CHAPTER 11

COMPUTER SCIENCE

Doctoral Theses

01. BAJAJ (Deepali) Nee TANEJA (Deepali)
Perspective Model for Microservice Identification Using SDLC Artifacts.
Supervisors: Prof. Anita Goel and Prof. S.C. Gupta
Th 27022

Abstract

Recently applications that require scaling for millions of concurrent users are becoming common. Traditional enterprise applications are generally developed as monolith applications. But, as monolithic systems become complex, they suffer from scalability, agility, and monolithic code to the microservice architectural (MSA) style In MSA applications consist of independent and decentralised services. Each microservices encapsulates a business capability and exposes its capabilities as APIs services in MSA can be independently developed, deployed scaled and managed. Thus, this architecture provides a great deal of advancements over legacy monolithic architectures. However to understand the microservice boundaries is a challenging, time –consuming and error prone task for system engineering. There is a need for new or improvised approaches for microservice identification. Sicnether is an absence of a structured document specifying the artefacts of different phase of SDLC that can be used for microservice identification, it becomes difficult to select a suitable migration .In this thesis, we developed a prescriptive model for identification of microservices based on SDLC artefacts. We also proposed a partial migration approach that reorganizes monolithic codebase into microservices, monolith and serverless model.

Contents

02. DIN (Maiya)
Swarm Intelligence Based Cryptanalysis.
Supervisors: Prof. Sushila Madan and Prof. Sunil Kumar Muttoo
Th 27023

Abstract

The nature inspired computational field is now being popularized as computational swarn intelligence in research communities and gives a new insight in the amalgamation of nature and science. Computaional swarn intelligence has also been used to solve many practical and difficult optimization problems. The past decade has witnessed a lot of interest in developing computational swarn intelligence based techniques for design of crypto primitives and cryptanalysis of various cryptosystems. The present research study introduces some of the theoretical aspects of swarn intelligence and give a description about the various swarn based techniques. Timely interception and decoding/deciphering of secure messages of eavesdroppers like terrorists and naxalites by intelligent requires such type of tools and techniques. The cryptanalytic tools are also requirement of paramilitary forces and department of police. According to this motivation I have purposed swarn intelligence based cryptanalysis techniques and also designed new S-boxes useful for designers of block ciphers. This research work would be useful for researchers working in the field of cryptology and information security. The constructed S-boxes would be useful in designing of novel for defence applications.

Contents

03. DESHMUKH (Sonia) nee Sonia
Mining Process Models Using Evolutionary Approach.
Supervisors: Prof. Naveen Kumar and Dr. Shikha Gupta
Th27263

Abstract

In the automation era, businesses heavily depend on information systems to record transactions and analysing the data from these systems provides valuable insights. Process mining focuses on extracting knowledge from event logs, which are sequences of recorded events during process execution. It aims to discover processes, ensure compliance and improve reference models, and finds applications in various domains including manufacturing, healthcare and information technology, where it improves efficiency detects inefficiencies and enhances security. Process mining techniques analyse event logs to identify derivations, bottlenecks and inefficient loops. Process discovery is a significant aspect of process mining involving creating accurate process models from event logs. The quality of process models is measured using metrics like completeness, preciseness simplicity and generalization. The thesis proposed several algorithms for discovering high quality process models from event logs using evolutionary algorithms, are proposed. Multi objective algorithms allow the discovery of multiple competing process models.

Contents

04. SUBODH KUMAR

Robust Semi-Blind Digital Watermarking Schemes for Images and Electrocardiograms.

