JCS Journal of Comprehensive Science
JOURNAL OF COMPREHENSIVE SCIENCE
Published by Green Publisher
Crossref Google Scholar GARUDA PKP|INDEX

p -ISSN: 2962-4738 e-ISSN: 2962-4584
Vol. 2 No. 6 Juni 2023

SYSTEMATIC LITERATURE REVIEW (SLR) : KEAMANAN DALAM SISTEM INFORMASI

Wahyu Nisfu Melati Sukma, Ardhito Reynata, Dhivon Auzini Yasmine, Dika Maulana Putra Pratama
Universitas Pembangunan Nasional "Veteran" Jawa Timur
Email: 22082010230@student.upnjatim.ac.id, 222082010233@student.upnjatim.ac.id, 322082010234@student.upnjatim.ac.id, 422082010241@student.upnjatim.ac.id

Abstrak

Keamanan sistem informasi menjadi sangat penting karena dalam era digital saat ini, manusia semakin mengandalkan teknologi informasi dan menyimpan data sensitif secara digital. Makalah ini melibatkan pencarian dalam berbagai sumber literatur, termasuk makalah/jurnal yang terkait dengan keamanan sistem informasi. Sebanyak 100 makalah/jurnal yang relevan yang diterbitkan antara tahun 2019 sampai dengan tahun 2023 telah diidentifikasi dan diseleksi. Temuan utamanya adalah tantangan dalam keamanan informasi yang umum dibahas termasuk Kebocoran data, Penyimpanan data yang tidak terstruktur sehingga menyebabkan data mudah hilang, kurangnya perhatian akan pentingnya keamanan dalam lingkup sistem informasi, dan kurangnya solusi yang menyediakan pemantauan secara real-time. Dan praktik terbaik untuk meminimalisir terjadinya masalah dalam keamanan sistem informasi meliputi penggunaan firewall yang lebih canggih, mengembangkan aplikasi yang sudah ada, melakukan audit keamanan sistem informasi secara rutin. Tinjauan literatur sistematis memberikan gambaran umum terbaru tentang penelitian keamanan sistem informasi yang mutakhir dan mengidentifikasi topik-topik utama untuk penelitian di masa depan. Temuan-temuan ini dapat membantu manusia menilai postur dan strategi keamanan mereka pada era digital saat ini.

Kata Kunci: Systematic Literature Review; keamanan sistem informasi, sistem informasi.

Abstract

Information system security is very important because in today's digital era, people increasingly rely on information technology and store sensitive data digitally. This paper involves a search in various literature sources, including papers/journals related to information system security. A total of 100 relevant papers/journals published between 2019 and 2023 were identified and screened. The main findings are commonly discussed challenges in information security include data leakage, unstructured data storage that causes data to be easily lost, lack of attention to the importance of security within the scope of information systems, and lack of solutions that provide real-time monitoring. And best practices to minimize the occurrence of problems in information system security include using more sophisticated firewalls, developing existing applications, conducting regular information system security audits. A systematic literature review provides an up-to-date overview of current information systems security research and identifies key topics for future research. These findings can help people assess their security posture and strategy in today's digital age.

Keywords: *Systematic Literature Review; information system security, information system.*

