: evaluation of the cybersecurity risks awareness. The study was conducted in march 2022. To maintain the confidentiality of the studied contexts, the anonymity of all the students, as well as the confidentiality of the HEI, one proceeded to their identification by HIE1 and HIE2.

The data collection procedure was performed by invitation for investigation, in writing, addressed to the Directors of Higher Education Institutions, and students were asked for participate threw an email with the survey link. The following questioner were implemented:

1. How do you rate your knowledge about security?
   A. Following the news using the regular press?
   B. I do try to learn more threw websites, book or other information sources?
   C. I am a typical careful Internet user?
2. Are you aware of the risks associated with login/Password credentials and how to avoid them?
   A. I do use long passwords with numbers and special characters?
   B. Some of my colleagues may know my login and password?
   C. I do change in a regular form my passwords?
   D. Do you memorize your passwords or are they stored on your mobile phone or computer?
   E. Sometimes I share passwords between different sites to help memorizing them?
3. Do you know the process of “phishing”?
   A. I do reply to all the challenges sent by email oi in social media even when the source of them is unknown?
   B. Are you confident enough to send sensitive personal data over Internet?
4. Do you the meaning of Ransomware?
   A. Typically, do you open all the links received by email or in Social networks?
   B. Do you certify the origin of an email or an invitation received in the social networks?
5. Are you aware of the necessity of software updates in your devices?
   A. Do you update all the software in your devices, frequently?
   B. Do you use devices with older versions of discontinued software?
6. Do you know all the risks associated to a Wi-Fi access?
   A. Do you use public Wi-Fi, in particular when it grants free access without any concerns?
   B. In order to achieve full Wi-Fi access do you use software that allows sharing access to several public Wi-Fi networks ?
   C. Do you only access important services (i.e., Banks and Email) when the connection is secure?

The main question (numerical marked) have the following replying options: R1 – no knowledge; R2- some knowledge; R3- enough knowledge; R4- good knowledge; R5- great knowledge.

5. Results

For a Universe of 78 answers the following results are detailed over several tables. The options R2 and R3 were grouped in pairs aiming to minimize eventual problems in the semantic understanding of the question. The same was made for R4 and R5. In this way, the results will be presented analyzing three levels of knowledge namely R1 state for" no knowledge", R2 for "some knowledge" and R3 for "good knowledge".

Table 1 – Table for question 1.

Q1		Q1A		Q1B		Q1C	
	Total (%)	Yes (%)	No (%)	Yes (%)	No (%)	Yes (%)	No (%)
R1	10,3	50,0	50,0	0,0	100,0	25,0	75,0
R2	73,1	82,5	17,5	52,6	47,4	80,7	19,3
R3	16,7	53,8	46,2	84,6	15,4	92,3	7,7

Comments on Table 1: When there is no literacy the enquired is not an active searcher for information. As soon as it shows more literacy its proactivity increases for more knowledge.

Table 2 – Table for question 2.

Q2		Q2A		Q2B		Q2C		Q2D		Q2E	
	Total (%)	Yes (%)	No (%)	Yes (%)	No (%)	Yes (%)	No (%)	Yes (%)	No (%)	Yes (%)	No (%)
R1	9,0	85,7	14,3	0,0	100,0	28,6	71,4	100,0	0,0	71,4	28,6
R2	61,5	83,3	16,7	2,1	97,9	37,5	62,5	87,5	12,5	56,3	43,8
R3	29,5	95,7	4,3	0,0	100,0	47,8	52,2	73,9	26,1	21,7	78,3

Comments on Table 2: As the literacy increases it promotes an increase in the password aging and in promiscuous credentials sharing. It is perceived that is a general perception about the secure methodologies.

Table 3 – Table for question 3.

Q3		Q3A		Q3B	
	Total (%)	Yes (%)	No (%)	Yes (%)	No (%)
R1	33,3	0,0	100,0	11,5	88,5
R2	43,6	8,8	91,2	17,6	82,4
R3	23,1	0,0	100,0	16,7	83,3

Comments on Table 3: There is a typical responsible behavior, even without literacy.

Table 4 – Table for question 4.

