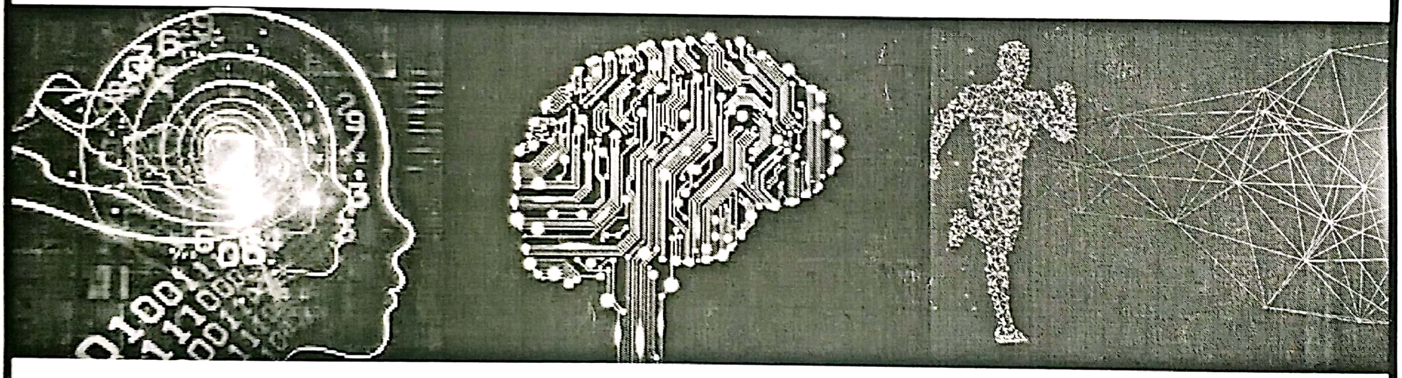
PROCEEDINGS
OF
NATIONAL CONFERENCE
ON
COMPUTATIONAL INTELLIGENCE AND DATA SCIENCE
NCCIDS-23

ISBN:978-93-80544-50-2



ORGANIZED BY

DEPARTMENT OF COMPUTER SCIENCE & APPLICATIONS

IN COLLABORATION WITH

CHAUDHRY RANBIR SINGH INSTITUTE OF SOCIAL & ECONOMIC CHANGE

&

TECHNICAL COLLABORATION WITH

COMPUTER SOCIETY OF INDIA

MAHARSHI DAYANAND UNIVERSITY, ROHTAK - 124001 (HARYANA)
NAAC ACCREDITED 'A+' GRADE STATE UNIVERSITY

www.mdurohtak.ac.in

P-156

IOT SECURITY CHALLENGES AND PROSPECTIVE MEASURES

Dr. Palak[1*], Dr. Preeti Gulia[2], Dr. Satish Kumar[3], Ms. Venu[4]
[1,3]Dept. of Computer Science, Govt. College, Narnaul, Haryana
[3]Dept. of Computer Science and Applications, MDU, Rohtak, Haryana
[4]Dept. of Computer Science, Govt. College, Sector 9, Gurugram, Haryana

Abstract

The large network of interconnected physical items (i.e., things) that share data with other devices and systems online is known as the Internet of Things (IoT). This paper presents the investigation and analysis of the current situation and problems with Internet of Things (IoT) security. The goal of the Internet of Things (IoT) framework is to globally connect everyone and everything. IoT security is a broad word that refers to the plans, instruments, systems, procedures, and techniques employed to safeguard every facet of the internet of things. In order to guarantee the availability, integrity, and confidentiality of IoT ecosystems, physical components, applications, data, and network connections must all be protected. Perceptual, network, and application layers often make up an IoT architecture. A variety of security principles must be implemented at each tier in order to realize a secure IoT. It can only be ensured that the IoT framework's future security issues are addressed and resolved. For the security problems specific to IoT layers and devices, many researchers have worked to develop suitable countermeasures. This article gives a general overview of security ideas, technological issues, and security risks. It also offers potential fixes and a look at the future of IoT security.

