Review Article

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

Mohammad Kamel Alomari, Habib Ullah Khan, Sulaiman Khan, Alanoud Ali Al-Maadid, Zaki Khalid Abu-Shawish, and Helmi Hammami

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

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]. Mehta 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 confined 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.

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.

<table>
<thead>
<tr>
<th>Research question</th>
<th>Combination of keywords</th>
<th>Relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. How can we enhance the efficiency and effectiveness of the user access and entitlement review process using AI capabilities?</td>
<td>(&quot;Efficiency&quot; OR &quot;effectiveness&quot; OR &quot;user access&quot;) AND (&quot;entitlement review&quot; OR &quot;entitlement&quot;) AND (&quot;artificial intelligence&quot; OR &quot;AI capabilities&quot;)</td>
<td>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</td>
</tr>
<tr>
<td>2. How can we reduce information security risks by generating and leveraging predictive intelligence?</td>
<td>(&quot;Information security risk&quot;) AND (&quot;generating&quot; OR &quot;leveraging&quot;) AND (&quot;predictive intelligence&quot; OR &quot;prediction&quot;)</td>
<td>The need to counter the mounting information security risk with emerging technologies such as predictive modelling is identified</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Database</th>
<th>Date accessed</th>
<th>No. of articles (without filters)</th>
<th>No. of articles (with filters)</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>RQ1</td>
<td>RQ2</td>
<td>RQ1</td>
</tr>
<tr>
<td>Science direct</td>
<td>19.4.2021</td>
<td>2376</td>
<td>88</td>
<td>40</td>
</tr>
<tr>
<td>Wiley online</td>
<td>17.4.2021</td>
<td>5477</td>
<td>4</td>
<td>29</td>
</tr>
<tr>
<td>ProQuest</td>
<td>23.4.2021</td>
<td>117</td>
<td>45</td>
<td>2</td>
</tr>
<tr>
<td>Tandfonline</td>
<td>16.4.2021</td>
<td>25</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Scopus</td>
<td>16.4.2021</td>
<td>162</td>
<td>65</td>
<td>5</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>8157</td>
<td>204</td>
<td>80</td>
</tr>
</tbody>
</table>

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

Figure 3: Inclusion and exclusion criteria followed for this SLR work.
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 4: Number of articles in the proposed SLR protocol.

Figure 5: Database-wise count of articles.
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
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 led 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


