Hindawi
Security and Communication Networks
Volume 2021, Article ID 8686469, 10 pages
https://doi.org/10.1155/2021/8686469

Review Article

Systematic Analysis of Artificial Intelligence-Based Platforms for Identifying Governance and Access Control

Mohammad Kamel Alomari,[1] **Habib Ullah Khan**,[1] **Sulaiman Khan**,[1,2] **Alanoud Ali Al-Maadid**,[3] **Zaki Khalid Abu-Shawish**,[1] **and Helmi Hammami**[4]

[1]*Department of Accounting and Information Systems, College of Business and Economics, Qatar University, Doha, Qatar*
[2]*Department of Computer Science, University of Swabi, Swabi, Pakistan*
[3]*Department of Finance & Economics, College of Business & Economics, Qatar University, Doha, Qatar*
[4]*Rennes School of Business, Rennes, France*

Correspondence should be addressed to Habib Ullah Khan; habib.khan@qu.edu.qa

Received 21 June 2021; Revised 28 August 2021; Accepted 2 December 2021; Published 18 December 2021

Academic Editor: Shehzad Ashraf Chaudhry

Artificial intelligence (AI) has become omnipotent with its variety of applications and advantages. Considering the other side of the coin, the eruption of technology has created situations that need more caution about the safety and security of data and systems at all levels. Thus, to hedge against the growing threats of cybersecurity, the need for a robust AI platform supported by machine learning and other supportive technologies is well recognized by organizations. AI is a much sought-after topic, and there is extolling literature available in repositories. Hence, a systematic arrangement of the literature that can help identify the right AI platform that can provide identity governance and access control is the need of the hour. Having this background, the present study is commissioned a Systematic Literature Review (SLR) to accomplish the necessity. Literature related to AI and Identity and Access Management (IAM) is collected from renowned peer-reviewed digital libraries for systematic analysis and assessment purposes using the systematic review guidelines. Thus, the final list of articles relevant to the framed research questions related to the study topic is fetched and is reviewed thoroughly. For the proposed systematic research work, the literature reported during the period ranging from 2016 to 2021 (a portion of 2021 is included) is analyzed and a total of 43 papers were depicted more relevant to the selected research domain. These articles were accumulated from ProQuest, Scopus, Taylor & Franics, Science Direct, and Wiley online repositories. The article's contribution can supplement the AI-based IAM information and steer the entities of diverse sectors concerning seamless implementation. Appropriate suggestions are proposed to encourage research work in the required fields.

1. Introduction

Being conceptualized during World War II, named during the 1950s, and updated in the 2000s, artificial intelligence (AI) has fuelled the global innovation landscape [3–5]. On the one hand, AI has unleashed various technologies across all domains, and on the other hand, it has created more security concerns across all sectors. In olden days, security concerns were used to confine to a particular sector or department. However, the advent of enterprise-level systems raised the necessity of comprehensive security solutions for which AI has become a panacea [6–9]. Thus, AI platforms that provide security solutions to organizations through Identity Access Management (IAM) and governance have become the most sought after. Studies established that AI provided the greater impetus to identity and access governance for all sectors [3, 10, 11].

Along with the increasing attention for AI, identity access management has become vital and throws challenges on the entities. Likewise, umpteen domain-specific applications are tailored far and wide [12–14]. The threat is more prevalent in advanced platforms that comprise fully

automated systems, predictive intelligence modelling, and other state-of-the-art technologies [4, 5, 15]. Identity and access management is much deployed in connected and autonomous vehicles (CAVs) through performance evaluation metrics, advanced driver assistant systems, security analysis of IoT devices through mobile computing, and so on [14,16]. Discussing the devastating effect of the Equifax Breach, Diesch et al. [6] opine that technical flaws lead to comprehensive complications related to identity, governance, and access control. Along with the growth of technology, there has always been a need for updating the security structure, frameworks, and policies of organizations. Thereby, access permission management can be well incorporated in the security profile [17].

AI-enabled platforms coupled with stringent security profiles and access management are identified as the future leaders of the market [7, 9, 18]. However, it is an undeniable fact that there are numerous instances that the AI-enabled systems led to wrong decisions. Krupiy shared the instances wherein the AI-enabled decision-making failed to do the correct entitlement [19]. Additionally, the unfair practices/decisions in refund entitlement that artificial technology-based gaming is causing are discussed by King et al. [20]. These fallacies often end up with consumer protection issues. Hence, the efficiency and effectiveness of the user entitlement through a robust AI framework are to be given high priority. The identity and access management model, which comprises components such as User Access Certification Services, Access Management Services, Identity Management Services, and many more, can provide solutions for AI betterment [21–23].

Discussing the features to be incorporated in the 5G architecture and the security profile as a part of the quality of service, Peinado et al. [24] felt the need for access control, highlighted the problems with existing security mechanisms, and proposed that network information and insights can help to develop a framework to overcome the drawbacks of AI-related security issues. Nevertheless, the information security risks always persist in every domain (campus-based or cloud-based or mobility-based) and mount along with technological emergence. In a study about the information security risks through cyberattacks for modern connected autonomous vehicles (CAVs), it is felt that cyber protection techniques coupled with predictive analytics can help counter the risks [25]. Methta et al. [26] share application of smart manufacturing analytics in the manufacturing process (ISA-95) that provides security to the system by giving efficient entitlement and employs predictive modelling.

1.1. Problem Statement. Since artificial intelligence-based platform for Identity Governance and Access Control is very much needed for all types of technology-based organizations/setups, literature about the topic is mammoth. The cognition of the dynamic stage of the artefact and the availability of abundant literature related to all these state-of-the-art technologies raised the need for organizing through a systematic literature review. The literature available is reviewed, and the following research questions are framed to understand the connectivity between the involved concepts of AI in a better matter.

