INDUSTRIAL INTERNET OF THINGS (IIOT) - SECURITY WEAKNESSES AND MOST COMMON TYPES OF ATTACKS – A SYSTEMATIC LITERATURE REVIEW

Vladimir Fabri[1] [ORCID 0000-0002-6218-7240], *Miroslav Stefanović*[1] [ORCID 0000-0002-0767-365X],
Đorđe Pržulj[1] [ORCID 0000-0001-5951-563X], *Teodora Vučković*[1] [ORCID 0000-0001-5522-6558],
Rogerio Dionisio[2] [ORCID 0000-0002-6810-2447]
[1]*Faculty of technical sciences, Department of Industrial Systems and Management, Novi Sad*
[2]*Instituto Politécnico de Castelo Branco: Castelo Branco, PT*

Abstract: *In recent years there has been a growing interest in the Industrial Internet of Things (IIoT) coming from business and scientific communities alike. One of the elementary concepts of the proposed Industry 4.0 is the IIoT which proposes the implementation of the regular Internet of Things (IoT) concept on a much larger scale within the industrial facilities, thus interconnecting devices in industrial settings. While the main focus of the scientific community is on the cost/benefit analysis and practical application of the mentioned concept, one often overlooked aspect is its security. The following paper presents a comprehensive systematic literature review for the Industrial Internet of Things security. It contains a review of the most common types of attacks committed within the Industrial Internet of Things and a consequential analysis of the weaknesses those attacks exposed*.

Key words: Industrial Internet of Things, IIoT, security, systematic literature review, SLR, secondary research, Internet of things, IoT

1. INTRODUCTION

In the not-too-distant past, most people would never have thought that by pressing a few buttons on their smartphone, they could command their household appliances to do their work without any human intervention. Even more inconvenient was the idea of a factory being run by machines and robots with absolutely minimal human oversight and control. This would, of course, as we know, change with the advent of one of the most important technologies to date, the Internet.

The meteoric rise of the internet at the turn of this century has led to the creation of new ways of communication, thinking, collaboration, connection, work, and generally - living. Consequentially, new opportunities and obstacles have appeared in our lives and workplaces. Furthermore, some of these opportunities would present themselves in places for which the Internet was not intentionally developed. For example, the Internet enables governments to provide crucial services for its citizens - e-government (Stefanović, 2021), the Internet allows educational institutions to share and teach academic subjects via the concept known as e-learning (Stefanović, 2020). Yet, in the context of industrial systems and manufacturing, new concepts have begun to emerge and gain momentum in the academic literature (Spasojević, 2021), these being the Internet of Things (IoT) and Industry 4.0.

The IoT is considered the next dawn of technology after the innovation that was the Internet. The IoT term was suggested, for the first time, by Kevin Ashton in 1999, it refers to a network within which information from all connected devices can be gathered, processed, and modified to offer new services (Litoussi, 2020).

The Internet of Things enables a large-scale of technological innovations and value-added services that personalize users' interactions with various "things" (Čolaković, 2018).

Yet the IoT does not come without flaws. Whereas IoT technologies bring convenience to people's lives, some security concerns also appear. Security is of the highest priority when enterprises consider deploying IoT systems, and most of them temporarily shelve their plans to deploy IoT because of these security concerns, which hinderd the rising trend of IoT and which have greatly affected the popularization and development of IoT. (Ma, 2022).

The Industrial Internet of Things (IIoT) refers to the use of smart sensors, actuators, fast communication protocols, and efficient cybersecurity mechanisms to improve industrial processes and applications (Latif, 2021).

Even though IIoT represents the implementation of IoT within industrial facilities, there are considerable differences between the two as stated by Martin Serror (Serror, 2021), these include criticality, number of devices, lifetime of devices, hardware complexity, data volume, data periodicity, etc.

These fundamental differences alongside specific requirements of IIoT, for example, a need for constant availability and data integrity (Serror, 2021) make attacks against these systems highly consequential and potentially devastating.

Thus, the development of large-scale IIoT systems faces various security challenges, which result in many large-scale cyberattacks, including fraudulent transactions or damage to critical infrastructure (Pal, 2021).

This paper represents secondary research conducted over the currently available reviews which regard the security within IIoT, with the main focus being frequency and the types of attacks that are conducted against systems that implement the aforementioned concept of IIoT. The main goal of this paper is to provide a high-level overview of the current representation of the attack types previously mentioned and security risks within IIoT in the literature.