PENDAHULUAN

Sistem informasi di perusahaan atau organisasi saat ini terus berkembang, dimana sistem informasi terus mengubah cara masyarakat luas dalam melakukan bisnis. Dikarenakan data yang dihasilkan semakin bertambah dan kompleks, saat ini organisasi atau perusahaan memerlukan analisis yang efektif untuk pengambilan keputusan bisnis yang tepat. Sistem informasi adalah cara untuk mengumpulkan, memasukkan, mengolah, dan menyimpan data serta informasi sedemikian rupa sehingga sebuah organisasi atau perusahaan dapat mencapai tujuan yang telah ditetapkan [1]. Sistem informasi membantu manusia dan organisasi atau perusahaan dalam penciptaan, modifikasi, penyimpanan, komunikasi dan/atau penyebaran informasi dalam berbagai bidang kehidupan. Namun, seiring perkembangannya, kemajuan teknologi terutama kemajuan sistem informasi tidak jarang dimanfaatkan oleh beberapa pihak yang tidak bertanggungjawab yang dapat menyebabkan munculnya ancaman dan resiko dari penggunaan teknologi. Keamanan informasi ditujukan untuk mendapatkan kerahasiaan, ketersediaan, serta integritas pada semua sumber daya informasi perusahaan bukan hanya perangkat keras dan data. Definisi dari keamanan informasi adalah sebagai pelindung informasi dan sistem informasi dari akses, penggunaan, pengungkapan, pengoperasian, modifikasi, atau penghancuran oleh pengguna yang tidak berwenang untuk memastikan kerahasiaan, integritas, dan kemudahan penggunaan. [2] G. J. Simons menyebutkan, keamanan sistem informasi adalah bagaimana kita dapat mencegah penipuan (cheating) atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik [3]. John D. Howard dalam bukunya "An Analysis of Security Incidents on The Internet" menyatakan bahwa keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab [4]. Penelitian ini dilakukan dengan tujuan untuk melakukan Systematic Literature Review (SLR) mengenai keamanan sistem informasi dalam melindungi kepentingan bisnis dan informasi pada sistem informasi. Data yang dikumpulkan dan diidentifikasi menggunakan metode SLR adalah jurnal yang membahas mengenai keamanan dalam sistem informasi dan bagaimana cara mengatasinya. Dengan metode SLR, memungkinkan untuk meninjau dan mengidentifikasi jurnal secara sistematis yang setiap prosesnya mengikuti langkah atau protokol yang telah ditentukan sebelumnya. Selain itu, identifikasi subjektif dapat dihindari dengan metode SLR dan diharapkan hasil identifikasi dapat melengkapi literatur penggunaan metode SLR dalam identifikasi jurnal. Dengan menganalisis penelitian dan mengambil kesimpulan terkait, penelitian ini akan memberikan pemahaman yang lebih baik mengenai konsep, metode, tren dan temuan terkait keamanan sistem informasi dalam melindungi kepentingan bisnis dan informasi. Hasil penelitian ini akan memberikan informasi penting bagi praktisi, akademisi, dan peneliti tentang potensi, manfaat, dan tantangan atas implementasi teknologi yang semakin luas.

METODE PENELITIAN

A. Objek Penelitian.

Objek penelitian ini adalah keamanan dalam sistem informasi. Pengambilan keamanan dalam sistem informasi sebagai objek penelitian memiliki beberapa alasan sebagai berikut:

1. Perkembangan teknologi dan sistem informasi yang semakin pesat memicu pertumbuhan terhadap tantangan keamanan dalam sistem informasi.
2. Tren pengembangan keamanan sistem informasi kedepannya.
3. Keamanan sistem informasi memiliki metode atau solusi yang beragam.

B. Metode Penelitian

1. Research Question.

Research Question atau pertanyaan penelitian dibuat berdasarkan kebutuhan dari topik yang dipilih. Berikut ini adalah pertanyaan penelitian dalam penelitian ini:

RQ1. Apa saja yang yang menjadi tantangan dalam keamanan dalam sistem informasi?

RQ2. Apa saja solusi yang ditawarkan untuk meminimalisir terjadinya masalah dalam keamanan sistem informasi?

2. Search Process

Proses pencarian digunakan untuk mendapatkan sumber informasi yang dibutuhkan untuk menjawab research question (RQ) dan referensi lainnya yang dibutuhkan. proses dilakukan dengan bantuan search engine (Google Chrome) dengan menggunakan alamat situs https://www.sciencedirect.com/ dan https://ieeexplore.ieee.org/Xplore/home.jsp sebagai sumber data primer dan https://www.google.com/ sebagai sumber data sekunder.

3. Inclusion and Exclusion Criteria.

Tahap ini dilakukan untuk mengambil keputusan apakah data yang ditemukan dapat digunakan dalam penelitian SLR atau tidak. Data dapat dipilih apabila terdapat kriteria berikut:

1. Data yang digunakan dalam rentang waktu 2019–2023.
2. Data diperoleh melalui situs https://www.sciencedirect.com/ dan https://ieeexplore.ieee.org/Xplore/home.jsp.
3. Data yang digunakan berhubungan dengan keamanan dalam sistem informasi.

4. Quality Assessment.

Dalam penelitian menggunakan SLR ini, data yang ditemukan akan dievaluasi berdasarkan pertanyaan kriteria penilaian kualitas sebagai berikut:

QA1. Apakah paper atau jurnal diterbitkan dalam rentang tahun 2019–2023?

QA2. Apakah pada paper atau jurnal terdapat informasi terkait dengan keamanan dalam sistem informasi?