1.2. Objectives. Main objectives of this SLR work include

To systematically analyze the extant reported (in well-reputed online repositories) during the period ranging from 2016 to 2021 for ensuring high security and authenticity within the organization using artificial intelligence and machine learning techniques.

Based on the systematic assessment, identify the gaps in the published research work and suggest new research direction for the researchers to explore in the near future. These new research directions will not only accurately combat the gaps addressed in this systematic analysis but will also ensure high security and integrity within the organizations.

To attract researchers and industrialists to contribute in the field of embedded and smart application domains to open new opportunities for the software developers and engineers to present their skills by developing optimum secure models.

1.3. Research Questions. Two research questions are formulated to assess the available literature published in the proposed field listed below:

(a) How can we enhance the efficiency and effectiveness of the user access and entitlement review process using AI capabilities?

(b) How can we reduce information security risks by generating and leveraging predictive intelligence?

Although there are many AI interventions across the globe, they are either confined to identity governance or access control mechanisms. Having understood the rising need for both topics (identity governance and access control) in the era of AI and the significance of these dynamic concepts, a systematic literature review is planned. The study proceeded as follows. The systematic literature review methodology is explained; the research process follows the protocol suggested in [1, 27, 28]. The search results as per the research questions and their quality assessment were done in the later sections.

Rest of the paper is organized as follows. The systematic review process and the proposed experimental setup are briefly explained in Section 2 of the paper. The findings of this SLR work and the results and discussion of this systematic analysis are detailed in Section 3. Section 4 of the paper has outlined the conclusion of this SLR work followed by the implications, and future research directions are introduced in Section 5 of the paper.

2. Systematic Literature Review Method

Systematic literature review is the process of identifying and analyzing the available literature by identifying the gaps in the available research work and suggesting future research work accordingly. Keeping these applications in mind, most

of the researchers, industrialists, and clinicians suggest to perform a systematic research work to get updated about the new research work reported in the topic of interest. Also, before deciding a new research direction, they conduct a systematic analysis to find the gaps in the available research trends. The term "artificial intelligence" is a buzzword, and AI technology is being deployed in every domain, particularly in emerging sectors [29–31]. Articles about the proposed study are downloaded from renowned data libraries. These libraries are selected depending on the data availability related to the study topic and the library's reputation. Thus, having the research questions framed, five data libraries are selected for performing SLR. The flowchart in Figure 1 explains the steps involved in carrying out the SLR process.

Thus, to get the answers to the research questions, queries are prepared with keywords, which are also called search string. The string is framed by selecting the keywords in the research question. In some databases, wherein the combination of keywords does not result in a list of articles, simple queries are given to extract the related articles. The research questions and the combination of keywords framed along with the relevance of the research question are given in Table 1.

Having decided the research questions and the combination of keywords, a range of renowned scientific data repositories named—Science Direct, Wiley Online, Proquest, Tandfonline, and Scopus—are reviewed. Artificial intelligence is the most embraced, technological artefact is much researched, and umpteen technological advancements are soaring in this domain day by day. Therefore, to appraise the latest developments related to AI, the SLR paper considered articles for the past five years (2016–2020) and a few months of 2021, the papers published between 2016 and April 2021. Furthermore, as AI applications are numerous across domains/subjects, articles related to 'computer science' or 'business' subjects are only considered for the study. This filtration is done to fetch the articles that are relevant to the research questions. As the global database consists of AI literature in various languages, the constraint related to language is also levied, and hence, the research confided on the articles in English only. Similarly, due to the restrictions to download the full content of the articles, Open Access articles alone are considered for the research. The bar chart given in Figure 2 narrates the total number of articles collected as per their year of publication.

Thus, a total of 124 articles are considered for the study, and for SLR, 94 articles from the identified data repositories published between the years 2016–2021 are only considered, and the remaining articles (30) are considered for conceptual support of the research work. The constraints of SLR are levied by keeping the scope of research questions in view. The type of data sources reviewed and the date of review are furnished in Table 2.

As shown in Table 2, a total of 8361 articles (for both research questions) are selected from the five libraries/datasets selected for the two research questions. The results obtained after entering the queries for both research questions are filtered using various criteria. They are year, article type, subject, language, availability in open source, and others. These criteria are listed in Figure 3.

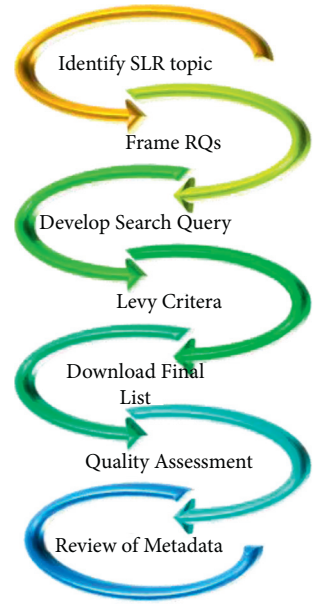

Figure 1: Steps involved in the SLR process.

The rationale behind the formation of queries based on the two research questions is to select the literature by appraising the latest technologies that emerged across the world in the AI domain and downloading such articles. Moreover, the literature other than articles such as workshop/conference proceedings, white papers, term reports of organizations, and others is omitted from the search. The results are downloaded in bibliography (.bib) file format. These files are organized into the corresponding folders of the data library using the reference manager software Mendeley. From the collected list of articles, the repetition is checked, and thus, the updated list is prepared. From the total 8391 articles (8361 for SLR and 30 supportive literature) collected for the study, seven articles are considered duplicate and hence removed from the study list. The steps involved in the whole process are depicted in Figure 4.