This paper was written in accordance with Kitchenham's (Kitchenham, 2007) guidelines for conducting a systematic literature review.

The reviewed papers that were used for the writing of this systematic literature review provided information on various attack types, IIoT architecture weaknesses, potential countermeasures, etc. Yet, no paper was found that exclusively focused on providing the researchers with a high-level statistical overview of the appearance frequency and research intensity of these attacks, within the available literature. Thus no paper presents the researchers with the ability to immediately grasp which types of attacks are the main focus of the available literature in the field of IIoT.

The study is organized as follows. Section 2 contains a detailed methodology which was conducted for the purpose of creating this paper; Section 3 discusses the data collected during the conduction of the process of Systematic literature review. Finally, Section 4 presents the author's final thoughts and conclusion.

2. METHODOLOGY

Systematic literature review method proposed by B. Kitchenham (Kitchenham, 2007) can be summarized into three main phases: Planning the Review, Conducting the Review, and Reporting the Review. The literature review is focused on a set of research questions, as well as the inclusion and exclusion criteria.

2.1. Planning the review

In the planning phase of the literature review, it is necessary to identify the needs for the review itself. The need for a systematic literature review can be established by reviewing existing literature reviews in that research area, following the guidelines proposed by Kitchenham (Kitchenham, 2007). During the planning phase several reviews on the subject of IIoT security have been discovered, and yet none of them dealt with the subject of quantifying and analyzing the frequency of occurrences of the various types of attacks within the literature itself. For this reason, this crucial and disregarded aspect represents the motive for writing this paper.

According to the aim and the research framework, the authors propose the following three research questions:

RQ1: Which types of attacks are mentioned in the literature reviews regarding IIoT security?
RQ2: Which types of attacks are most prevalent in the literature?
RQ3: Which part of the IIoT architecture is most susceptible to attacks according to the existing literature?

For this literature review, the following databases were searched:

- Scopus
- Web of science

Scopus uniquely combines a comprehensive, expertly curated abstract and citation database with enriched data and linked scholarly literature across a wide variety of disciplines (Elsevier, Accessed 21 July 2023). The Web of Science (WoS) database is a selective citation index of scientific and scholarly publishing covering journals, proceedings, books, and data compilations. It is the oldest citation index for the sciences, having been introduced commercially by the ISI in 1964 (Birkle, 2020).

Search terms defined for search in these databases are presented below:

("Industrial internet of things" OR "IIoT" OR "Industrial IoT") AND ("Security" OR "Securing" OR "Safety") AND ("Challenges" OR "Opportunities") AND Language = "English" AND Doctype = "re"

The inclusion criteria defined for this review are:

IC1: The paper must contain a mention and/or detailed explanation of the types of attacks that occur in the context of IIoT.

IC2: Papers that contain explanations of architectural framework or layers of IIoT alongside their security downsides are to be included.

IC3: The publications must be published in the previous six years.

The exclusion criteria defined for the review are:

EC1: If the paper mentions security risks, concerns or attacks only in the context of IoT without any kind of practical translation or reference to the IIoT.

EC2: If the paper is not open access, it should be removed.

EC3: Duplicate papers found in different databases should be removed.

For each paper, the following features will be extracted to answer the research questions:

1. Publication year;
2. Mentioned/referenced/explained the type of attack;
3. Corresponding architectural layers which are targeted by the mentioned attacks;

2.2. Conducting and reporting the review

The reviews that met the inclusion and exclusion criteria in the literature review phase are presented in Table 1.

Table 1: Results of the exclusion and inclusion process

Resource	Initial search results	Number of duplicates removed	Results after removal of non-open access papers	Final selection results
Scopus	30	/	23	8
Web of science	49	16	12	5

The previous chapter defined the inclusion and exclusion criteria, as well as the database search string. After applying the previously defined sequence, a total of 79 results were obtained. Of those 30 were obtained from Scopus and 49 were obtained from Web of Science. To implement exclusion criteria 3 Scopus was selected as a reference database when determining duplicates, in other words, all of the obtained research papers from Scopus were considered unique and the papers found and obtained on Web of Science were considered duplicated. Consequently, 16 duplicates were found and removed. Following this, the exclusion criteria 2 was applied on the remaining papers, resulting in 23 open-access reviews from Scopus and 12 from Web of Science. Furthermore, inclusion criteria 1 and 2, along with exclusion criteria 1 were implemented by reviewing the title, abstract, and content of remaining works, which resulted in the final selection of results regarding the 8 reviews obtained from Scopus and 5 reviews from the Web of Science.