Supervisor: Prof. Neeraj Kumar Sharma

Th 26617

Abstract

With the rapid growth of information and communication technologies, digital content is extensively shared over the Internet. This has increased security, authenticity, and copyright concerns. Digital watermarking addresses these concerns by embedding a watermark into the host signal. The quality of a watermarking scheme is assessed based on its characteristics, like imperceptibility, robustness, capacity, computational efficiency, and security. Often, one needs to strike a trade-off between imperceptibility, robustness, and capacity. This thesis is focused on developing improved robust semi-blind watermarking schemes for images and electrocardiograms for applications like telemedicine, copyright protection, and content authentication. Towards our first effort in this direction, we developed a chest X-ray image watermarking scheme (CXRmark) using an online sequential reduced kernel extreme learning machine (OS-RKELM) that achieves improved visual quality and robustness. By segmenting a chest X-ray image into the region of interest (ROI) and the region of non-interest (RONI), we were able to use a variable watermark embedding strength—a higher embedding strength for RONI and a lower embedding strength for ROI. As existing watermarking schemes based on meta-heuristic algorithms are inherently slow, they are unsuitable for real-time applications. Therefore, we have proposed MantaRayWmark, an image adaptive multiple embedding strength (MES)-based watermarking scheme that uses manta ray foraging optimization to optimize the MES locally. We have employed a bidirectional ELM to estimate the MES quickly. We have also developed a CNN-based geometric correction procedure to enhance robustness against geometric attacks. Next, we proposed WSOmark—a dual-purpose color image watermarking scheme that simultaneously embeds a robust and a semi-fragile watermark for copyright protection and tamper localization, respectively. It employed white shark optimizer to locally optimize the MES and the Levenberg-Marqurdt BPNN to quickly estimate the MES. Application of Arnold transform and SVD-based perceptual hashing further improved the security of the watermark. In this thesis, we also worked on watermarking the electrocardiograms. We employed ELM to develop ROSEmark, a semi-blind watermarking scheme for electrocardiograms that achieves improved visual quality and robustness. The use of a randomly generated bit-mask sequence resulted in improved security. Another proposed scheme, HGSmark—an adaptive MES-based watermarking scheme is based on hunger games search meta-heuristic algorithm to optimize the MES locally. Further, the use of Bayesian-regularization BPNN helps in determining the multiple embedding strengths quickly. Through extensive experimentation, we have demonstrated that the proposed watermarking schemes score over their competitors in terms of visual quality, robustness, capacity, security, and time required for watermarking.

Contents

05. SUSHIL KUMAR
Prediction Models for Orthogonal Defect Classification.
Supervisor: Prof. Meera Sharma
Th 26618

Abstract

Predicting the category of software defects is crucial for effective defect management and timely defect resolution. Orthogonal Defect Classification (ODC) is a widely used methodology for classifying software defects based on their characteristics and impact on the system. It provides a structured approach for identifying, categorizing, and analyzing defects, enabling organizations to gain valuable insights into the root causes of software defects. ODC classifies defects into various categories. Each category represents a specific aspect of the defect, allowing for a comprehensive classification scheme. In this research, we proposed prediction models that leverage machine learning and deep learning algorithms in predicting software defect categories as defined within ODC. The proposed defect prediction models have been evaluated and validated using data from various open source projects. The results highlight the potential of machine learning and deep learning approaches in improving defect management and aiding in the efficient resolution of software defects.

Contents

06. VERMA (Vinita)
Malware Detection for Windows Operating System.
Supervisors: Dr. Meera Sharma, Prof. V.B. Singh and Prof. Sunil Kumar Muttoo
Th 27024

Abstract

In the present era of information technology, the use of computers amongst technology devices is very common among students, employees and other people ar work and at home. Computer are commonly used for crating and storing data sending data receiving data using internet connectivity, for entertainment and much more. For desktop computers and laptops, Microsoft windows usually referred to as windows, is the dominantly used operating system (OS). It's large user base windows a popular target of malicious threats. The sources of such threats are intrudes and/or malware. Therefore, it is a dire need to protect windows, indeed data on windows computer systems, from any such threats. The research presented in this thesis brings out techniques for attaining this goal. In this thesis, one of the techniques is to secure sensitive data stored in computer systems from intrudes

who pose security violations via a data branch, in which such data can be accessed with a malicious intent to view, steal ,copy the data, etc. Therefore it is proposed a data hiding techniques to hide such confidential data within digital image files on the system itself to disable a trace of its presence. Concerning the malicious use of data hiding techniques to hide malware within digital media files, a tool is proposed to detect intrusion of such malware into computer systems through image files massively used in cyberspace. A key feature the tool offers is the functionality to output the hidden malicious data making it accessible for analysis.

Contents