Thus, 8361 articles are retrieved by entering the queries for both research questions for the SLR study. However, after deploying the criteria, filtration has resulted in 80 and 14 articles for the research questions RQ1 and RQ2, respectively (Table 2). The digital library-wise literature reveals that, for RQ1, 40 articles were retrieved from Science Direct, 29 from Wiley Online, 2 from ProQuest, 4 from Tandfonline, and 5 from Scopus. Similarly, for RQ2, 5 articles were retrieved from Science Direct, 4 from Wiley Online, 1 from ProQuest, 2 from Tandfonline, and 2 from Scopus. In addition to the articles related to the five data repositories, supportive articles related to AI are collected in a folder named others. Thus, the total number of articles collected (124) is represented pictorially in Figure 5.

2.1. Study Selection. The articles thus selected are downloaded using the reference manager, Mendeley, and are placed in separate folders named per library. Other articles selected for the conceptual base of the research study from

Table 1: List of the keywords selected for the study.

Research question	Combination of keywords	Relevance
1. How can we enhance the efficiency and effectiveness of the user access and entitlement review process using AI capabilities?	(("Efficiency" OR "effectiveness" OR "user access") AND ("entitlement review" OR "entitlement") AND ("artificial intelligence" OR "AI capabilities")) ("User access" OR "artificial intelligence" OR "entitlement")	As the AI technology is very dynamic, the research questions aim at the means to enhance the efficiency of user access and entitlement from time to time
2. How can we reduce information security risks by generating and leveraging predictive intelligence?	("Information security risk") AND ("generating" OR "leveraging") AND ("predictive intelligence" OR "prediction") ("Information security risk") AND ("predictive intelligence")	The need to counter the mounting information security risk with emerging technologies such as predictive modelling is identified

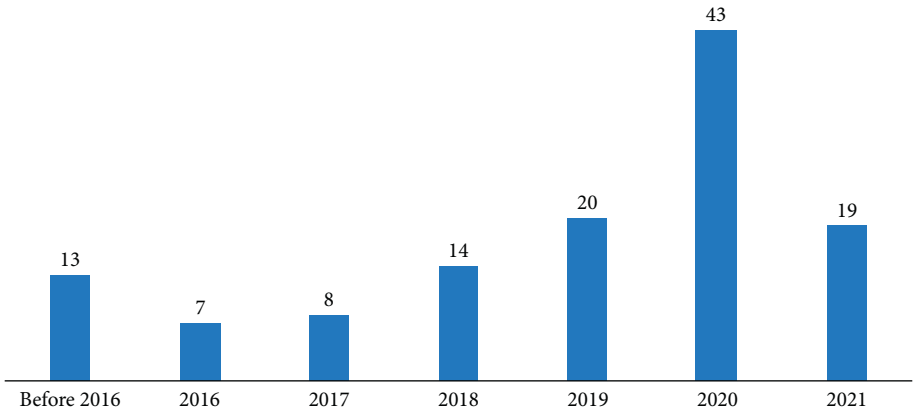

Figure 2: Count of articles selected as per year of publication.

Table 2: Details of the articles' search for research questions.

Database	Date accessed	No. of articles (without filters)		No. of articles (with filters)		Total
		RQ1	*RQ2*	*RQ1*	*RQ2*	
Science direct	19.4.2021	2376	88	40	5	45
Wiley online	17.4.2021	5477	4	29	4	33
ProQuest	23.4.2021	117	45	2	1	3
Tandfonline	16.4.2021	25	2	4	2	6
Scopus	16.4.2021	162	65	5	2	7
Total		8157	204	80	14	94

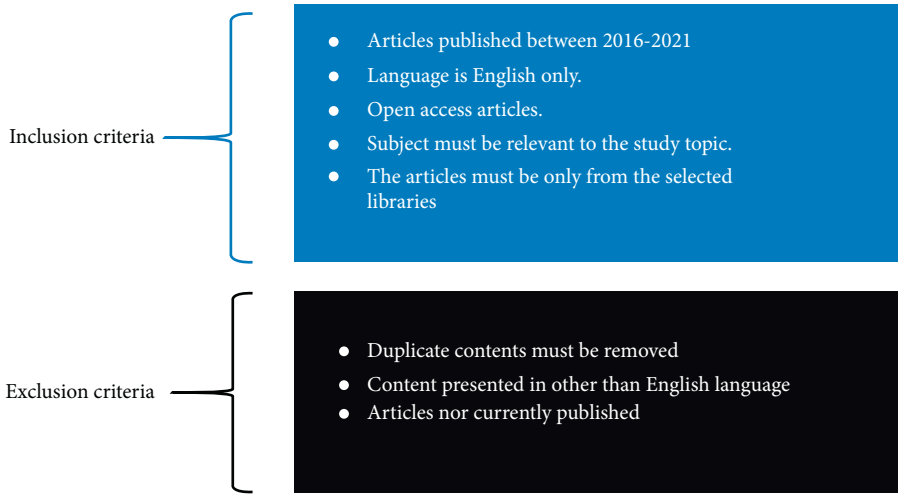

Figure 3: Inclusion and exclusion criteria followed for this SLR work.

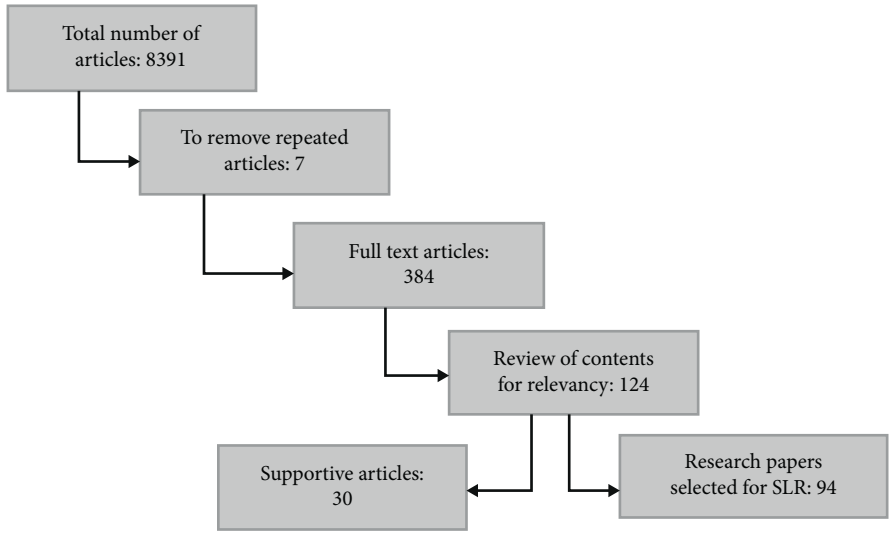

Figure 4: Number of articles in the proposed SLR protocol.

