+966504321050
Jeddah, Saudi Arabia
Eabozinadah@kau.edu.sa
https://twitter.com/eabozinadah
https://www.linkedin.com/in/e-abozinadah

EHAB ABOZINADAH, P.hD

ACCOMPLISHMENTS

Assistant Professor at Computing and Technology Collage – Vice Dean for Development at e-Learning Deanship – Director for High Performance Computing (HPC) center – King Abdul-Aziz University

Supporting an AI research groups to optimize the benefit of the high-performance computer system on speeding up the data processing for AI models. Also, Moreover, working in many research that focus on Artificial intelligent, Cyber security and Social media mining for building smart detection systems that identify cybercriminal accounts and misleading content to improve security on Social media.

Supervising an AI awareness program, that offering an AI curriculum for all undergraduate program in KAU. Also, participating on smart e-learning research team on KAU that focus on the usability of the massive e-learning data that include the learning styles, students' behavior, and measurable learning outcome on building smart e-learning system.

Specialization: Cyber Security – Artificial Intelligent - NLP – Big Data – Social media Mining – Arabic Stemming - Data Scientist

PROFESSIONAL EXPERIENCE

Director, High performance Supper computing(HPC) center – King Abdul-Aziz University Jeddah, Saudi
(Oct2020 – Present)

Vice Dean of Development, Deanship of e-learning – King Abdul-Aziz University Jeddah, Saudi
(July2018 – Present)

Director, AI curriculums board for undergraduate degree programs– King Abdul-Aziz University Jeddah, Saudi
(Oct2019 – Present)

Duty technical manager, High performance Supper computing center – King Abdul-Aziz University Jeddah, Saudi
(May2018 – Oct2020)

System technical Supervisor, Jeddah Advanced Women Driving School – King Abdul-Aziz University Jeddah, Saudi
(Jan2018 – September 2018)

Assistant Professor of Smart cybersecurity, Computing Collage – King Abdul-Aziz University Jeddah, Saudi
(Jan2018 – Present)

The team Cybercrime Detection Team Leader, Cyber Forensic Lab-George Mason University Fairfax, VA - USA
(June2014 – Dec2017)

- The team was focusing on gathering leaking data from the dark web and identify the cybercriminal network on social media by using machine learning technique to identify the malicious behavior.
- We were analyzing the internet of things devices that do leak information about the user on the web.
- Analyzing the wiped hard drives and building a digital forensic process to figure the applications that was used on the driver.
- Gathered more than million recorded from Twitter.
- Built a customized tool that can Hack twitter data.
- Built Novelty Multidimensional artificial intelligent method that capable of detecting abusive accounts with 90% accuracy rate.

Project Assistant, *Intel-Internship, Hillsboro, OR - USA*

(May2008 – July2008)

- Analyzing the input and the output of the processor
- Testing the performance of innovated processors and reporting the bugs.
- Building low level codes that can mimic human interaction

Data Analysis, *WOU Provost Office-Internship, Monmouth, OR - USA*

(Mar2008 –May2008)

- Analyzing the student record mathematically
- Using pivot tables to constrict different elements on the dataset

Project Member, *WOU Lab Local Network, Monmouth, OR - USA*

(Mar2008 – May2008)

- Building servers that support virtual machines
- Configuring firewalls and security rules
- Implementing backup systems and disaster recovery.

Project Member, *WOU Website Project, Monmouth, OR - USA*

(*Jun2007* –Dec 2007)

- Constricting databases
- DNS configuration
- Designing interfaces

EDUCATION

PhD in Information Technology (Cyber Security-Artificial Intelligent)Dec 2017

- School of Engineering-George Mason University, Fairfax, VA - USA
- Research Focus: Cyber Crime – Big Data – Artificial Intelligence
- **Research Title:**
  DETECTING ABUSIVE ARABIC LANGUAGE TWITTER ACCOUNTS USING A MULTIDIMENSIONAL ANALYSIS MODE

Abstract -- Twitter is one of the most popular social media sources for disseminating news and propaganda in the Middle East. The increased use of social media has motivated spammers to post malicious content on social media sites. Some of these Arabic language spammers use adult content to further the distribution of their malicious activities.

However, the extensive number of users posting adult content in social media degrades the experience for other users for whom the adult content is not desired or appropriate. These accounts would be suspended or terminated from Twitter whenever reported by Twitter's users as Twitter prohibits adult content in an image, a video, or a text. Moreover, some countries have attempted to detect these accounts, but have failed as these accounts use informal Arabic language and misspelled words that cannot be detected using blacklisted keywords.