Q4		Q4A		Q4B	
	Total (%)	Yes (%)	No (%)	Yes (%)	No (%)
R1	51,3	5,0	95,0	70,0	30,0
R2	41,0	6,3	93,8	93,8	6,3
R3	7,7	0,0	100,0	100,0	0,0

Comments on Table 4: there is a distrust even without literacy. Subjective behaviors even without knowledge.

Table 5 – Table for question 5.

Q5		Q5A		Q5B	
	Total (%)	Yes (%)	No (%)	Yes (%)	No (%)
R1	5,1	100,0	0,0	25,0	75,0
R2	71,8	89,3	10,7	21,4	78,6
R3	23,1	88,9	11,1	22,2	77,8

Comments on Table 5: there is a strong knowledge about the topic.

Table 6 – Table for question 6.

Q6		Q6A		Q6B		Q6C	
	Total (%)	Yes (%)	No (%)	Yes (%)	No (%)	Yes (%)	No (%)
R1	9,0	85,7	14,3	0,0	100,0	28,6	71,4
R2	61,5	83,3	16,7	2,1	97,9	37,5	62,5
R3	29,5	95,7	4,3	0,0	100,0	47,8	52,2

Comments on Table 6: a strong believe in the security of private networks. More special attention to personal data transit then Internet browsing.

Final comments: the dimension of the sample disabled the possibility of other statistical tools rather a detailed semantic analysis.

6. Conclusions

The REP solutions are increasing, as described in previous sections, by the several pressures: 2022 energy crisis, environment concerns and worldwide legislation push.

The REP are moving towards solutions fully supported by IT trends solutions such as cloud solutions, AI and many others. The full convexity to Internet is upscaling a panoply of new security challenges.

The enquiry promoted some answers to the overall awareness of Engineering students for the cybersecurity problem. It is clear that there is no adequate literacy, only some care in terms of security behavior aimed by general information sources such as regular press and focused on personal safety.

The University plays a relevant role in upgrading the curricula for the new era challenges introducing the cybersecurity issue to the academic schedule in a professional approach.

References

[1] S. H. Ahmed, N. Razzaq, Z. Malik, U. Qadeer, I. Sarfraz and A. Sharif, "Design & fabrication of MATLAB based solar powered CNC machine," *2017 3rd IEEE International Conference on Control Science and Systems Engineering (ICCSSE)*, 2017.

[2] Z. Chen, Q. Liu, X. Xiao, N. Liu and X. Yan, "Integrated mode and key issues of renewable energy sources and electric vehicles' charging and discharging facilities in microgrid," *2nd IET Renewable Power Generation Conference (RPG 2013)*, 2013.

[3] D. Mooney, B. Kroposki and W. Kramer, "Renewable and efficiency systems integration at the National Renewable Energy Laboratory," *2011 IEEE Power and Energy Society General Meeting,* 2011.

[4] J. Bai, J. Wang, Y. Huang, Y. Li and S. Zhang, "A Renewable Energy Capacity Allocation Planning Method Considering the Balance of Renewable Energy Accommodation and System Investment Costs," *2021 China International Conference on Electricity Distribution (CICED),* 2021.

[5] Y. Li, H. Liu, Y. Chi, Y. Fan, X. Li, F. Cheng, Z. Wang, C. Wei and L. Xie, "Fault Ride-through Demand of Large-scale Islanded Renewable Energy Connected to VSC-HVDC System and Its Key Technologies," *2020 4th International Conference on HVDC (HVDC),* 2020.

[6] J. Valencia-Calvo, G. Olivar-Tost and M. García-Ortega, "Model and Simulation of a Renewable Energy Market: Integration of Renewable Energy Sources with the Conventional Generation System," *2020 15th Iberian Conference on Information Systems and Technologies (CISTI),* 2020.

[7] F. AYADI, I. COLAK, I. GARIP and H. I. BULBUL, "Targets of Countries in Renewable Energy," *2020 9th International Conference on Renewable Energy Research and Application (ICRERA),* 2020.

[8] L. Yan, C. Yongning, T. Haiyan, T. Xinshou, Z. Zhankui and J. Jianqing, "Common Focus and New Requirement on Technical Standards of Renewable Energy Grid Integration," *2019 Chinese Automation Congress (CAC),* 2019.