2.3. Data extraction and compression

Using data extraction, the studies selected in the previous stages of a systematic review of the literature were summarized and then presented in the next section. The tables and graphs provide a visual representation of the papers which were selected based on the criteria for data extraction. The bracketed numbers in the tables reference corresponding literature as follows: [1] (Abosata, 2021), [2] (Astorga, 2022.), [5] (Dhirani, 2021.), [7] (Fun, 2021), [8] (Jayalaxmi, 2021), [11] (Latif, 2021), [13] (Ma, 2022.), [14] (Mansour, 2023.), [15] (Mirani, 2022.), [16] (Pal, 2021.), [17] (Prinsloo, 2019), [18] (Raimundo, 2022.), [19](Sengupta, 2020.). As shown in Table 2, the most common types of attacks appearing in the literature are Denial of Service (DoS) attacks and their advanced version – Distributed Denial of Service (DDoS), appearing in some form in roughly 77% of reviews.

Table 2: Display of attacks and percentage of reviews in which they appear

Type of the attack	Review in which attack is mentioned/explained	%
Attack on industrial devices	[5],[14],[16],[19]	30
Jamming	[1],[7],[16],[19]	30
Injection attack	[1],[5],[7],[15],[17],[19]	46
Node capture attack	[1],[8]	15
Sleep deprivation attack	[1],[19]	15
Roughly defined network attack	[2],[8],[13],[15]	30
Blackhole	[1], [16]	15
Wormhole	[1], [8], [16], [19]	30
Sinkhole	[1], [16],[19]	23
Sybil attack	[1],[7],[16],[19]	30
Pharming attack	[7], [16]	15
Routing attack	[19]	7
Man in the middle attack	[1], [7], [8], [15] , [16], [19]	46
Eavesdropping	[1], [5], [8], [14], [15],[16], [17]	54
Dos/DDoS	[1], [5], [7], [8], [11], [14],[15] , [17], [18], [19]	77
Selective forwarding attack	[1], [19]	15
SYN	[7], [16]	15
Replay attack	[1],[8],[17],[19]	30
Spoofing	[5],[7],[14],[16],[19]	38
Data theft and breaches	[5],[7], [11],[13] ,[19]	38
Data distortion/inconsistency attack	[1],[5],[19]	23
Attacks targeted against ICS	[1],[5],[8], [15] ,[18],[19]	46
Malware attacks	[1],[5],[8], [11] ,[15] ,[17],[19]	54
Phishing attacks	[5],[7],[8],[16],[17]	38
Modern botnets	[14]	7
Advanced persistent threat	[7], [15]	15
Outdated devices	[5],[8],[13],[19]	30
Attacks by malicious insiders	[17]	7

According to Abosata (Abosata, 2021) and Pal (Pal, 2021) the IIoT's system architecture can be divided into 4 layers: The Perception layer, The Network layer, The Processing or Support layer, and The Application layer. Additionally, attack types from table 2 can be sorted by the layer which is ussually their main target. Thus rows starting at attack on industrial devices all the way to the sleep deprivation attack can be classified as attacks targeted against perception layer, network layer attacks include rows from roughly defined network attacks to spoofing. Data theft and breaches, data distortion attacks and ICS attacks ussually target support layer while malware attacks, phishing attacks and modern botnets target application layer. Based on this division, the types of attacks mentioned in Table 2 were sorted into the appropriate layers as shown in Table 3. Some of the attacks from Table 2 can't be exclusively placed into one of the four mentioned layers due to their complex nature, these include:

- Advanced persistent threat – this represents the threats from individuals or organizations affiliated with organized cybercrimes;

- Outdated devices – while not being representative of the type of attack *per se*, outdated devices can be considered a security concern that could present themselves as an ideal entry point for future attacks and a severe security weakness;
- Attacks by malicious insiders – Due to their unhindered access and knowledge of the system, these individuals can cause severe damage that would otherwise be impossible or less severe if the individuals were conducting the same attack from the outside of the system;

These 3 special types were sorted into “Other security threats” in Table 3.