QA3. Apakah paper atau jurnal yang diterbitkan memberikan solusi terkait topik permasalahan keamanan dalam sistem informasi?
Dari masing-masing paper, akan diberi nilai jawaban di bawah ini untuk tiap-tiap pertanyaan di atas.
Y (Ya) : untuk data dan metode yang dibutuhkan tertulis pada paper atau jurnal diterbitkan dalam rentang waktu 2019–2023 dan,
T (Tidak) : untuk jurnal yang tidak terkait dengan sistem informasi dan solusi yang tidak ditawarkan.

5. Data Collection.

Data Collection adalah tahap dimana dilakukan pengumpulan data untuk penelitian. Data yang dikumpulkan dalam penelitian ini adalah data primer dan sekunder.

6. Data Primer.

Data primer adalah informasi yang dikumpulkan melalui cara yang disesuaikan dengan kebutuhan seperti survei, wawancara, observasi, dan kajian pustaka. Data primer yang digunakan pada penelitian ini adalah jurnal-jurnal yang berasal dari https://www.sciencedirect.com/ dan https://ieeexplore.ieee.org/Xplore/home.jsp dengan alasan sebagai berikut situs tersebut memberikan fasilitas yang lengkap, data mudah dicari, dan data yang ditampilkan sesuai dengan kebutuhan.

7. Data Sekunder.

Data sekunder digunakan untuk melengkapi data primer apabila pada data primer hanya terdapat abstrak. Data sekunder diperoleh melalui Google. Pengumpulan data dalam penelitian diperoleh melalui beberapa tahap, meliputi:

1. Observasi, yaitu tahapan pengumpulan data melalui pengamatan langsung ke sumber https://www.sciencedirect.com/ dan https://ieeexplore.ieee.org/Xplore/home.jsp.
2. Studi Pustaka adalah tahap untuk melakukan studi pengkajian data terkait dengan Metode SLR pada jurnal yang diperoleh dari https://www.sciencedirect.com/ dan https://ieeexplore.ieee.org/Xplore/home.jsp.

HASIL DAN PEMBAHASAN

A. Hasil Search Process

Hasil search process yang ditampilkan pada tabel 1 dituliskan berdasarkan judul jurnal yang diperoleh melalui search process.

Tabel 1. Pengelompokan berdasarkan jurnal

No.	Tipe Jurnal	Jumlah
	IEEE Access (Volume: 9)	6
2.	IEEE Access (Volume: 10)	6
3.	Computers and Electrical Engineering Volume 105	1
4.	Computers & Security volume 117	2
5.	IEEE Access (Volume: 11)	2

6.	Egyptian Informatics Journal Volume 23, Issue 3	4
7.	IEEE Access (Volume: 8)	3
8.	Informatics in Medicine Unlocked Volume 39	1
9.	International Journal of Information Management Data Insights Volume 1, Issue 2	2
10.	Procedia Computer Science Volume 217	1
11.	Procedia Computer Science Volume 183	2
12.	Egyptian Informatics Journal Volume 20, Issue 2	1
13.	IEEE Access (Volume: 7)	3
14.	Computer Science Review Volume 45	2
15.	Procedia Computer Science Volume 204	2
16.	Procedia Computer Science Volume 149	2
17.	Computers & Security Volume 109	2
18.	Procedia Computer Science Volume 104	1
19.	Procedia Computer Science 215	2
20.	CSEE Journal Of Power And Energy Systems Volume	1
21.	Procedia Computer Science Volume 112	1
22.	Procedia Computer Science Volume 216	1
23.	IEEE Access (Volume: 2)	1
24.	Procedia Computer Science Volume 219	3
25.	IEEE Access (Volume: 5)	1
26.	IERI Procedia Volume 2	1
27.	Procedia Computer Science Volume 176	1
28.	Procedia Computer Science Volume 192	1
29.	Procedia Computer Science Volume 28	1
30.	Engineering Applications of Artificial Intelligence Volume 106	1
31.	IEEE Access (Volume: 6)	1
32.	Heliyon Volume 9	1
33.	Journal of Industrial Information Integration Volume 33	1
34.	Energy Reports Volume 7	1
35.	Computers & Security Volume 128	3