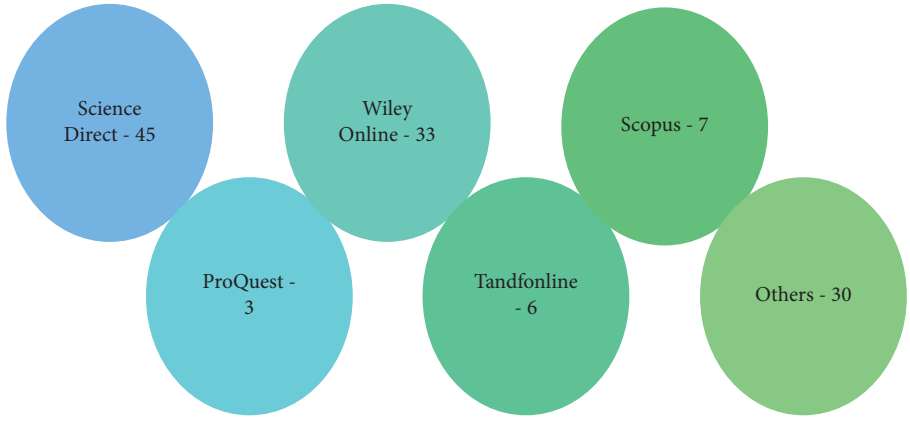

Figure 5: Database-wise count of articles.

various sources are placed in the folder "Others." Articles are reviewed individually for relevance concerning abstracts and content. This filtration process aided in identifying the existing literature that can help to answer the research questions. The content of the article and the suitability of the article are verified with the help of literary works as discussed by Kitchenham et al. [27]. The graphs in Figures 6 and 7 explain the relative proportion of articles drawn from various renowned digital repositories for the research questions RQ1 and RQ2 individually.

Similarly, the articles drawn from the databases for the second research question (RQ2) are depicted in the following chart.

2.2. Quality Checking. Having the set of articles downloaded, it is equally important [17, 32] to check the quality of the articles by assessing their relevance to the research questions. The articles selected for SLR are reviewed individually to understand the extent of suitability of the content to answer the study's research questions. As advocated by the scholars of the SLR method, the articles are reviewed and are assigned to suitable values by examining their content relevancy. Figure 8 highlights the quality assessment flow during this process.

> Q1. Does the article provide a content base for understanding the means to enhance user access and entitlement review process efficacy using AI capabilities?
>
> Q2. Does the article provide the means to reduce the information security risks by generating and leveraging predictive intelligence?

Articles collected are reviewed individually with the above questions, and they are given a value 1 (YES) if the article's content is added to the sought questions. Similarly, if the article is partially able to answer the questions, it is given a value 0.5 (PARTIAL). Otherwise, the value allotted is 0 (NO). Hence, the values obtained for quality assessment of the articles are plotted in the following chart for better understanding.

Following the method of aggregated value calculation proposed by Tahir et al. [7], the total score of quality assessment is estimated. As there are two research questions, a

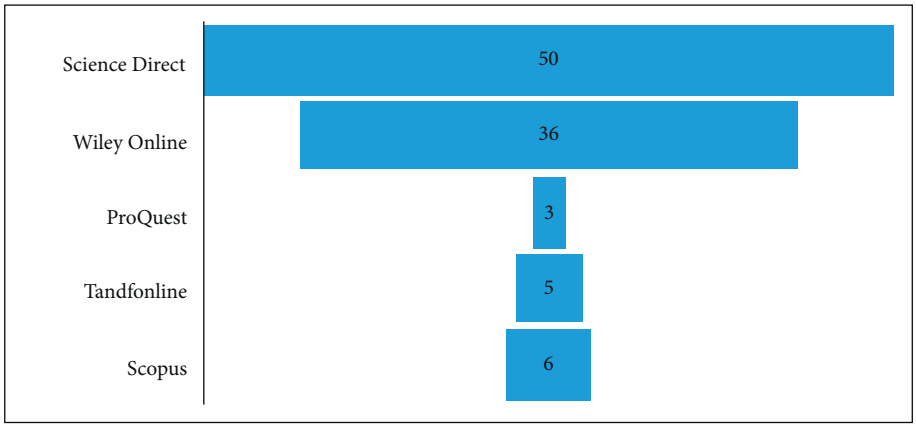

Figure 6: Proportion of articles considered for RQ1.

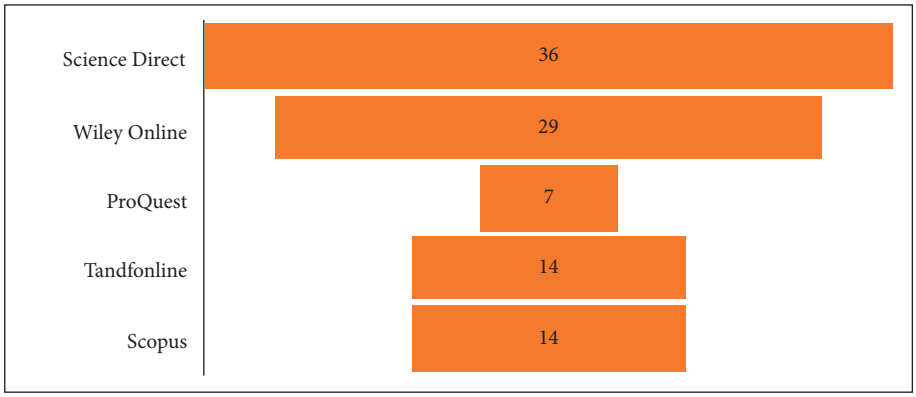

Figure 7: Proportion of articles considered for RQ2.