Keywords—Internet of things; IoT; Security, Attacks, connectivity.

I. INTRODUCTION

The Internet of Things (IoT) idea entails expanding Internet connectivity to a variety of gadgets and common objects in addition to traditional devices like desktop and laptop computers, smartphones, and tablets. Offering enhanced device, system, and service connectivity that extends beyond machine-to-machine communications and encompasses a range of protocols, domains, and applications is the ultimate goal of the Internet of Things. IoT has quickly expanded to play a significant role in how people live, interact, and conduct business. Web-enabled devices are transforming our universal rights into a larger switched-on space to live in all over the world. Transportation, agriculture, healthcare, and the production and distribution of energy are just a few of the IoT's many application fields. IoT devices employ an identity management tactic to set themselves apart from a collection of connected but disparate devices. With the Internet of Things, an IP address can also define a region, although each entity within a region has a distinct address.

By enabling the intelligent gadgets all around us to perform routine tasks, IoT aims to fundamentally alter the way we live today. The words that are used in relation to IoT include "smart" homes, "smart cities," "smart infrastructure," etc. IoT applications can be found in a wide variety of environments, from private homes to commercial buildings [1]. The consequences of IoT security breaches can be highly damaging. This is because the Internet of Things affects both virtual and physical systems. IoT users can engage with their surroundings thanks to applications in the personal and social domain, and human users can uphold and develop social connections. IoT is being used in the transportation sector to provide safe and convenient transportation options through a variety of smart vehicles, smart infrastructure, and smart traffic signals. The technologies of Radio Frequency Identification (RFID) and Wireless Sensor Networks have allowed IoT applications to advance quickly in recent years (WSN).

The remainder of this article is structured as follows. The three-layer IoT architecture is described in Section II. The security concerns related to various security tenets and the characteristics of IoT devices are described in Section III. The section also discusses the security concerns related to each IoT tier. The research that has recently been done to try and find solutions to the IoT security problems is covered in Section IV. The overview of all the IoT work that has been studied is provided in Section V.

DE GRUYTER

Palak
Book chapter

Requires Authentication Published by De Gruyter 2022

Decision tree–based improved software fault prediction: a computational intelligence approach

From the book Computational Intelligence in Software Modeling

Palak and Preeti Gulia

https://doi.org/10.1515/9783110709247-011

Abstract

Software plays a significant role in our daily lives. The use of smart real-time devices has increased dramatically in the recent decade, necessitating the creation of fault-tolerant, high-reliability software. The basic goal of dependable and robust software is to reduce the quantity of failures that occur when a program is executed. Software fault prediction is a key activity for increasing quality assurance efficiency, economy, and precision. Fault prediction is critical for identifying software components that are prone to flaws. The majority of previous software fault prediction research has concentrated on categorizing software modules whether they are faulty or not. The most important criterion for developing an effective fault prediction model is to identify a dependable fault prediction technique. Due to some inherent constraints, manual techniques of forecasting and finding defects in complex systems may not guarantee a fault-free system, and they are generally time intensive. Computational intelligence (CI) techniques provide promising approaches for solving such problems. In this chapter, we investigate the applications of CI in optimizing various phases of software development. Further, the application of decision tree regression (DTR) for improving fault percentage prediction in different scenarios is the main contribution of this chapter. Two datasets of different sizes from PROMISE repository are extracted and used for performance analysis of the proposed model. The results reveal that DTR generated significant prediction accuracy in intra-release projects.

Conf Proc.
(Book Chap)

Communication and Computing Systems – Prasad et al. (eds)
© 2019 Taylor & Francis Group, London, ISBN 978-0-367-00147-6

ACO and GA based test suite reduction for component based software: A hybrid approach

Palak & Preeti Gulia
Department of Computer Science and Applications, MDU, Rohtak, India

ABSTRACT: The quality of a software application depends on the effectiveness of the testing carried out during development and maintenance phase. Testing is a crucial but time consuming activity that influences the overall cost of software development. Thus a minimal but efficient test suite selection is the need of the hour. This paper presents a hybrid technique based on ACO (Ant Colony Optimization) and GA (Genetic Algorithm) for selection of promising test cases to reduce the overall development cost and time of the application. We took component based software into consideration as they offer some inherent advantages over traditional software development paradigms.