36.	Computers & Security Volume 113	1
37.	Computers & Security Volume 124	4
38.	Procedia Computer Science Volume 208	1
39.	Safety Science Volume 144	1
40.	Computers & Security Volume 120	1
41.	Computers in Industry Volume 132	1
42.	Computers & Security Volume 131	1
43.	Computers & Security Volume 116	1
44.	Progress in Nuclear Energy Volume 161	1
45.	Communications in Transportation Research Volume 2	1
46.	Annual Reviews in Control Volume 53	1
47.	Computers & Security Volume 122	1
48.	Journal of King Saud University - Science Volume 35	1
49.	Computers & Security Volume 125	1
50.	Energy Reports Volume 7	1
51.	Procedia Computer Science Volume 218	1
52.	Journal of King Saud University - Computer and Information Sciences Volume 34, Issue 8, Part B	1
53.	ICT Express Volume 8, Issue 3	1
54.	Computers & Security Volume 129	2
55.	Procedia Computer Science Volume 196	1
56.	Future Generation Computer Systems	1
57.	Journal of Open Innovation	1
58.	Computer Network Volume 193	1
59.	Computer & Security Volume 106	1
60.	Transportation Research Procedia Volume 63	1
61.	Heliyon Volume 7, Issue 3	1
62.	Computer & Security Volume 114	1
63.	Heliyon Volume 7, Issue 9	1
64.	Journal of King Saud University - Computer and Information Sciences Volume 34, Issue 6, Part A	1

65.	Computer & Security Volume 99	1
66.	Procedia Computer Science Volume 138	1
67.	Procedia Computer Science Volume 166	1
68.	Computer & Science Volume 118	1
	Total	102

1. Hasil Seleksi Inclusion and Exclusion Criteria.

Hasil dari proses pencarian (*search process*) akan diseleksi berdasarkan kriteria batasan dan pemasukan (*inclusion and exclusion criteria*). Proses ini menyisakan 67 jurnal yang selanjutnya akan dilakukan scanning data. Tabel 2 menunjukkan hasil kualitas penilaian untuk yang memperlihatkan apakah data tersebut digunakan atau tidak dalam penelitian ini.

2. Hasil Kualitas Penilaian (Quality Assessment)

Tabel 2. Hasil Kualitas Penilaian (Quality Assessment)

Penulis	Jurnal	Tahun	QA1	QA2	QA3	Hasil
Yuchong Li, Qinghui Liu	A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments	2021	Y	Y	Y	✓
Morteza Safaei Pour, Christelle Nader, Kurt Friday, Elias Bou-Harbb	A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security	2023	Y	Y	Y	✓
Arnau Erolaa, Ioannis Agrafiotis, Jason R.C. Nurse, Louise Axona, Michael Goldsmitha, Sadie Creesea	A system to calculate Cyber Value-at-Risk	2021	Y	Y	Y	✓
Enoch Agyepong, Yulia Cherdantseva, Philipp Reinecke, Pete Burnap	A systematic method for measuring the performance of a cyber security operations centre analyst	2022	Y	Y	Y	✓
Yingjie Zenga	AI Empowers Security Threats and Strategies for Cyber Attack	2022	Y	Y	Y	✓
Nelson H. Carreras Guzman, Igor Kozine, Mary Ann Lundteigen	An integrated safety and security analysis for cyber-physical harm scenarios	2021	Y	Y	Y	✓

Alok Mishraa, Yehia Ibrahim Alzoubi, Memoona Javeria Anwar, Asif Qumer Gill	Attributes impacting cybersecurity policy development : An evidence from seven nations	2022	Y	Y	Y	✓
Ángel Jesús Varela-Vacaa, David G. Rosado, Luis E. Sánchez, María Teresa Gómez-López, Rafael M. Gascaa, Eduardo Fernández-Medin	CARMEN : A framework for the verification and diagnosis of the specification of security requirements in cyber-physical systems	2021	Y	Y	Y	✓
Anna Cartwrighta, Edward Cartwrightb , Esther Edunc	Cascading information on best practice : Cyber security risk management in UK micro and small businesses and the role of IT companies	2023	Y	Y	Y	✓
Joseph Da Silva	Cyber security and the Leviathan	2022	Y	Y	Y	✓
Abiodun Ayodeji a,* , Mokhtar Mohamed b , Li Li c , Antonio Di Buono d , Iestyn Pierce b , Hafiz Ahmed a,	Cyber security in the nuclear industry : A closer look at digital control systems, networks and human factors	2023	Y	Y	Y	✓
Zezhou Wang, Xiang Liu *	Cyber security of railway cyber-physical system (CPS) – A risk management methodology	2022	Y	Y	Y	✓
Ferda Özdemir Sönmez a,⁎ , Chris Hankina , Pasquale Malacaria b	Decision support for healthcare cyber security	2022	Y	Y	Y	✓
Chirag Ganguli a , Shishir Kumar Shandilya a , Ivan Izonin b,⇑	Design and implementation of adaptive network stabilization based on artificial bees colony optimization for nature inspired cyber security	2023	Y	Y	Y	✓
Faheem Ahmed Shaikh⁎ , Mikko Siponen	Information security risk Assessments following cybersecurity breaches : The mediating role of top management attention to cybersecurity	2022	Y	Y	T	X