Table 3: Percentage of reviews which mention attacks that happen on corresponding architectural layers

Architectural layer	Review	%
Perception layer	[1],[5],[7],[8], [15] ,[16],[17],[19]	62
Network layer	[1],[2],[5],[7],[8], [11], [13], [14] ,[15] ,[16],[17],[18],[19]	100
Support layer	[1],[5],[7],[8], [11], [13], [15] ,[18],[19]	69
Application layer	[1],[5],[7],[8], [11], [15] ,[16],[17],[19]	69
Other security threats	[5],[7],[8], [13] ,[15] ,[17],[19]	54

As shown by Table 3, 100% of reviews mention or explain the attacks which happen on the Network layer, while only 62% of reviews deal with attacks that are related to the Perception layer. Table 4 shows the publication year of the researched reviews. Most of the reviews- 6, were published during 2021, followed by five publications in 2022.

Table 4: Publication year of reviews

Publication year	Review
2023	[14]
2022	[2],[13],[15],[18]
2021	[1,[5],[7],[8],[11],[16]
2020	[19]
2019	[17]

A combination of data from Tables 3 and 4 is presented in Figure 1. Figure 1 shows the publication year of the review and the number of reviews that mention or explain the types of attacks belonging to one of the corresponding architectural layers. As Table 3 shows, all reviews mention attacks that correspond to the Network layer. Figure 1 clearly presents this reality by showing that all reviews used for the purpose of writing this paper mentioned the Network layer, in other words, attacks corresponding to the Network layer were mentioned in reviews published from 2019 to 2023.

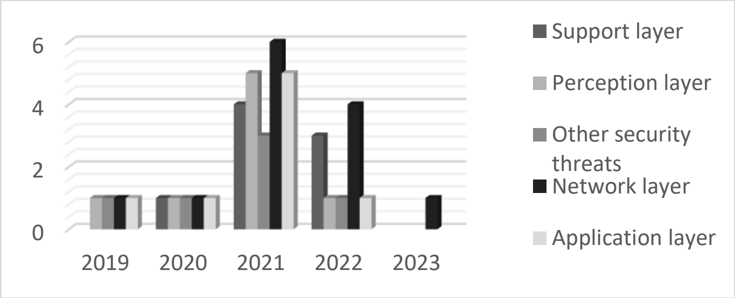

Figure 1: Distribution of reviews mentioning attacks within shown layers over five years

3. DISCUSSION

In this section, the obtained results of a systematic review of the literature will be presented and analyzed. The mentioned types of attacks in reviewed literature are presented in Table 2. By examining the results shown in Table 2, it can be deduced that 25 distinct types of attacks emerge in the reviewed literature. After adjusting the taxonomy model provided by Kaur (Kaur, 2023) these attacks can be sorted into groups based on their working mechanisms, the layers they target or the general concept that they are based on. Consequently, following groups emerge Physical attacks, Node attacks, Flooding attacks, Eavesdropping attacks, Spoofing attacks, and Data attacks.

The most prevalent types of attacks recorded in reviewed literature are Denial of Service (DoS) and Distributed Denial of Service (DDoS), appearing in a total of 77% of all reviewed literature. When combined with SYN and Selective forwarding attacks they constitute a group called the Flooding attacks which are described in detail by Pal (Pal, 2021), these types of attacks appear in 85% of all reviewed literature. Potential reason why this is so is because the majority of devices, when damaged, are unable to provide their intended services and essentially this is what DoS represents. With the majority of attacks causing some sort of a damage on the hardware or the software of the device it is plausible that DoS also represents a consequence of the other types of attacks thus inflating its occurrences within various reviews.

Based on the data shown in Table 3 and Figure 1, it can be concluded that all reviewed literature more or fewer deals with attacks that are related to the Network layer, thus it can be argued that the Network layer of IIoT architecture is the one that is most susceptible to attacks.

According to these insights several plausible conclusions can be assumed, these conclusions are listed as follows:

1. DoS and DDoS attacks are the most common occurring types of attacks in the context of IIoT systems.
2. DoS, DDoS and generally Flooding attacks are the most researched and mentioned group of attacks in the reviewed literature.
3. Previously mentioned attacks are given highest priority and attention in research circles regarding the subject of IIoT security. Potentially, these kinds of attacks are best understood and researched.
4. Overall, attacks which correspond to the Network layer are most commonly occurring attacks and the Network layer itself presents the most common target for malicious attacks.
5. Due to the previous statement, majority of attacks targeted against IIoT systems have the goal of causing industrial damage, system stoppage and sabotage, because the attacks against Internet layer prevent functional and adequate communication between industrial devices, thus causing miscommunication and reduction of system availability and responsiveness.
6. Less common goals of attacks against IIoT systems appear to be data theft and data distortion as advocated by the fact that Support and Application layers are next in line as the most common targets in IIoT architecture. Consequently, attackers are potentially seeking to conduct industrial espionage or pave the way for attacks against the Internet or Perception layers.
7. Attacks against the Perception layer seem to be least frequent. Possible reasons for this might include the fact that conducting attacks against perception layer usually requires attacker's physical presence near the industrial devices.