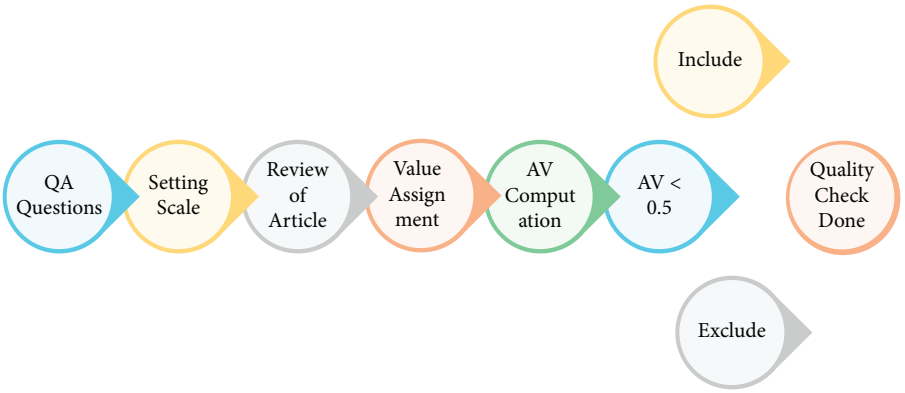

Figure 8: Quality assessment (QA) flow.

cut-off value of 0.5 is decided for identifying the most relevant articles. If the aggregated value is greater than or equal to 0.5, the article is selected considering that it is catering to the information of either of the research questions. The articles listed in such a process are given in Table 3. The articles whose score is less than 0.5 are not considered for the study.

The values of 'total score' obtained by quality assessment can be seen in Table 3. As it can be observed, the more relevant articles to the research questions are arranged in the

Table 3: Quality assessment of the articles based on the relevancy.

Ref	Topic covered	RQ1 score	RQ2 score	Aggregate score
[21]	Security-as-a-service for identity access management	1	1	2
[33]	Identity provision and user access provision through IDP session	1	1	2
[34]	Role based access for system security	1	1	2
[10]	AI and the applications for user interface and others	1	0.5	1.5
[6]	Organizational information security management through management success factors (MSF)	1	0.5	1.5
[35]	Single-sign-on service for identity management	0.5	1	1.5
[36]	Attribute based access control for IAM to achieve total attribute quality management (TAQM)	1	0.5	1.5
[17]	Policy perspective of dynamic identity and user management	1	0.5	1.5
[25]	Information security with predictive mechanisms	0.5	1	1.5
[37]	Integration of artificial intelligence activities in software development processes	0.5	1	1.5
[38]	Predictive intelligence to the edge of the IoT network.	0.5	1	1.5
[39]	Attribute-centric access control	1	0.5	1.5
[13]	Role-based access control	1	0.5	1.5
[40]	Cleaning unauthorized access	1	0.5	1.5
[41]	Comprehensive overview of AI-based techniques used in wireless sensor networks (WSN)	0.5	0.5	1
[19]	Entitlement decision and prediction with the help of AI	0.5	0.5	1
[42]	Functional requirement for authority data and for subject authority data-related models	1	0	1
[43]	AI systems and applications	0.5	0.5	1
[44]	Applications of artificial intelligence, deep learning, and machine learning	0.5	0.5	1
[39]	Decentralized IAM	1	0	1
[30]	Modelling for predictive algorithms to provide information security, transparency, and accountability in decision-making	0	0.5	0.5
[45]	Virtual engineering process, predictive management, and allied concepts for effective decision-making	0	0.5	0.5
[46]	AI tools for user behaviour assessment and interaction with environment	0.5	0	0.5
[47]	Knowledge representation model for prediction mechanism	0	0.5	0.5
[29]	Development of system compatible with advanced technologies such as AI, which ensure security	0.5	0	0.5
[20]	Application of AI for entitlement review	0.5	0	0.5
[48]	AI and accessibility	0.5	0	0.5
[49]	Unexplored areas of computer science applications	0.5	0	0.5
[50]	Perspectives on digital identity systems	0.5	0	0.5
[40]	Predictive intelligence	0	0.5	0.5

descending order of the total score. However, it can be noticed that the relevant articles for the first research questions are more available than those for the second. This affirms the research work's need concerning predictive intelligence modelling of information security mechanisms.

3. Results and Discussion

This section of the paper outlines the results and discussion based on the analysis using the final set of relevant articles. Recently, AI has been applied in diverse research fields due to its high capabilities of generating optimum results in comparatively small time with low simulation and hardware costs. Keeping these applications in mind, the researchers reported a huge number of publications in the selected domain. Reviewing all these research articles and retrieving the information regarding a specific of interest is a hectic job. To address this problem, a systematic research work is presented that has analyzed the research work reported during the period ranging from 2016 to 2021 (a section of 2021 is included) to outline the most relevant research work reported in the proposed field. Two different research questions are selected for outlining this systematic analysis. The underline results and discussion is outlined below based on the formulated research questions.

3.1. RQ1: How Can We Enhance the Efficiency and Effectiveness of the User Access and Entitlement Review Process Using AI Capabilities? The shortcomings in data management systems in organizations lead to many loopholes in the enterprise systems and mechanisms. There are many examples for such technologies such as hierarchical access setup, cloud server setup, and others [23, 40]. The concept of identity and access management (IAM) and entitlement review can be understood as traditional and cloud-based [21, 39]. In the case of former IAM, the digital identity of people used to be given priority. However, in the latter case, a range of concepts such as IoT-based, decentralized identifiers, and verifiable credentials opened new avenues in IAM. Notwithstanding this, the emerging applications of artificial intelligence have fuelled the exploration of efficient means for access and entitlement review process in various domains [19, 36].