Daniel Jorge Ferreiraa,d, Nuno Mateus-Coelhob,d, Henrique S. Mamedec	Methodology for Predictive Cyber Security Risk Assessment (PCSRA)	2023	Y	Y	Y	✓
Haralambos Mouratidis a,∗ , Shareeful Islamb , Antonio Santos-Olmoa,c , Luis E. Sanchez a,c , Umar Mukhtar Ismail d	Modelling language for cyber security incident handling for critical infrastructures	2023	Y	Y	T	X
Chen Ma	Smart city and cyber-security; technologies used, leading challenges and future recommendations	2021	Y	Y	Y	✓
Jagpreet Kaur, K .R. Ramkumar	The recent trends in cyber security : A review	2021	Y	Y	T	X
Mohammad Wazida , Ashok Kumar Dasb,∗ , Vinay Chamolac , Youngho Parkd,∗	Uniting cyber security and machine learning : Advantages, challenges and future research	2022	Y	Y	T	X
HAICHUN ZHANG1, YUQIAN PAN, ZHAOJUN LU, JIE WANG, ZHENGLIN LIU	A Cyber Security Evaluation Framework for In-Vehicle Electrical Control Units	2021	Y	Y	Y	✓
Alladean Chidukwani, Sebastian Zander , Polychronis Koutsakis	A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations	2022	Y	Y	Y	✓
Duncan Ki-Aries, Shamal Faily B, Huseyin Dogana, Christopher Williams	Assessing system of systems information security risk with OASoSIS	2022	Y	Y	Y	✓
Bader Alkhazi, Moneer Alshaikh, Sulaiman Alkhezi, And Hamza Labbaci	Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior	2022	Y	Y	Y	✓
Daun Jung, Jiho Shin, Chaechang Lee, Kookheui	Cyber Security Controls in Nuclear Power Plant	2023	Y	Y	Y	✓

Kwon, And Jung Taek Seo	by Technical Assessment Methodology					
Hamed Sarjan, Amir Ameli (Member, IEEE), Mohsen Ghafouri (Member, IEEE)	Cyber-Security of Industrial Internet of Things in Electric Power Systems	2022	Y	Y	Y	✓
Khairur Razikin, Benfano Soewito	Cybersecframeworkurity decision support model to designing information technology security system based on risk analysis and cybersecurity	2022	Y	Y	Y	✓
Jung Hwan Kim, Younggeol Cho, Young-A Suh, Man-Sung Yim	Development of an Information Security-Enforced EEG-Based Nuclear Operators' Fitness for Duty Classification System	2021	Y	Y	Y	✓
Ana Kovačević, Nenad Putnik, Oliver Tošković	Factors Related to Cyber Security Behavior	2020	Y	Y	T	X
S. A. Abdymanapov, M. Muratbekov, S. Altynbek , A. Barlybayev	Fuzzy Expert System of Information Security Risk Assessment on the Example of Analysis Learning Management Systems	2021	Y	Y	Y	✓
Adabi Raihan Muhammad, Parman Sukarno , Aulia Arif Wardana	Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning.	2023	Y	Y	Y	✓
Yanqing Ding, Zheng Wu, Zhuantiao Tan, Xin Jiang	Research and application of security baseline in business information system	2021	Y	Y	Y	✓
Rong Fu, Xiaojuan Huang, Yusheng Xue, Yingjun Wu, Yi Tang (Member, IEEE), Dong Yue (Senior Member, IEEE)	Security Assessment for Cyber Physical Distribution Power System Under Intrusion Attacks	2019	Y	Y	Y	✓
Anas Irsheid, Ahmad Murad, Mohammad	Information security risk management models for	2022	Y	Y	Y	✓

