Social Media Data Analysis Trends and Methods

Mahmoud Rokaya[1,2] and Sanaa Al Azwari[1],

[1]Department of Information Technology, College of Computers and Information Technology,
Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia.
[2]Tanta University, Faculty of Science, Tanta, Egypt

Summary
Social media is a window for everyone, individuals, communities, and companies to spread ideas and promote trends and products. With these opportunities, challenges and problems related to security, privacy and rights arose. Also, the data accumulated from social media has become a fertile source for many analytics, inference, and experimentation with new technologies in the field of data science. In this chapter, emphasis will be given to methods of trend analysis, especially ensemble learning methods. Ensemble learning methods embrace the concept of cooperation between different learning methods rather than competition between them. Therefore, in this chapter, we will discuss the most important trends in ensemble learning and their applications in analysing social media data and anticipating the most important future trends.

Keywords:
Social Media, Ensemble Learning, Security Risks, Identity Theft, Fraud, Malware, Adware, Bot, Phishing, Fake, DDoS

1. Introduction

Social media become a part of daily life for most of the world population. This brings a huge of opportunities as well as a tremendous number of security and privacy issues. Ensemble learning is old as the oldness of the human race itself. However, considering ensemble learning in machine learning and deep learning is very young. Taking the experience of many experts to solve a problem is the core idea behind ensemble learning. Also, ensemble learning can be considered for solving problems that have more than one aspect. For example, autonomous driving or security system can be divided into many parts depending on the data type or the target output. Assigning one expert or more to produce the solution corresponding to different types of inputs or outputs is a large field for applying ensemble learning.

2. Social media security and privacy issues

2.1 Tables and Fig.s

Applications, websites, and tools that enables users to develop and distribute their own content are called social media [1]. Virtual networks communities are the computer-based technology where people can create and share their thoughts and ideas [2]. Through Social media tools and internet-based applications, users can quickly build communication contents composed of personal information, photos, videos, and documents. Any device that can reach the internet and has any limited storage and processing capacity can be used as a tool to develop and distribute social media content. PCs, smartphones, and tablets are examples of such tools. The users of social media tools either as developers or followers increases in noticeable rate, for example, 4.62 billion people around the world uses social media resources on daily bases [3]. Social media brings special importance for the users' privacy [4].

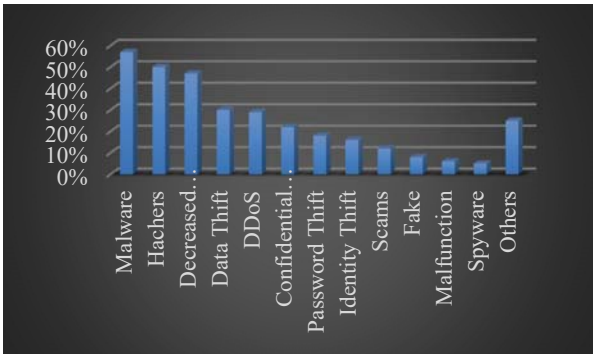

Fig. 1. Types of risks on social media statistics

Source: https://www.securityexecutivecouncil.com/insight/risk-based-security/top-security-risk-to-organizations-today-2021-32402-1432

Users on social media faces many security risks. Fig. 1 shows the distribution of security risks. Malware presents the most common risk. The rate that many users faced data breaches leads many of them to give a real consideration of their privacy and might bring them to carefully reconsider their relationship to the social media. One clear example that bring the privacy issues to be under eye is the scandal of exploiting more than 50 million of accounts for users on Facebook during the American elections 2016 [5]. Social media platforms are the media that the users used to communicate. Most of these platforms belongs to Facebook or a variation like Facebook applications. Fig. 2 shows the percent of users of the most common social media platforms.

Manuscript received September 5, 2022
Manuscript revised September 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.9.48

The public trust in social media become less and less and the users have become wondering their ability to keep and control their own data to be save [6]. The extreme power of businesses and advertisers accessing and using the users posts on social media made more than 80% of users have concerns regarding the rights of these businesses and advertisers to access their data [7].

