I.J. Modern Education and Computer Science, **2022, 1, 44-55**
Published Online February 2022 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2022.01.04

Artificial Intelligence in Collaborative Information System

Monika Arora
Apeejay School of Management, Dwarka, New Delhi, India
Email: marora.asm@gmail.com

Indira Bhardwaj
Vivekananda School of Business Studies, VIPS, New Delhi, India
Email: indira@dsb.edu.in

Received: 07 February 2021; Revised: 09 March 2021; Accepted: 15 April 2021; Published: 08 February 2022

Abstract: All organizations have a collaborative information system, which is a shared system between employees and teams in the organisation. All such information systems in organizations need to be flawlessly secure. Securing information systems through the latest technologies like Artificial Intelligence, Deep Learning and Blockchain is one of the latest trends in information sciences. This paper tries to explore them in detail through data on user's login time and time spent on the websites along with user actions. The objective is to develop a model that will be used for authentication of the user. This will allow early detection of frauds so that preventive and remedial actions like blocking access to the user can be initiated well in advance. The dataset used to develop this model is the user log data and technique of logistic regression is used to create the regression model for authentication of the user. Logistic regression-based classification is used on the attributes taken to record and analyze entries recorded on the system leading to identification of a cluster based on normal and suspicious users. The accuracy of logistic regression has been analyzed and implemented to secure the collaborative system. This study will help the researcher to implement the AI in the system. It also discusses its future prospects and the disruptive changes in implementation of Information Systems. Finally, the research considers combining blockchain (BC) and deep learning (DL) with Artificial Intelligence (AI) and discusses the revolutionary changes that would result by rapidly advancing the AI field.

Index Terms: AI, Deep Learning, Blockchain, Information System, Security

1. Introduction

Data security has gained momentum in the last few years given the volume of data that gets generated every second. Collaborative security is an abstract concept, where collaboration between different technologies and their compatibility with each other is a significant determinant of their success. Security is often centrally managed and emerging trends such as Artificial Intelligence (AI), Blockchain (BC) and Deep Learning (DL) are used in collaboration to provide high-end security through technology [1]. Implementation of security systems poses challenges related to complexity and compatibility of technologies, sometimes leading to artificial stupidity. Ethical and Legal aspects related to Privacy/Security/Safety of data while implementing Artificial Intelligence (AI), Blockchain (BC) and Deep Learning (DL) are also an increasing cause of concern.

Artificial Neural Networks (ANN) started in the 1950s with the basic programming of machines and it was by the 1990s that the machines had started using explicit programs to evolve their processes and become agile and smart [37]. By the end of the first decade of the 21st Century the concept of Deep Learning had already gained momentum. A collaborative security system recommends the best use of technology such as AI, BC and DL together. Many secure systems offer the security services such as user authentication, use of anti-virus, anti-malware/spyware, intrusion detection etc. The databases used in the organisation and business information can be extracted from these data stores for decision making concerning customer transaction behavior patterns. The organisation is facing increased competition for different reasons, including the user entrance in various applications such as online shopping, banking systems etc. In various online transactions is based on a wide range of offered products and services to the public. As a consequence, the online industry strives to succeed by putting the topic of rapid and changing customer needs on their agenda.

The objectives of corporate security include increased security that leads to gain trust and have better customer response that will improve customer loyalty. The potential areas of application of data-mining techniques are wide. In