4. CONCLUSION

Based on the results presented in sections 2 and 3, the following conclusions are proposed:

The most frequently mentioned group of attacks within the reviewed literature are the Flooding attacks, specifically DoS/DDoS attacks. This group is closely followed by Eavesdropping, Man-in-the-Middle, and Malware attacks. If the propensity for attacks was determined only based on how many times a certain attack corresponding to a certain layer was mentioned in the literature, we could say that the Internet layer is the one that is most prone to attacks followed, in equal measure, by Support and Application layers.

In response to RQ1, it can be concluded that 25 distinct types of attacks were identified in the reviewed literature.

In response to RQ2, it can be concluded that the most prevalent types of attacks recorded in reviewed literature are Denial of Service (DoS) and Distributed Denial of Service (DdoS).

In response to RQ3, it can be concluded that all reviewed literature more or less deals with attacks that are related to the Network layer, thus it can be argued that the Network layer of IIoT architecture is the one that is most susceptible to attacks.

As the industrial production paradigm slowly begins to shift, enterprises will likely seek to gain competitive advantage over their commercial rivals by accommodating newly emerging concepts of Industry 4.0. One of the potential cornerstone's of this implementation will be IIoT, the success of its implementation might highly depend on utilization of its strengths and elimination of its weaknesses, amongst which security is a major one.

To successfully navigate this process, enterprises will have to rely on academia and scientific community for insights, theoretical and practical solutions to the issues present in IIoT. Consequently, researchers themselves will have to rely on existing literature to grasp the extent of current research on the subject.

Thus, the goal of this Systematic Literature Review was to give researchers a concise high-level overview of the literary coverage of various types of attacks within the IIoT.

Based on the publication years of reviewed literature, it can be argued that research in the area of IIoT security is still in its nascent stages and further research is encouraged.

5. REFERENCES

Abosata, N., Al-Rubaye, S., Inalhan, G., & Emmanouilidis, C. (2021). Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications. In *Sensors* (Vol. 21, Issue 11). MDPI AG. https://doi.org/10.3390/s21113654

Astorga, J., Barcelo, M., Urbieta, A., & Jacob, E. (2022). Revisiting the Feasibility of Public Key Cryptography in Light of IIoT Communications. In *Sensors* (Vol. 22, Issue 7). MDPI. https://doi.org/10.3390/s22072561

Birkle, C., Pendlebury, D. A., Schnell, J., & Adams, J. (2020). Web of science as a data source for research on scientific and scholarly activity. *Quantitative Science Studies*, *1*(1), 363–376. https://doi.org/10.1162/qss_a_00018

Čolaković, A., & Hadžialić, M. (2018). Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. In *Computer Networks* (Vol. 144, pp. 17–39). Elsevier B.V. https://doi.org/10.1016/j.comnet.2018.07.017

Dhirani, L. L., Armstrong, E., & Newe, T. (2021). Industrial iot, cyber threats, and standards landscape: Evaluation and roadmap. In *Sensors* (Vol. 21, Issue 11). MDPI AG. https://doi.org/10.3390/s21113901

Elsevier. *About Scopus*. https://www.elsevier.com/solutions/scopus

Fun, T. S., & Samsudin, A. (2021). Recent technologies, security countermeasure and ongoing challenges of industrial internet of things (Iiot): A survey. In *Sensors* (Vol. 21, Issue 19). MDPI. https://doi.org/10.3390/s21196647

Jayalaxmi, P., Saha, R., Kumar, G., Kumar, N., & Kim, T. H. (2021). A Taxonomy of Security Issues in Industrial Internet-of-Things: Scoping Review for Existing Solutions, Future Implications, and Research Challenges. *IEEE Access*, *9*, 25344–25359. https://doi.org/10.1109/ACCESS.2021.3057766

Kaur, B., Dadkhah, S., Shoeleh, F., Neto, E. C. P., Xiong, P., Iqbal, S., Lamontagne, P., Ray, S., & Ghorbani, A. A. (2023). Internet of Things (IoT) security dataset evolution: Challenges and future directions. In *Internet of Things (Netherlands)* (Vol. 22). Elsevier B.V. https://doi.org/10.1016/j.iot.2023.100780

Kitchenham, B. (2007). *Guidelines for performing Systematic Literature Reviews in Software Engineering*.