AlNajdawi, Abdullah Qusef	cloud hosted systems: A comparative study					
Andrii Boiko, Vira Shendryk, Olha Boiko	Information systems for supply chain management: uncertainties, risks and cyber security	2019	Y	Y	Y	✓
Mario Antunes, Marisa Maximiano, Ricardo Gomes	A Customizable Web Platform to Manage Standards Compliance of Information Security and Cybersecurity Auditing	2022	Y	Y	T	X
Rohani Rohan, Debajyoti Pal, Jari Hautamaki, Suree Funilkul, Wichian Chutimaskul, Himanshu Thapliyal	A systematic literature review of cybersecurity scales assessing information security awareness	2023	Y	Y	T	X
Arif Khan, Muhammad Ibrahim, Abid Hussain	An exploratory prioritization of factors affecting current state of information security in Pakistani university libraries	2021	Y	Y	Y	✓
Khando Khando, Shang Gao, Sirajul M. Islam, Ali Salman	Enhancing employees information security awareness in private and public organisations: A systematic literature review	2021	Y	Y	Y	✓
Svetlana Kirilchuk, Viktor Reutov, Ekaterina Nalivaychenko, Elena Shevchenko, Angela Yaroshenko	Ensuring the security of an automated information system in a regional innovation cluster	2022	Y	Y	Y	✓
Kwesi Hughes-Lartey, Meng Li, Francis E. Botchey, Zhen Qin	Human factor, a critical weak point in the information security of an organization's Internet of things	2021	Y	Y	Y	✓
Mansour Naser Alraja, Usman Javed Butt, Maysam Abbod	Information security policies compliance in a global setting: An employee's perspective	2023	Y	Y	Y	✓
Fredrik Karlsson, Ella Kolkowska, Johan Petersson	Information security policy compliance-eliciting requirements for a computerized software to	2021	Y	Y	T	T

	support value-based compliance analysis					
Bemenet Kasahun Gebremeskel, Gideon Mekonnen Jonathan, Sileshi Demesie Yalew	Information Security Challenges During Digital Transformation	2023	Y	Y	Y	✓
Miroslaw Hajdera, Janusz Kolbusza, Piotr Hajderb, Mariusz Nyczc, Mateusz Liputa	Data Security Platform Model in Networked Medical IT Systems based on Statistical Classifiers and ANN	2020	Y	Y	Y	✓
Hamed Taherdoost	Cybersecurity vs. Information Security	2022	Y	Y	T	x
Khairur Razikin, Benfano Soewito	Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework	2022	Y	Y	Y	✓
Adam Sulich, Malgorzata Rutkowska, Agnieszka Krawezyk-Jezierska, Jaroslaw Jezierskib, Tomasz Zema	Cybersecurity and Sustainable Development	2021	Y	Y	Y	✓
Olha Shulha, Iryna Yanenkova, Mykhailo Kuzub, Iskandar Muda, Viktor Nazarenko	Banking Information Resource Cybersecurity System Modeling	2022	Y	Y	Y	✓
Alberto Blanco-Justicia, Josep Domingo-Ferrer, Sergio Martínez, David Sánchez,Adrian Flanagan, Kuan Eeik Tan	Achieving security and privacy in federated learning systems: Survey, research challenges and future directions	2021	Y	Y	Y	✓
Rong Jiang, Mingyue Shi, dan Wei Zhou	A Privacy Security Risk Analysis Method for Medical Big Data in Urban Computing	2019	Y	Y	Y	✓

Avi Shaked	A model-based methodology to support systems security design and assessment	2023	Y	Y	Y	✓
Faheem Ahmed Shaikh, Mikko Siponen	Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity	2022	Y	Y	T	X
Anas Irsheid, Ahmad Murad, Mohammad AlNajdawi, Abdullah Qusef	Information security risk management models for cloud hosted systems: A comparative study	2022	Y	Y	Y	✓
Andrii Boiko, Vira Shendryk, Olha Boiko	Information systems for supply chain management: uncertainties, risks and cyber security	2019	Y	Y	Y	✓
Mahmoud Maqableh, Hazar Y. Hmoud, Mais Jaradat, Ra'ed Masa'deh	Integrating an information systems success model with perceived privacy, perceived security, and trust: the moderating role of Facebook addiction	2021	Y	Y	Y	✓
Basil Al-Kasasbeh	Model of the information security protection subsystem operation and method of optimization of its composition	2022	Y	Y	Y	✓
Jamal N. Al-Karaki, Amjad Gawanmeh, Sanaa El-Yassami	GoSafe: On the practical characterization of the overall security posture of an organization information system using smart auditing and ranking	2020	Y	Y	Y	✓
Elham Rostami, Fredrik Karlsson, Shang Gao	Requirements for computerized tools to design information security policies	2020	Y	Y	T	X
Yanqing Ding, Zheng Wu, Zhuantiao Tan, Xin Jiang	Research and application of security baseline in business information system	2021	Y	Y	Y	✓