[9] W. Feng, B. Yanhong, R. Jingjing, R. Xiancheng, L. Shaofeng and T. Wang, "Study on Online Recognition Method of Renewable Energy Cascading Tripping Evaluation Based on Machine Learning," *2019 4th International Conference on Power and Renewable Energy (ICPRE),* 2019.

[10] B. Kroposki, D. Mooney, T. Markel and B. Lundstrom, "Energy systems integration facilities at the national renewable energy laboratory," *2012 IEEE Energytech,* 2012.

[11] M. Riasetiawan, F. Anggara, A. Ashari, S. Winardi and B. N. Prastowo, "Data Model and Analysis for Big Data Mapping and Management in the Energy Data Platform," *2021 International Conference on Data Science, Artificial Intelligence, and Business Analytics (DATABIA),* 2021.

[12] H. He, T. Haibo, Q. Hui, F. Wei and D. Xiaofeng, "Optimization of Renewable Energy Big Data Transactions Based on Vector Evaluated Genetic Algorithm," *2018 China International Conference on Electricity Distribution (CICED),* 2018.

[13] J. Wu, S. Guo, J. Li and D. Zeng, "Big Data Meet Green Challenges: Big Data Toward Green Applications," *IEEE Systems Journal,* vol. 10, 2016.

[14] A. C. Şerban and M. D. Lytras, "Artificial Intelligence for Smart Renewable Energy Sector in Europe—Smart Energy Infrastructures for Next Generation Smart Cities," *IEEE Access,* vol. 8, 2020.

[15] S. E. Haupt, T. C. McCandless, J. C. Lee, B. Kosović, S. Alessandrini, S. Dettling, T. Hussain and M. Al-Rasheedi, "Combining Physical Modeling with Artificial Intelligence for Solar Power Forecasting," *2020 47th IEEE Photovoltaic Specialists Conference (PVSC),* 2020.

[16] V. Puri, S. Jha, R. Kumar, I. Priyadarshini, L. H. Son, M. Abdel-Basset, M. Elhoseny and H. V. Long, "A Hybrid Artificial Intelligence and Internet of Things Model for Generation of Renewable Resource of Energy," *IEEE Access,* vol. 7, 2019.

[17] Alankrita and S. K. Srivastava, "Application of Artificial Intelligence in Renewable Energy," *2020 International Conference on Computational Performance Evaluation (ComPE),* 2020.

[18] W. Feng, B. Yanhong, R. Jingjing, R. Xiancheng, L. Shaofeng and T. Wang, "Study on Online Recognition Method of Renewable Energy Cascading Tripping Evaluation Based on Machine Learning," *2019 4th International Conference on Power and Renewable Energy (ICPRE),* 2019.

[19] D. K. Aagri and A. Bisht, "Export and Import of Renewable energy by Hybrid MicroGrid via IoT," *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU),* 2018.

[20] C.-S. Choi, J.-D. Jeong, I.-W. Lee and W.-K. Park, "LoRa based renewable energy monitoring system with open IoT platform," *2018 International Conference on Electronics, Information, and Communication (ICEIC),* 2018.

[21] C.-H. Shin, S. Lee, J. Kim, H.-s. Nam and Y. K. Jeong, "A Study on the Implementation of Economic Zero Energy Building according to Korea's Renewable Energy Support Policies and Energy Consumption Patterns," *2018 International Conference on Information and Communication Technology Convergence (ICTC),* 2018.

[22] H. A. Illias, N. S. Ishak, H. Mokhlis and M. Z. Hossain, "IoT-based Hybrid Renewable Energy Harvesting System from Water Flow," *2020 IEEE International Conference on Power and Energy (PECon),* 2020.

[23] S. N. Altun, M. Dörterler and I. A. Dogru, "Fuzzy Logic Based Lighting System Supported with IoT for Renewable Energy Resources," *2018 Innovations in Intelligent Systems and Applications Conference (ASYU),* 2018.

[24] A. F. Rodrigues, B. M. Monteiro and I. Pedrosa, "Cybersecurity risks : A behavioural approach through the influence of media and information literacy," *2021 16th Iberian Conference on Information Systems and Technologies (CISTI),* 2021.

[25] N. Holton and S. Furnell, "Assessing the provision of public-facing cybersecurity guidance for end-users," *2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC),* 2020.