Latif, S., Driss, M., Boulila, W., Huma, Z. E., Jamal, S. S., Idrees, Z., & Ahmad, J. (2021). Deep learning for the industrial internet of things (Iiot): A comprehensive survey of techniques, implementation frameworks, potential applications, and future directions. In *Sensors* (Vol. 21, Issue 22). MDPI. https://doi.org/10.3390/s21227518

Litoussi, M., Kannouf, N., El Makkaoui, K., Ezzati, A., & Fartitchou, M. (2020). IoT security: Challenges and countermeasures. *Procedia Computer Science*, *177*, 503–508. https://doi.org/10.1016/j.procs.2020.10.069

Ma, J., Shangguan, X., & Zhang, Y. (2022). IoT Security Review: A Case Study of IIoT, IoV, and Smart Home. In *Wireless Communications and Mobile Computing* (Vol. 2022). Hindawi Limited. https://doi.org/10.1155/2022/6360553

Mansour, M., Gamal, A., Ahmed, A. I., Said, L. A., Elbaz, A., Herencsar, N., & Soltan, A. (2023). Internet of Things: A Comprehensive Overview on Protocols, Architectures, Technologies, Simulation Tools, and Future Directions. In *Energies* (Vol. 16, Issue 8). MDPI. https://doi.org/10.3390/en16083465

Mirani, A. A., Velasco-Hernandez, G., Awasthi, A., & Walsh, J. (2022). Key Challenges and Emerging Technologies in Industrial IoT Architectures: A Review. In *Sensors* (Vol. 22, Issue 15). MDPI. https://doi.org/10.3390/s22155836

Pal, S., & Jadidi, Z. (2021). Analysis of security issues and countermeasures for the industrial internet of things. In *Applied Sciences (Switzerland)* (Vol. 11, Issue 20). MDPI. https://doi.org/10.3390/app11209393

Prinsloo, J., Sinha, S., & von Solms, B. (2019). A review of industry 4.0 manufacturing process security risks. In *Applied Sciences (Switzerland)* (Vol. 9, Issue 23). MDPI AG. https://doi.org/10.3390/app9235105

Raimundo, R. J., & Rosário, A. T. (2022). Cybersecurity in the Internet of Things in Industrial Management. In *Applied Sciences (Switzerland)* (Vol. 12, Issue 3). MDPI. https://doi.org/10.3390/app12031598

Sengupta, J., Ruj, S., & Das Bit, S. (2020). A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. In *Journal of Network and Computer Applications* (Vol. 149). Academic Press. https://doi.org/10.1016/j.jnca.2019.102481

Serror, M., Hack, S., Henze, M., Schuba, M., & Wehrle, K. (2021). Challenges and Opportunities in Securing the Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, *17*(5), 2985–2996. https://doi.org/10.1109/TII.2020.3023507

Spasojevic, I., Havzi, S., Stefanovic, D., Ristic, S., & Marjanovic, U. (2021). Research Trends and Topics in IJIEM from 2010 to 2020: A Statistical History. *International Journal of Industrial Engineering and Management*, *12*(4), 228–242. https://doi.org/10.24867/IJIEM-2021-4-290

Stefanovic, D., Milicevic, A., Havzi, S., Lolic, T., & Ivic, A. (2021, March 17). Information Systems Success Models in the E-Government : Context: A Systematic Literature Review. *2021 20th International Symposium INFOTEH-JAHORINA, INFOTEH 2021 - Proceedings*. https://doi.org/10.1109/INFOTEH51037.2021.9400653

Stefanovic, D., Spasojevic, I., Havzi, S., Lolic, T., & Ristic, S. (2020). Information systems success models in the e-learning context: A systematic literature review. *Annals of DAAAM and Proceedings of the International DAAAM Symposium*, *31*(1), 555–564. https://doi.org/10.2507/31st.daaam.proceedings.07