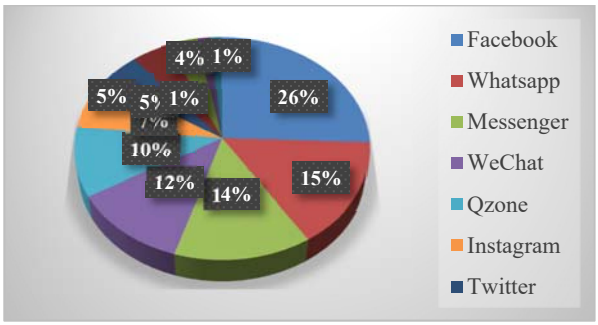

Fig. 2. Social media users' distribution over some social media platforms

Global Social Media Statistics: https://datareportal.com/social-media-users

These risks led to an increase in privacy concerns, which led to advocacy demands to tighten privacy rules and to subject companies working in the field of data exchange to more scrutiny about the protection of personal data. [8]. These concerns and the growing human rights demand to protect personal information have created a growing demand for cybersecurity and artificial intelligence professionals to play a vital role in maintaining privacy in social media work environments, and this undoubtedly requires a professional level and advanced capabilities for those who wish to work in these fields. Every day increasing numbers are joining the social media user's day by day.

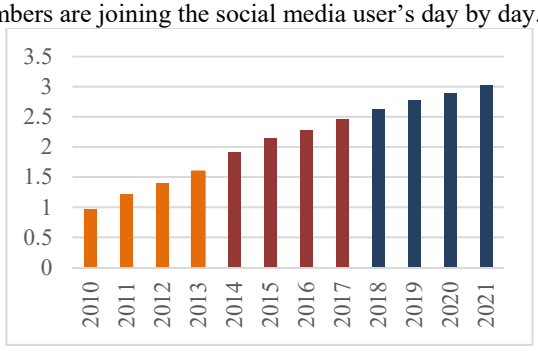

Fig. 3. Growth of user's numbers for social media from 2010 to 2021

Source: https://knowledge4policy.ec.europa.eu/visualisation/number-social-media-users-worldwide-2010-17-forecasts-2021_en

In the last decade the number of users on social media is doubled 6 times from 0.5 billion in 2010 to become 3.5 billion in 2021 and it is expected to increase to include the majority of people population in the few coming years as shown in Fig. 3. Approximately three and a half billion people (45% of the world's population) participate in some form of daily social media exposure and are vulnerable to many risks in several ways [9]. About 13% of Americans have had their social media accounts hacked. These hacks by malicious and unauthorized access to information can harm people through information theft, forced sharing, and directing users to malicious software [10]. Social media platforms that contain vast amounts of information with marginal government oversight are magnets for all criminal actors seeking to use personal information for theft and fraud [11]. The danger does not come from unofficial parties only, but the greater danger may be from government agencies that carry out major attacks at the general level to manipulate opinions in favour of certain parties or a small number of individuals, as happened when the Russian intelligence agency was accused of interfering in social media with the aim of spreading misinformation that provoked public opinion and lost confidence [12].

2.1 Types of Social media threats

In what follows a discussion of the most common attacks and threats on social media will be reported. It is common to classify attacks into two main categories, penetration which include all types of attacks that tries to get illegal benefits from victims through controlling their computing resources, and Denial of Service (DDoS) where the attacker aims to destroy or delay the ability of the victim to serve its customers. However, there is a need to go beyond this traditional categorization as shown below

2.1.1 Theft of personal information and tricking users

Theft of personal information and tricking users into handing over their account information is at the top of what attackers excel at via social media [11]. In many cases, social media platforms share users' information with parties without permission or even the user's knowledge. User information such as name, date of birth, nationality, geographical location, personal interests, as well as user behavior during contacting social media are often stored, processed, and used to better targeting advertisements to users. This opens the door to all methods of data analysis, whether the purpose is good or bad, to get everything possible through the mining of user data. Therefore, data mining methods and the related areas of machine learning, deep learning, and ensemble learning, occupy an advanced position in the areas of protection, fraud, or information hacking on social media platforms [13].

2.1.2 phishing

On social media, users' lack of information is often exploited to fall victim to phishing scams as happened on Instagram phishing when a fake two-factor authentication system was used to trick users into a fake Instagram page. Phishing is one of the most dangerous fraud methods where the user is deceived through email, phone call or text message to lure the user to share sensitive information such as passwords and credit card details [14].