On the contrary, the authors also highlighted the possible general errors in identity and access management and entitlement review using AI technology. For instance, the

mistakes that occur in the process of AI-based refund entitlement in video games are shared [20]. It is advocated that AI technology must be developed considering the social, psychological, and user-oriented aspects stipulated in a legal framework. Furthermore, the fallacies that occur due to the biased entitlement in the AI-based social justice process are highlighted by Krupiy et al. [19]. Based on the studies carried out by considering the incidents of AI-based social injustice mechanism that resulted in disadvantage and discrimination of individuals, it is suggested to employ AI decision-making considering coupled with human decision-making. Only through embedding, customized and feasible procedures can it increase AI-enabled user access and entitlement review process efficiency and effectiveness.

3.2. RQ2: How Can We Reduce Information Security Risks by Generating and Leveraging Predictive Intelligence? In the era of information, the upgradation of security technologies and malware has become more prevalent, resulting in many intentional and unintentional security risks. Many security models are explained that can help predict and counter the information security risks efficiently. Predictive modelling techniques are deployed to reduce information security risks in many ways. For instance, models such as security-as-a-service (Saas), Identity Access Management (IAMaas), Identity management as a service (IDaaS), and others are recommended for security provided through cloud services. Discussing the view about AI in healthcare solutions, Kunz et al. [48] opined that, in the wake of an emerging healthcare, applications of AI, models that predict and protect the security and privacy of users not only by inductive but also by deductive disclosure were much anticipated.

Explaining the role of AI in the future, Shabbir et al. [3] shared the significance of the transition from GUI to CUI and explained how predictive modelling could play a vital role in forecasting various vital aspects of technology. Furthermore, the significance of the waterfall model in software development and integration of AI is explained by Kulkarni and Padmanabham [37]. The role of predictive modelling coupled with other techniques in software development is also proposed for the effective management of information. Elaborating on edge analytics and predictive intelligence, Harth et al. [40] explained how predictive intelligence could help enterprise management of IoT devices.

Identity governance and access control have become complex with the technological evolution. The systems' requirements and their management have also multiplied along with the shift from local area-bound networks to cloud-based networks. One of such demanding artefacts is a security system. Artificial intelligence is a game changer in various domains; organizations have supported AI for leapfrogging in the space of identity governance and access management. The present SLR is commissioned to organize the literature evolved in these lines to supplement the evolving information related to identity governance, access control, and AI. Research questions are prepared to attain the objective of the SLR study. Literature related to these questions is obtained from five renowned digital repositories.

From the peer-reviewed articles selected from the repositories, literature related to the study topic is retrieved by imposing the general inclusion and exclusion criteria. The filtered list of articles is reviewed, and their relevance is identified along with the content quality. Thus, the research questions are answered with the content obtained. However, as the study topics AI-based identity governance and access control are still in a nascent stage and not domain specific, the relevant literature is found very scant. Research work in these lines can underpin the ins and outs of the topics that are specific to global sectors.

4. Conclusion and Recommendations

Artificial intelligence has played a revolutionary role in diverse research fields including healthcare, pattern recognition problems, Big Data, transportation, and many others. After this systematic analysis, it was concluded that AI applications have left no stone unturned in the present technological era. However, specific AI platforms with user orientation, community orientation, and compatibility are much anticipated by research communities and organizations. The literature has highlighted the need for specific AI-enabled cybersecurity tools that can hedge against emerging cyber threats and proactively forecast possible risks. Additionally, unlike the traditional campus-confined information security systems, enterprise-wide and cloud-based AI platforms that provide seamless Identity Governance and User Access can address a range of security challenges concerning tracking, managing, and restricting access entitlement services. The inputs gained from the SLR related to AI platform and Identity Governance revealed that the extol literature has evolved, highlighting the capabilities of AI in providing information security for organizations. With the shift from microunits to macroentities, information security has become a vital factor. Simultaneously, user access entitlement turned out to be inevitable for the mere existence of data-centric organizations. However, a thorough review of the articles collected regarding both research questions furnished exciting facts. It is observed from the literature that there is more research work going on regarding the former research question than the latter.

5. Implications and Future Research Directions

Following are the implication and new future research directions of this SLR work:

(1) The SLR could accrue more inputs about enhancing the efficiency and effectiveness of user access and entitlement review process using AI capabilities.

(2) Additionally, the literature established the need for more research work to be encouraged regarding information security risks by generating and leveraging predictive intelligence. In the wake of mounting malware technologies, digital economies, and spread of data-centric businesses, there is every need to deploy up-to-date information security systems and supporting frameworks. This necessity

has to be given high priority across the domains, which can only be realized with the help of stringent AI platforms and efficient predictive modelling systems.

(3) Hybrid deep learning models and smart AI solutions are the new future tools of the IIoT applications.

Data Availability

No data were used to support the findings of the study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by Qatar University (Internal Grant no. IRCC-2021-010).

References

[1] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering - a systematic literature review," *Information and Software Technology*, vol. 51, no. 1, pp. 7–15, 2009.

[2] S. Pahlevan Sharif, P. Mura, and S. N. R. Wijesinghe, "Systematic reviews in Asia: introducing the "PRISMA" protocol to tourism and hospitality scholars," *Quantitative Tourism Research in Asia*, Springer, Berlin/Heidelberg, Germany, pp. 13–33, 2019.

[3] J. Shabbir and T. Anwer, "Artificial intelligence and its role in near future," *ArXiv*, vol. 14, no. 8, pp. 1–11, 2018, [Online]. Available: http://arxiv.org/abs/1804.01396.