[26] I. Hameed and S. A. A. Naqvi, "An Analysis of the factors affecting Cybercrime against individuals in Pakistan," *2021 15th International Conference on Open Source Systems and Technologies (ICOSST),* 2021.

[27] P. K. Jagalur, P. L. Levin, K. Brittain, M. Dubinsky, K. Landau-Jagalur and C. Lathrop, "Cybersecurity for Civil Society," *2018 IEEE International Symposium on Technology and Society (ISTAS),* 2018.

[28] E. Troja, J. E. DeBello and N. Roman, "Teaching Efficient Computer Science and Cybersecurity Courses Amidst the COVID-19 Pandemic," *2021 IEEE Global Engineering Education Conference (EDUCON),* 2021.

[29] A. Aldea, E. Vaicekauskaitė, M. Daneva and J. P. S. Piest, "Enterprise Architecture Resilience by Design: A Method and Case Study Demonstration," *2021 IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW),* 2021.

[30] T. Weil and S. Murugesan, "IT Risk and Resilience—Cybersecurity Response to COVID-19," *IT Professional* , vol. 22, pp. 4-10, 2020.

[31] M. Misbahuddin, B. S. Bindhumadhava and B. Dheeptha, "Design of a risk based authentication system using machine learning techniques," *2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI),* 2017.

[32] N. Djosic, B. Nokovic and S. Sharieh, "Machine Learning in Action: Securing IAM API by Risk Authentication Decision Engine," *2020 IEEE Conference on Communications and Network Security (CNS),* 2020.

[33] A. Waheed, M. A. Shah and A. Khan, "Secure login protocols: An analysis on modern attacks and solutions," *2016 22nd International Conference on Automation and Computing (ICAC),* 2016.

[34] B. N. Biswas, S. D. Bhitkar and S. N. Pundkar, "Secure Login: A Blockchain based web application for Identity Access Management System," *2021 2nd International Conference for Emerging Technology (INCET),* 2021.

[35] T. Nathezhtha, D. Sangeetha and V. Vaidehi, "WC-PAD: Web Crawling based Phishing Attack Detection," *2019 International Carnahan Conference on Security Technology (ICCST),* 2019.

[36] M. Higashino, T. Kawato, M. Ohmori and T. Kawamura, "An Anti-phishing Training System for Security Awareness and Education Considering Prevention of Information Leakage," *2019 5th International Conference on Information Management (ICIM),* 2019.

[37] S. P. Ripa, F. Islam and M. Arifuzzaman, "The Emergence Threat of Phishing Attack and The Detection Techniques Using Machine Learning Models," *2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI),* 2021.

[38] M. A. Ayub, A. Continella and A. Siraj, "An I/O Request Packet (IRP) Driven Effective Ransomware Detection Scheme using Artificial Neural Network," *2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI),* 2020.

[39] R. Agrawal, J. W. Stokes, K. Selvaraj and M. Marinescu, "Attention in Recurrent Neural Networks for Ransomware Detection," *ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP),* 2019.

[40] A. Alzahrani, H. Alshahrani, A. Alshehri and H. Fu, "An Intelligent Behavior-Based Ransomware Detection System For Android Platform," *2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA),* 2019.

[41] E. Iannone, R. Guadagni, F. Ferrucci, A. D. Lucia and F. Palomba, "The Secret Life of Software Vulnerabilities: A Large-Scale Empirical Study," *IEEE Transactions on Software Engineering,* 2022 .

[42] P. K. Shamal, K. Rahamathulla and A. Akbar, "A study on software vulnerability prediction model," *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET),* 2017.

[43] N. Visalli, L. Deng, A. Al-Suwaida, Z. Brown, M. Joshi and B. Wei, "Towards Automated Security Vulnerability and Software Defect Localization," *2019 IEEE 17th International Conference on Software Engineering Research, Management and Applications (SERA),* 2019.

[44] A. Ghosh, T. O'Connor and G. McGraw, "An automated approach for identifying potential vulnerabilities in software," *Proceedings. 1998 IEEE Symposium on Security and Privacy (Cat. No.98CB36186),* 1998 .

[45] J. D. Pereira, "Techniques and Tools for Advanced Software Vulnerability Detection," *2020 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW),* 2020.