2.1.3 Malware

Malware such as spyware to steal sensitive information and ransomware to extort money and profit through forced advertising through adware poses a serious threat to users of the computer and the Internet in general. Social media platforms are an ideal way to distribute malware. Once a user's device is compromised by phishing, the attacker can take over that account and then distribute the malware to all the user's friends or contacts [15].

2.1.4 Distributed denial of service

When many fake accounts are created that are automatically generated to follow certain accounts or to spread posts on a large scale whenever a particular term is mentioned, a large automated electronic attack is launched to steal accounts, launch distributed denial of service (DDoS) attacks, or create an extensive spam collection. This is done through what is known as bot attacks, which are one of the most powerful means used by cybercriminals to gain access through social media to people's devices and networks [16, 17].
In our discussion related to how machine learning is employed to detect and prevent attacks, we will use more restricted type of classification based on the current direction of research to study these attacks.

3. Ensemble learning

In the recent years, ensemble learning has received special attention in the computational intelligence community. Ensemble learning is as old as human existence itself. Poll the opinion of a group of experts on a particular issue and then combine those opinions to come up with a conclusion that is better than all the individual opinions. Originally, ensemble learning is based on the concept of diversity where the merging process aims to reduce this diversity and thus obtain higher accuracy than that of all experts. Machine learning developed ensemble learning to be used with the goal of creating an automated decision-making system in various applications by sculpting and then integrating several individual decision-making techniques. Ensemble learning is used not only for merging individual experts results but also in many various applications. The effectiveness of ensemble learning has been verified in a variety of real-world applications such as learning concept drift from nonstationary distributions, error correction, incremental learning, confidence estimation, feature selection, missing feature, and class imbalanced data. This part provides an overview of cluster systems and their characteristics and how they can be applied to such a wide range of applications. [18]

3.1 Development of Ensemble Systems

The work of Dasarathi and Sheila in 1979, in which they presented a method for dividing features over a number of classifiers, is perhaps one of the first to be mentioned in the field of ensemble learning [19]. Well-known AdaBoost algorithms were pioneered by constitutive posting theory, which has also been used for ensemble learning in solving multi-layer and regression problems [20, 21]. This was followed by the emergence of many applications of ensemble learning in various fields of machine learning. Random forests (composite classifier systems) [19], mixture of experts (MoE) [22, 23], consensus aggregation [24], combination of multiple classifiers [25-29], stacked generalization [30] and others. The pillars of any ensemble learning are the selection of data, the preparation of individual trainers, and the creation of inclusion rules for group decision-making.
The first step in ensemble learning, in fact, in any machine learning is the data sampling. For ensemble learning data sampling is essential and the diversity is very important as well.

The diversity property can be achieved for any group of trainers through selecting the suitable data sample for each trainer. Different strategies for selecting data samples for achieving diversity led to a different type of ensemble learning. Fig. 4 illustrates how different sampling strategy for each trainer leads to a different type of ensemble learning. For example, the replication strategy leads to what is called bagging ensemble learning, while the reliance on the statistical distribution that separates the classes of the wrongly categorized samples lead to boosting algorithms. Random subspace methods are obtained when each trainer is trained on a different part of the features. [31]. On the other hand, the structure of the individual trainer can be controlled to create the required diversity. For example, the number of hidden layers or the number of components of each layer can be adjusted when using a group of similar type of sub-trainer of the same of neural network type. Also, a number of trainers of heterogeneous types can be used as members of the group. There is no standard definition of diversity scale. [32-34] provided a number of different definitions of the measure of diversity. The diversity scale

is important in ensemble learning. However, the direct relationship between accuracy and diversity is not precisely clear [34, 35].

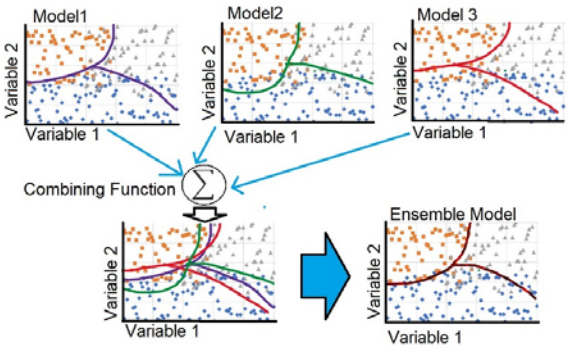

Fig. 4. How ensemble combining function reduce the diversity of individual models