KEYWORDS: Ant Colony Optimization, Genetic Algorithm, Test Case selection, Components

1 INTRODUCTION

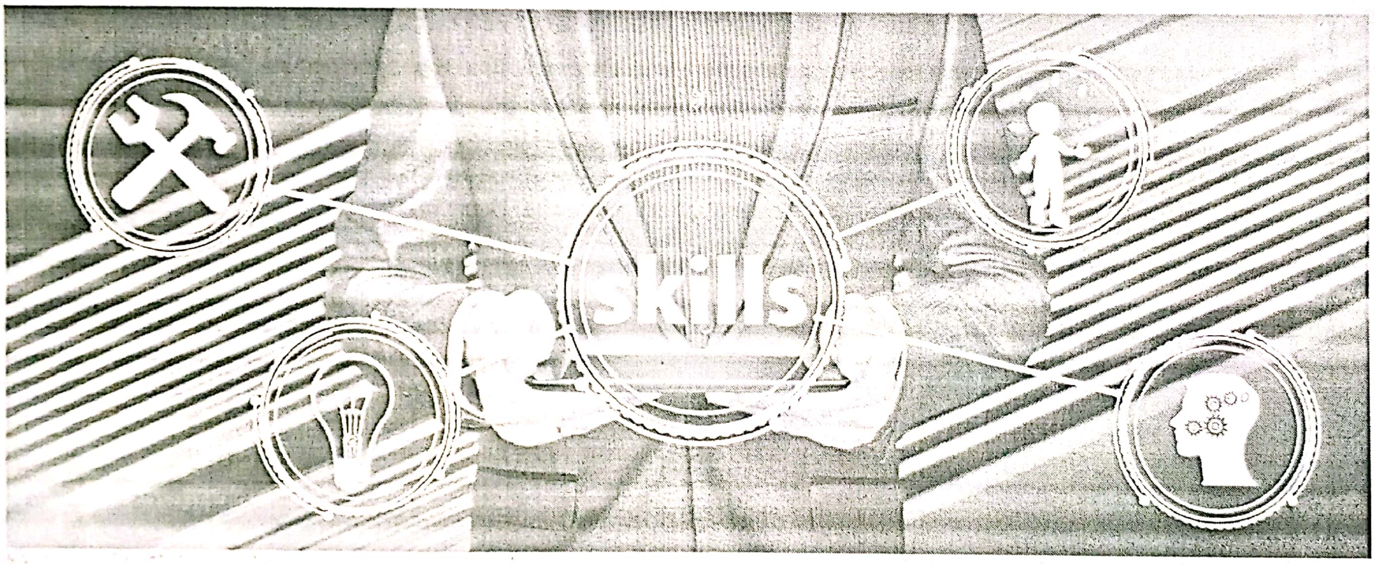
The hardware and software industries are growing together at very fast pace to meet the growing need of smart devices. The smart gadgets have invaded our lives so badly that we can't predict our future without them. The software embedded with these devices play a crucial role to provide best known user experiences to provide the intended functionality. This scenario raises many challenges in front of the software developers to fulfill the quality needs of the end user. Software testing is a crucial and unavoidable step to achieve the same. The role of test cases in the process of testing is very important to verify the functionality and detect faults. A software failure can claim many lives in case of critical systems. Moreover the development paradigms have evolved a long way from traditional procedural approach to a modular component based approach. Component based software engineering (CBSE) (Szyperski, 2002) evolved back in late 1980's and growing since then. It works on the principle of reusability and the software in developed in small chunks called components. Each component has some set of functionality and interacts with other components through interfaces. They provide a black box view of the functionality. Commercial off the shelf (COTS) is gaining popularity with time. Considering the impracticality of the exhaustive testing, it becomes the need of the hour to select a promising suite of test data that is capable of providing higher fault coverage.