[46] B. Peerzada and D. Kumar, "Analyzing Software Vulnerabilities Using Machine Learning," *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO),* 2021 .

[47] E. Baray and N. K. Ojha, "WLAN Security Protocols and WPA3 Security Approach Measurement Through Aircrack-ng Technique'," *2021 5th International Conference on Computing Methodologies and Communication (ICCMC),* 2021.

[48] H. M. Furqan, M. S. J. Solaija, H. Türkmen and H. Arslan, "Wireless Communication, Sensing, and REM: A Security Perspective," *IEEE Open Journal of the Communications Society,* vol. 2, 2021.

[49] A. Abdelrahman, H. Khaled, E. Shaaban and W. S. Elkilani, "Detailed Study of WLAN PSK Cracking Implementation," *2020 15th International Conference on Computer Engineering and Systems (ICCES),* 2020.

[50] L. Zhang, L. Yan, B. Lin, H. Ding, Y. Fang and X. Fang, "Augmenting Transmission Environments for Better Communications: Tunable Reflector Assisted MmWave WLANs," *IEEE Transactions on Vehicular Technology,* Vols. 69,, 2020.

[51] E. B. Hreinsson, "The renewable energy resources of Iceland and their extended future utilization," *2009 44th*

International Universities Power Engineering Conference (UPEC), 2009.

[52] E. B. Hreinsson, "Accumulation of a resource fund for Iceland's renewable energy resources," *2015 50th International Universities Power Engineering Conference (UPEC),* 2015 .

[53] E. Shafiei, B. Davidsdottir, J. Leaver, H. Stefansson and E. I. Asgeirsson, "Economic impact of adaptation to climate change in Iceland's energy supply sector," *2015 12th International Conference on the European Energy Market (EEM),* 2015 .

[54] E. B. Hreinsson, "Harvesting the Benefits of Iceland's Energy Resources," *2019 54th International Universities Power Engineering Conference (UPEC),* 2019.

[55] E. B. Hreinsson, "Environmental, technical, economics and policy issues of the master plan for the renewable hydro and geothermal energy resources in Iceland," *2007 42nd International Universities Power Engineering Conference,* 2007 .

[56] W.-Y. Chang, B.-Y. Hsu and J.-W. Hsu, "Real-Time Collision Avoidance for Five-Axis CNC Machine Tool Based on Cyber-Physical System," *2018 IEEE International Conference on Advanced Manufacturing (ICAM),* 2018.

[57] Y. Li, Q. Liu, J. Xiong and J. Wang, "Research on data-sharing and intelligent CNC machining system," *2015 IEEE International Conference on Mechatronics and Automation (ICMA),* 2015.

[58] H. Yu, D. Yu, Y. Hu and C. Wang, "Research on CNC Machine Tool Monitoring System Based on OPC UA," *2019 Chinese Control And Decision Conference (CCDC),* 2019.

[59] K. A. Masalimov, "A Machine Learning based Approach to Autogenerate Diagnostic Models for CNC machines," *2020 35th IEEE/ACM International Conference on Automated Software Engineering (ASE),* 2020.

[60] L. Martinova, A. Obukhov and S. Sokolov, "Practical Aspects of Ensuring Accuracy of Machining on CNC Machine Tools within Framework of “Smart Manufacturing”," *2020 International Russian Automation Conference (RusAutoCon),* 2020.

[61] Y. Yong and W. Shan, "Distributed Intelligent Maintenance System for CNC Machine Tools Based on Kansei Engineering," *2009 International Conference on Artificial Intelligence and Computational Intelligence,* vol. 4, 2009.

[62] S. Sandhya and K. S. Devi, "Contention for Man-in-the-Middle Attacks in Bluetooth Networks," *2012 Fourth International Conference on Computational Intelligence and Communication Networks,* 2012 |.

[63] J. Huang, Y. Wang, H. Wang, Z. Li and J. Huang, "Man-in-the-middle attack on BB84 protocol and its defence," *2009 2nd IEEE International Conference on Computer Science and Information Technology,* 2009.

[64] R. Joshi, A. K. Bairwa, V. Soni and S. Joshi, "Data Security Using Multiple Image Steganography and Hybrid Data Encryption Techniques," *2022 International Conference for Advancement in Technology (ICONAT),* 2022.