[4] A. Ghosh, D. Chakraborty, and A. Law, "Artificial intelligence in Internet of things," *CAAI Transactions on Intelligence Technology*, vol. 3, no. 4, pp. 208–218, 2018.

[5] P. D. Mausam and D. S. Weld, "Artificial intelligence for artificial artificial intelligence," *Proc. Natl. Conf. Artif. Intell.,* vol. 2, pp. 1153–1159, 2011.

[6] R. Diesch, M. Pfaff, and H. Krcmar, "A comprehensive model of information security factors for decision-makers," *Computers & Security*, vol. 92, Article ID 101747, 2020.

[7] A. Tahir, F. Chen, H. U. Khan et al., "A systematic review on cloud storage mechanisms concerning e-healthcare systems," *Sensors*, vol. 20, no. 18, pp. 5392–5432, 2020.

[8] C. Meske and I. Amojo, "Status Quo, critical reflection, and the road ahead of digital nudging in information systems research: a discussion with markus weinmann and alexey voinov," *Communications of the Association for Information Systems*, vol. 46, pp. 402–420, 2020.

[9] B. Shneiderman, "Bridging the gap between ethics and practice," *ACM Transactions on Interactive Intelligent Systems*, vol. 10, no. 4, pp. 1–31, 2020.

[10] Z. Wang, L. Xie, and T. Lu, "Research progress of artificial psychology and artificial emotion in China," *CAAI Transactions on Intelligence Technology*, vol. 1, no. 4, pp. 355–365, 2016.

[11] C. Gunter, D. Liebovitz, and B. Malin, "Experience-based access management: a life-cycle framework for identity and access management systems," *IEEE Security and Privacy Magazine*, vol. 9, no. 5, pp. 48–55, 2011.

[12] D. Servos and S. L. Osborn, "Current research and open problems in attribute-based access control," *ACM Computing Surveys*, vol. 49, no. 4, pp. 1–45, 2017.

[13] M. A. Habib, M. Ahmad, N. Mahmood, and R. Ashraf, "An evaluation of role based access control towards easier management compared to tight security," *Proceedings of the International Conference on Future Networks and Distributed Systems*, in *Proceedings of the International Conference on Future Networks and Distributed Systems*, New York, NY, USA, July 2017.

[14] N. Naik and P. Jenkins, "A secure mobile cloud identity: criteria for effective identity and access management standards," *2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, in *Proceedings of the 2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, pp. 89-90, Oxford, UK, April 2016.

[15] R. S. Moghadam and R. Colomo-Palacios, "Information security governance in big data environments: a systematic mapping," *Procedia Computer Science*, vol. 138, pp. 401–408, 2018.

[16] A. Lopez, A. V. Malawade, M. A. Al Faruque, S. Boddupalli, and S. Ray, "Security of emergent automotive systems: a tutorial introduction and perspectives on practice," *IEEE Design & Test*, vol. 36, no. 6, pp. 10–38, 2019.

[17] G. Peinado Gomez, J. Mongay Batalla, Y. Miche et al., "Security policies definition and enforcement utilizing policy control function framework in 5G," *Computer Communications*, vol. 172, no. 2020, pp. 226–237, 2021.

[18] T. Krupiy, "A vulnerability analysis: theorising the impact of artificial intelligence decision-making processes on individuals, society and human diversity from a social justice perspective," *Computer Law & Security Report*, vol. 38, Article ID 105429, 2020.

[19] D. L. King, P. H. Delfabbro, S. M. Gainsbury, M. Dreier, N. Greer, and J. Billieux, "Unfair play? video games as exploitative monetized services: an examination of game patents from a consumer protection perspective," *Computers in Human Behavior*, vol. 101, no. March, pp. 131–143, 2019.

[20] D. H. Sharma, C. A. Dhote, and M. M. Potey, "Identity and access management as security-as-a-service from clouds," *Procedia Computer Science*, vol. 79, pp. 170–174, 2016.

[21] M. Kunz, L. Fuchs, M. Hummer, and G. Pernul, "Introducing dynamic identity and access management in organizations," in *Proceedings of the International Conference on Information Systems Security*, pp. 139–158, Hyderabad, India, December 2015.

[22] I. Indu, P. M. R. Anand, and V. Bhaskar, "Identity and access management in cloud environment: mechanisms and challenges," *Engineering Science and Technology, an International Journal*, vol. 21, no. 4, pp. 574–588, 2018.

[23] P. Mehta, S. Butkewitsch-Choze, and C. Seaman, "Smart manufacturing analytics application for semi-continuous manufacturing process - a use case," *Procedia Manufacturing*, vol. 26, pp. 1041–1052, 2018.

[24] A. Alaassar, A.-L. Mention, and T. H. Aas, "Exploring a new incubation model for fintechs: regulatory sandboxes," *Technovation*, vol. 103, Article ID 102237, 2021.

[25] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and Y. Chen, "Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions," *Accident*

Analysis & Prevention, vol. 148, p. 105837, Article ID 105837, 2020.

[26] B. Kitchenham, R. Pretorius, D. Budgen et al., "Systematic literature reviews in software engineering - a tertiary study," *Information and Software Technology*, vol. 52, no. 8, pp. 792–805, 2010.

[27] D. Tokody, L. Ady, L. F. Hudasi, P. J. Varga, and P. Hell, "Collaborative robotics research: subiko project," *Procedia Manufacturing*, vol. 46, no. 2019, pp. 467–474, 2020.

[28] P. B. de Laat, "Algorithmic decision-making based on machine learning from big data: can transparency restore accountability?" *Philosophy & Technology*, vol. 31, no. 4, pp. 525–541, 2018.