Ant Colony Optimization (M. Dorigo et.al., 1999) and Genetic Algorithm (Mitchell et. al., 1996) are search based techniques that are inspired from nature and natural phenomenon. They are meta-heuristic techniques that are problem independent and can work with incomplete knowledge. In contrast to heuristics, meta- heuristics provide randomness during searching and prevent us to get stuck in local optima. We exploited the advantages of both to develop a hybrid approach that is capable of selecting promising test cases to reduce the size of test suite without compromising with the efficiency and test coverage.

Palak

Book Chapter

New Paradigm in Business & Education



EDITORS

Dr. Deepak Gupta

Ms. Payal Jain

NEW PARADIGM IN BUSINESS AND EDUCATION

EDITORS

Dr. Deepak Gupta
Assistant Professor, Dept. of Commerce
Indra Gandhi University, Meerpur, Rewari, Haryana, India

Payal Jain
Assistant Professor, Dept. of English
Pt. Neki Ram Sharma Govt. College, Rohtak, Haryana, India

ISBN No: 978-81-944303-8-4

Published By:
National Press Associates, New Delhi
www.npapublishing.in

ROLE OF BLOCKCHAIN IN EDUCATION SECTOR

Preeti Gulia, Ayushi Chahal, Palak

Dept. of Computer Science & Applications, Maharshi Dayanand University, Rohtak

Abstract

Blockchain is an emerging technology, which is upgrading day by day. It is a digital platform which is disrupting every market. Blockchain is a digital platform which provides a crypto-currency named Bitcoin. Bitcoin is a most famous application of blockchain, which is the most well-known virtual currency world-wide. But now, Blockchain dose not only support the financial sector, it also has deepened its roots in other industries also like healthcare, smart-cities, education etc. Blockchain in the education sector is still very new and unexplored in different areas. Blockchain has considerable amount of potential to completely change conventional education system by providing every facility online. This study discusses different features of Blockchain like trust, data sharing, security, decentralized etc. Blockchain provides decentralized domain, which helps in removing third party involvement in any sort of communication or transaction. This paper presents potential uses for Blockchain technology in the education sector. Blockchain and education system unification could set a very promising trend. Because of its major feature "security", it helps in improving the online education system, by securing the personal data/information of academicians, students, developers, content producers and other employees of education system. In COVID-19 pandemic, only that sector can show their presence to the world which can work online by maintaining social distance. And hence, online education system is widely adopted by students as well as different educational institutes. Online education has become the backbone of education sector which helps it running in this difficult time also. Different application of Blockchain in education system like certification, securing sensitive data, helping in verifying fraudulent degrees etc. are presented in this paper. Blockchain helps in building innovative learning ecosystem for learners which fills the gap in credentialing, copyright protection, and efficient communication.

Keywords: Blockchain, Education technology, healthcare, finance, protection, security.

INTRODUCTION

Blockchain is just a "chain" of "blocks". Here Block is referred as digital information and chain represents public database. So, blockchain is digital information which is stored in a public database.. Blockchain is used to create and store these cryptocurrency electronically using encryption technique.[1]

In blockchain Blocks are made up of three type of information[12]:

Block stores the information like date, time and cost of the transaction.

Block stores information of "who" have participated in the transaction.

Block stores information about their own identities. They store unique hash function which helps in distinguishing between them.

Experiments for blockchain were started on early 1990's but it was introduced in 2008. Blockchain has gained the fame through bitcoin technology. Bitcoin is a cryptocurrency which have existance due to blockchian technology. One can divide Blockchain history in three generation: [6]

First generation: Digital currencies

First existence of Blockchain was as bitcoin. A white paper was released by the name Satoshi Nakamoto from which blockchain gained its popularity. And first well known blockchain is Bitcoin. [2]

Second generation: Smart Contracts