In this research, I built a model to detect abusive Arabic language Twitter accounts that use obscenity, profanity, or inappropriate words in tweet content. The model is based on a multi-dimensional analysis approach by using independent lexical analysis, social graph analysis, and statistical analysis. Independent lexical analysis approaches are used to overcome the limitation of Arabic language analysis tools for correcting the misspelled words in the tweet, finding the abusive and non-abusive related words, and finding the concept related to the word. Social graph analysis is used to identify the user connectivity relationships on Twitter. Statistical analysis is used to identify the user's tweeting characteristics.

The analysis was based on real data collected from Twitter. The data was manually labeled to support a supervised machine learning technique (Support Vector Machine (SVM)). The constructed model contains 31 distinct features that are formed from profile information, social graph centrality measures, tweet elements' counts, and tweet lexical analysis measures. The model was evaluated against a previously unseen subset of the collected data and achieved 90% average accuracy

Master of Information System ***May 2013***
School of Engineering-George Mason University, Fairfax, VA - USA

Master of Science in Education-Information Technology ***May 2008***
Western Oregon University, Monmouth, OR - USA
Thesis Topic: Virtual Reality

Graduate certificate of E-commerce ***Dec 2015***
School of Engineering-George Mason University, Fairfax, VA - USA

Graduate certificate of Security Assurance ***May 2011***
School of Engineering-George Mason University, Fairfax, VA - USA

Bachelor of Science in Computer Science ***May 2004***
King Abdul Aziz University, Jeddah, Saudi Arabia
Graduation Research Topic: Wireless Networks

PUBLICATION

Focus Areas: Artificial Intelligence System, Machine Learning, Big data, Data Mining, Classification, Language processing, Cyber Criminal network analyst, Social media mining, Security analyst.

A healthcare evaluation system based on automated weighted indicators with cross-indicators based learning approach in terms of energy management and cyber security 2020 IJMI

Abstract -- Hospital performance evaluation is vital in terms of managing hospitals and informing patients about hospital possibilities. Also, it plays a key role in planning essential issues such as electrical energy management and cybersecurity in hospitals. In addition to being able to make this measurement objectively with the help of various indicators, it can become very complicated with the participation of subjective expert thoughts in the process.

Similarity Measures and Distance Measures Applications: A Software Engineering Prospective 2020 SAIS

Abstract -- In this paper, several applications that use similarity and/or distance measures. The review is mainly focusing on the prospective of systems design and analysis (i.e. software requirements analysis, interface design, software maintenance, etc.).

SelecWeb: A Software Tool for Automatic Selection of Web Frameworks 2019 Springer

Abstract -- Web applications and services are fundamental to designing smart infrastructure and cities. Developers often use various development technologies when developing web or cloud applications. One of such major technologies is web frameworks (e.g., Rails, Spring, Django, and CodeIgniter), which permit developers to develop without worrying about the low-level details. Programmers may choose from a variety of web frameworks, and different languages that support them, each with its own strengths and weaknesses. Organizations work in different application domains and have diverse priorities and constraints with regard to the development of applications and services. In this paper, we propose an automatic tool, SelecWeb, for selecting a web framework based on a set of criteria and developer preferences. The set of selection criteria is developed by us and is a contribution of this paper

A Statistical Learning Approach to Detect Abusive Twitter Accounts 2017 ICCDA

Abstract -- The increased use of social media has motivated spammers to post their malicious activities on social network sites. Some of these spammers use adult content to further the distribution of their malicious activities. Moreover, the extensive number of users posting adult content in social media degrades the experience for other users for whom the adult content is not desired or appropriate. In this paper, we aim to detect abusive accounts that post adult content using Arabic language to target Arab speakers. There is limited natural language processing (NLP) resources for the Arabic language, and to the best of our knowledge no research has been done to detect adult accounts with Arabic language in social media. We used a statistical learning approach to analyze Twitter content to detect abusive accounts that use obscenity, profanity, slang, and swearing words in Arabic text format. Our approach achieved a predictive accuracy of 96% and overcomes imitations of the bag-of-word (BOW) approach.