Ankur Shukla, Basel Katt, Livinus Obiora Nweke , Prosper Kandabongee Yeng,Goitom Kahsay Weldehawaryat	System security assurance: A systematic literature review	2022	Y	Y	Y	✓
Hao Hao Song	Testing and Evaluation System for Cloud Computing Information Security Products	2020	Y	Y	Y	✓
Maiju Kyytsönen, Jonna Ikonen, Anna-Mari Aalto, Tuulikki Vehko	The self-assessed information security skills of the Finnish population: A regression analysis	2022	Y	Y	T	X
Duncan Ki-Aries, Shamal Faily, Huseyin Dogan, Christopher Williams	Assessing system of systems information security risk with OASoSIS	2022	Y	Y	Y	✓
Khairur Razikin, Benfano Soewito	Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework	2022	Y	Y	Y	✓
Mona Mirtscha, Knut Blind, Claudia Kocha, Gabriele Dudek	Information security management in ICT and non-ICT sector companies: A preventive innovation perspective	2021	Y	Y	Y	✓

Keterangan simbol:
√ : Untuk jurnal atau data yang digunakan penelitian. Data tersebut dipilih karena memiliki pendekatan, informasi, dan isi yang cukup untuk pemilihan data.
X : Untuk jurnal atau data yang tidak digunakan dalam penelitian karena data ataupun informasi yang kurang memadai untuk pemilihan data.

3. Analisis Data (Data Analysis)

Tahapan ini akan menjawab pertanyaan dari *Research Question* (RQ) dan membahas hasil dari metode serta pendekatan yang dominan muncul dari tahun 2013–2018.

B. Pembahasan Hasil.

RQ1. Apa saja yang yang menjadi tantangan dalam keamanan dalam sistem informasi?

Setelah dilakukan pencarian melalui *search process*, didapatkan 102 jurnal. Setelah itu dilakukan proses seleksi yang dikerjakan berdasarkan *inclusion and exclusion*

criteria dengan menggunakan kata kunci "*information system security*" dan "*cyber security*" sehingga didapatkan 67 jurnal. Setelah itu ditanyakan *Quality Assessment* dimana terdapat 67 jurnal relevan yang kemudian dikelompokkan berdasarkan pengembangan dan pendekatan yang digunakan untuk menjawab *research question* 1 dan 2. Pada diketahui bahwasanya aspek-aspek yang menjadi tantangan terkait keamanan dalam sistem informasi antara lain:

1. Kebocoran data: Kebocoran data didefinisikan sebagai pengunggahan informasi pribadi secara berlebihan ke internet. Dalam hal ini, kebocoran data dalam lingkup sistem informasi yang terjadi dikarenakan beberapa faktor, antara lain ruang penyimpanan perusahaan yang tidak mengembangkan sistem keamanan yang memadai, kurangnya kewaspadaan akan ancaman kejahatan siber yang semakin luas, dan metode atau aplikasi keamanan perusahaan yang kurang menyeluruh sehingga masih menyebabkan adanya kebocoran data.
2. Penyimpanan data yang tidak terstruktur sehingga menyebabkan data mudah hilang: Penyimpanan data yang tidak struktur dapat dialami suatu perusahaan apabila perusahaan tersebut tidak memiliki ruang penyimpanan atas data mereka secara memadai. Kehilangan data menjadi salah satu masalah dalam perusahaan terkait dengan topik keamanan sistem informasi. Apabila perusahaan tidak segera membenahi sistem mereka dalam menyimpan data, maka dampak buruk selain data yang mudah hilang adalah data tersebut dapat bocor ke pihak manapun sehingga memiliki efek yang lebih buruk dibanding kehilangan data itu sendiri.
3. Kurangnya perhatian akan pentingnya keamanan dalam lingkup sistem informasi : Dalam beberapa kasus, ditemukan bahwa masih banyak organisasi maupun perusahaan yang belum memahami akan pentingnya menjaga keamanan dalam sistem informasi. Penyebab data yang mudah bocor, data yang hilang, modifikasi data secara ilegal mayoritas didasari akan kurangnya kepedulian akan keamanan terutama dalam lingkup sistem informasi. Hal tersebut dapat membuat
4. Kurangnya solusi yang menyediakan pemantauan secara real-time dan deteksi jalur kebocoran. kekurangan ini memungkinkan penyerang bergerak di dalam jaringan tanpa terdeteksi, sehingga meningkatkan risiko kebocoran data atau serangan yang tidak terdeteksi. Tantangan ini perlu diatasi guna meningkatkan keamanan dalam sistem informasi dan melindungi data dari ancaman yang ada.