[29] H. S. Lee, Y. Baek, Q. Lin et al., "Efficient defect identification via oxide memristive crossbar array based morphological image processing," *Advanced Intelligent Systems*, vol. 3, no. 2, Article ID 2000202, 2021.

[30] S. I. Shafiq, G. Velez, C. Toro, C. Sanin, and E. Szczerbicki, "Designing intelligent factory: conceptual framework and empirical validation," *Procedia Computer Science*, vol. 96, pp. 1801–1808, 2016.

[31] G. Pereira, R. Prada, and P. A. Santos, "Integrating social power into the decision-making of cognitive agents," *Artificial Intelligence*, vol. 241, pp. 1–44, 2016.

[32] M. Hummer, M. Kunz, M. Netter, L. Fuchs, and G. Pernul, "Adaptive identity and access management-contextual data based policies," *EURASIP Journal on Information Security*, vol. 2016, no. 1, 2016.

[33] Q. Jin and D. Kudeki, "Identity and access management for libraries," *Technical Services Quarterly*, vol. 36, no. 1, pp. 44–60, 2019.

[34] R. H. Kulkarni and P. Padmanabham, "Integration of artificial intelligence activities in software development processes and measuring effectiveness of integration," *IET Software*, vol. 11, no. 1, pp. 18–26, 2017.

[35] D. Irgasheva and S. Rustamova, "Development of role model for computer system security," in *Proceedings of the 2019 International Conference on Information Science and Communications Technologies (ICISCT)*, Tashkent, Uzbekistan, November. 2019.

[36] T. Rausch and S. Dustdar, "Edge intelligence: the convergence of humans, things, and AI," in *Proceedings of the 2019 IEEE Int. Conf. Cloud Eng. IC2E 2019*, no. June, pp. 86–96, Prague, Czech Republic, June 2019.

[37] E. Schoemaker, D. Baslan, B. Pon, and N. Dell, "Identity at the margins: data justice and refugee experiences with digital identity systems in Lebanon, Jordan, and Uganda," *Information Technology for Development*, vol. 27, no. 1, pp. 13–36, 2021.

[38] N. Harth, C. Anagnostopoulos, and D. Pezaros, "Predictive intelligence to the edge: impact on edge analytics," *Evolving Systems*, vol. 9, no. 2, pp. 95–118, 2018.

[39] X. Fan, Q. Chai, L. Xu, and D. Guo, "DIAM-IoT: a decentralized identity and access management framework for internet of things," in *Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure*, pp. 186–191, New York, NY, USA, October 2020.

[40] A. Castiglione, A. De Santis, B. Masucci et al., "Hierarchical and shared access control," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, p. 1, 2015.

[41] A. B. A. Majeed, "Roboethics - making sense of ethical conundrums," *Procedia Computer Science*, vol. 105, no. December 2016, pp. 310–315, 2017.

[42] A. Holzinger, G. Langs, H. Denk, K. Zatloukal, and H. Müller, "Causability and explainability of artificial intelligence in medicine," *WIREs Data Mining and Knowledge Discovery*, vol. 9, no. 4, Article ID e1312, 2019.

[43] K. Mangaroska, R. Martinez-Maldonado, B. Vesin, and D. Gašević, "Challenges and opportunities of multimodal data in human learning: the computer science students' perspective," *Journal of Computer Assisted Learning*, vol. 37, no. 4, pp. 1030–1047, 2021.

[44] C. Anagnostopoulos and K. Kolomvatsos, "Predictive intelligence to the edge through approximate collaborative context reasoning," *Applied Intelligence*, vol. 48, no. 4, pp. 966–991, 2018.

[45] B. Chander and G. Kumaravelan, "Outlier detection strategies for WSNs: a survey," *Journal of King Saud University - Computer and Information Sciences*, 2021.

[46] M. R. Morris, "AI and accessibility," *Communications of the ACM*, vol. 63, no. 6, pp. 35–37, 2020.

[47] L. Ramamoorthi and D. Sarkar, "Single sign-on implementation: leveraging browser storage for handling tabbed browsing sign-outs," in *Smart Innovation, Systems and Technologies*, vol. 152, pp. 15–28, Springer Science and Business Media Deutschland GmbH, Berlin/Heidelberg, Germany, 2020.

[48] M. Kunz, A. Puchta, S. Groll, L. Fuchs, and G. Pernul, "Attribute quality management for dynamic identity and access management," *Journal of Information Security and Applications*, vol. 44, pp. 64–79, 2019.

[49] A. Fatima, Y. Ghazi, M. A. Shibli, and A. G. Abassi, "Towards attribute-centric access control: an ABAC versus RBAC Argument," *Security and Communication Networks*, vol. 9, no. 16, pp. 3152–3166, 2016.

[50] M. J. Haber and D. Rolls, "The identity governance process," in *Identity Attack Vectors*, pp. 51–97, Springer, Berlin/Heidelberg, Germany, 2020.

[51] E. Berman, "Individualized suspicion in the age of big data," *Iowa Law Review*, vol. 105, no. 2, pp. 463–506, 2020, [Online]. Available: http://0-search.proquest.com.mylibrary.qu.edu.qa/scholarly-journals/individualized-suspicion-age-big-data/docview/2381617248/se-2?accountid=13370.

[52] G. Mohindru, K. Mondal, and H. Banka, "Internet of things and data analytics: a current review," *WIREs Data Mining and Knowledge Discovery*, vol. 10, no. 3, Article ID e1341, 2020.

[53] J. Moraros, M. Lemstra, and C. Nwankwo, "Lean interventions in healthcare: do they actually work? a systematic literature review," *International Journal for Quality in Health Care*, vol. 28, no. 2, pp. 150–165, 2016.

[54] M. M. Abdul Jalil, C. P. Ling, N. M. Mohamad Noor, and F. Mohd, "Knowledge representation model for crime analysis," *Procedia Computer Science*, vol. 116, pp. 484–491, 2017.