Improved Micro-Blog Classification for Detecting Abusive Accounts 2016 IJDK

Abstract -- The increased use of social media in Arab regions has attracted spammers seeking new victims. Spammers use accounts on Twitter to distribute adult content in Arabic-language tweets, yet this content is prohibited in these countries due to Arabic cultural norms. These spammers succeed in sending targeted spam by exploiting vulnerabilities in content-filtering and internet censorship systems, primarily by using misspelled words to bypass content filters. In this paper we propose an Arabic word correction method to address this vulnerability. Using our approach, we achieve a predictive accuracy of 96.5% for detecting abusive accounts with Arabic tweets.

Evaluating Classifiers in Detecting 419 Scams in Bilingual Cybercriminal 2015 IJCSIS

Abstract -- Incidents of organized cybercrime are rising because of criminals are reaping high financial rewards while incurring low costs to commit crime. As the digital landscape broadens to accommodate more internet-enabled devices and technologies like social media, more cybercriminals who are not native English speakers are invading cyberspace to cash in on quick exploits. In this paper we evaluate the performance of three machine learning classifiers in detecting 419 scams in a bilingual Nigerian cybercriminal community. We use three popular classifiers in text processing namely: Naive Bayes, k-nearest neighbors (IBK) and Support Vector Machines (SVM). The preliminary results on a real world dataset reveal the SVM significantly outperforms Naive Bayes and IBK at 95% confidence level.

Detect Abusive Account in Social Network with Arabic Tweets 2015 ICKD

Abstract -- Twitter is one of the most popular sources for disseminating news and propaganda in the Arab region. Spammers are now creating abusive accounts to distribute adult content in Arabic tweets, which is prohibited by Arabic norms and cultures. Arab governments are facing a massive challenge to detect these accounts. This paper evaluates different machine learning algorithms for detecting abusive accounts with Arabic tweets, using Naïve Bayes (NB), Support Vector Machine (SVM), and Decision Tree (J48) classifiers. We are not aware of another existing data set of abusive accounts with Arabic tweets, and this is the first study to investigate this issue. The data set for this analysis was collected based on the top five Arabic swearing words. The results show that the Naïve Bayes (NB) classifier with 10 tweets and 100 features has the best performance with 90% accuracy rate.

Constructing and Analyzing Criminal Networks 2014 IEEE

Abstract -- Analysis of criminal social graph structures can enable us to gain valuable insights into how these communities are organized. Such as, how large scale and centralized these criminal communities are currently? While these types of analysis have been completed in the past, we wanted to explore how to construct a large scale social graph from a smaller set of leaked data that included only the criminal's email addresses. We begin our analysis by constructing a 43 thousand node social graph from one thousand publicly leaked criminals' email addresses. This is done by locating Facebook profiles that are linked to these same email addresses and scraping the public social graph from these profiles. We then perform a large-scale analysis of this social graph to identify profiles of high rank criminals, criminal organizations and large-scale communities of criminals. Finally, we perform a manual analysis of these profiles that results in the identification of many criminally focused public groups on Facebook. This analysis demonstrates the amount of information that can be gathered by using limited data leaks.

TECHNICAL SKILLS

- Machine Learning
- Cloud computing
- Parallel computing
- Social media mining
- NLP

- Data Mining
- Social Graph analysis
- Python
- Data Analytics
- SQL
- Security +
- Windows Server 2012
- HTML
- MS Project
- C++, C#
- Dreamweaver
- System security (XAML) (RBAC)
- Financial analysis (DPL 7)
- System engineering (SYSML)

COMITTEE

- Director for HPC development committee - KAU
- Director for AI curriculums program for undergraduate program – KAU
- Member for Cyber security research committee – KAU
- Member for Artificial Intelligence research committee – KAU
- Member for AI and COVID-19 research committee – KAU
- Director for E-learning development committee – KAU
- Director for E-learning strategic plan committee – KAU

MEMBERSHIP

- Information System Security Association (ISSA)
- Association of Advance Artificial Intelligence (AAAI)
- European Association of Artificial Intelligence (EurAi)
- Institute of Electrical and Electronic Engineering (IEEE)
- Associate of Computer Machinery (ACM)
- Mason Competitive Cyber (MCC)

AWARD

- SHAMS best e-Learning System 2018
- Saudi Culture Mission Best Research in Arab Cyber Security 2017
- 2015 ICKD Best Research paper in Machine Learning 2015
- 2014 DFDARG Best Smart Cyber Security abstract 2014
- UNIQUe e-learning accreditation 2011