RQ2. Apa saja solusi yang ditawarkan untuk meminimalisir terjadinya masalah dalam keamanan sistem informasi?

1. Meneliti metode atau aplikasi yang sudah ada dan menyempurnakannya: Seiring dengan berkembangnya teknologi informasi yang semakin pesat, metode atau aplikasi yang digunakan untuk melindungi keamanan sistem informasi semakin beragam. dimulai dari metode konservatif seperti memperkuat lapisan keamanan dengan mengimplementasikan teknologi enkripsi data yang lebih aman dan menggunakan firewall yang lebih canggih untuk melindungi sistem dari luar.
2. Mengembangkan metode atau aplikasi baru: Selain meneliti dan mengembangkan metode atau aplikasi yang sudah ada, mengembangkan

metode atau aplikasi baru menjadi salah satu solusi untuk meminimalisir terjadinya masalah keamanan dalam sistem informasi.

Melakukan audit keamanan: audit keamanan sistem informasi secara rutin dapat membantu menemukan kesalahan dalam sistem informasi, melacak aktivitas yang mencurigakan dan memastikan bahwa kebijakan keamanan yang telah ditetapkan telah dilaksanakan dengan benar. Audit dapat dilakukan oleh tim internal perusahaan atau oleh pihak luar yang independen.

KESIMPULAN

Mengacu kepada hasil SLR, didapatkan bahwasanya keamanan sistem informasi mengacu pada perlindungan sistem informasi otomatis dari gangguan yang tidak disengaja atau disengaja dalam proses normal fungsinya, serta dari upaya untuk mencuri, memodifikasi atau menghancurkan komponennya. Dengan berkembangnya zaman dan semakin majunya teknologi informasi, sistem informasi saat ini mengalami beberapa masalah termasuk ke dalamnya mengenai sistem keamanan, baik keamanan dalam sistem informasi lingkup luas seperti perusahaan maupun lingkup sempit seperti organisasi. Kebocoran data serta kemungkinan data yang hilang menjadi masalah yang paling umum terjadi. Kebocoran data adalah pengunggahan informasi pribadi secara berlebihan ke internet. Namun dalam hasil SLR ini didapati bahwa kebocoran data biasa terjadi akibat kurangnya mekanisme keamanan yang tepat untuk melindungi data pengguna, kebijakan dan peraturan privasi yang tidak memadai, kesalahan manusia atau kelalaian, serangan cyber dan upaya peretasan. Maka dari itu, untuk mengamankan data perlu meminimalkan terjadinya masalah dalam keamanan sistem informasi dengan menerapkan pemantauan real-time dan deteksi jalur kebocoran, pengujian kebijakan segmentasi, dan secara teratur dan otomatis inventarisasi perangkat dan sistem yang terhubung ke jaringan. Ini menunjukkan bahwa kebocoran data dapat terjadi karena kurangnya langkah-langkah keamanan yang tepat dalam sistem informasi.

BIBLIOGRAFI

[1] Krismiaji, Sistem Informasi Akuntansi, Keempat. Yogyakarta: UPP STIM YKPN, 2015.

[2] Nurul, S., Anggrainy, S., & Aprelyani, S., "Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review SIM)," Jurnal Ekonomi Manajemen Sistem Informasi, 2022, 3(5), 564-573.

[3] Rahardjo B, "Keamanan Sistem Informasi Berbasis Internet," Bandung, 2002.

[4] Harliana P, Perdana A, Prasetyo RMK, "Sniffing dan Spoofing Pada Aspek Keamanan Komputer," Pada https://www.academia.edu/5088063/JurnalKeamanan-Komputer, diakses pada 25 Mei 2023.

[5] O.P. Brereton, B.A. Kitchenham, D. Turner Budgen, M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," Journal of Systems and Software 80 vol. 4, 2007, 571–583.

[6] Lusiana and M. Suryani, "Metode SLR untuk Mengidentifikasi Isu-Isu dalam Software Engineering," SATIN (Sains dan Teknologi. Informasi), vol. 3, no. 1, 2014

[7] R. T. S. Hariyati, "Mengenal Systematic Review Theory dan Studi Kasus," J. Keperawatan Indones., vol. 13, no. 2, pp. 124–132, 2010.