There are several ways to accomplish the second step in ensemble learning is to train the sub-trainers and here there are several methods the most important of which are MOE hierarchy, stack generalization and boosting but bagging (and related algorithms arc-x4 and random forests) remain the most common methods used. [36]

Combining the individual trainers' results is the final step in any ensemble learning methods. Simple or weighted majority voting is suitable for trainers that give discrete-valued label outputs such as support vector machine trainers [36]. Sum, mean and product are examples of arithmetic combines. These combines are suitable for multilayer perceptron [37]. The usual application of these combining methods might be after completing the training step of the individual trainers. However, complex combination requires an additional training step, for example, stacked generalization or hierarchical MoE [38, 39].

4. Ensemble learning application in social media and privacy

In the following subsections, the role of ensemble learning in developing methods in various areas of securing and detecting security risks in social media. The methodology is to divide the security risks to main categories, namely, DDos, Fake new detection, Theft of identity, Adware, Bot, Fraud, Malware and phishing. In each of these areas, the individual learner's combination, the features selections for each individual learners and the combining method will be explored. In the discussion part, the common features selection methods, the most common individual models and the combination methods will be analyzed and discussed.

4.1A DDoS Attack Detection and ensemble learning

A Distributed Denial of Service (DDoS) attack happened when a large capacity of traffics from millions of PCs are targeted to a specific server to crash its system and disrupt its function [16]. Every year, DDoS came at the top of attacks that causes a huge cost to the overall global economy [16]. Most of the method use ensemble learning as a tool for preprocessing of the data to select the optimal features set before feeding these data to the classifiers. For example,

SHAHZEB HAIDER et. al., (2020) developed a detection system for DDoS attack. In their system, same data are passed to different homogenous deep networks composed of similar CNN, RNN an LSTM networks. The results of each network are merged using the function ADD from KERAS. The output of the ADD function and the original data inputs are passed to a classification method to decide if there is a DDoS attack. In this method, ensemble learning is not used to get the final output, it is used as an immediate step to prepare the features prior to the final classification step [40].

Opeyemi Osanaiye et al. (2016) presented an ensemble filtering method for selecting features that can be used to detect DDoS attach. Filtering methods are independent from the classification method and can dramatically accelerate the classification process which in turn highly important in detecting DDoS attack. Namely, Information gain, Gain ratio, Chi-squared and ReliefF were used as four different filtering methods. The whole data are passed to each filter to get the filtered features. The output features of each filter are arranged in one vector to be passed to a decision tree classifier. The objective here is to used ensemble process as a selection feature tool instead of a learning tool [41].

Saikat Das and Frederick T. Sheldon (2020) used intrusion detection benchmark dataset NSL-KDD as the input to 7 different features selection methods to choose the optimal features set. Simple majority voting method was applied to decide a given feature will be among the optimal features set. The seven features selection methods are Pearson's Correlation, Chi-Square, Mutual Information, Recursive Feature Elimination, LASSO Regression, Logistic Regression and Random Forests. The whole data were passed to each method individually to get the filtered features set corresponding to this method. A feature will be among the optimal set of features if the majority of filters include this feature in its selected features. The resulting features were fed to a variety of classifiers including SVM, Logistic Regression, Neural Network, Naïve Bayes and decision trees are used to evaluate the proposed selection method [42].

Few works used the ensemble learning as the main learning tool. For example, to get the higher True Negative

Rate (TNR), (2017) Bin Jia et. al. built an ensemble classifier to detect DDos attach depending on a heuristic detection algorithm based on Singular Value Decomposition (SVD) and a hybrid heterogeneous multi-classifier. The data were split disjoint sets based on selected features and the voting scheme depends on simple majority voting. They claimed that their proposed algorithms can compete other algorithms [43].

4.2 Fake news detection and ensemble learning

Fake news is hard to be detected even for humans Since it is written with the intension of misleading and hoodwink. Fake news is a danger that threats public trust and justice and it is highly important to detect and mitigate fake news [14, 15]. Arvin Hansrajh et. al. (2021) proposed an ensemble learning method to detect fake news in social media. The whole data are fed to each classifier to achieve the training phase. Namely, they used Liar and ISOT data sets to train logistic regression, support vector machine, linear discriminant analysis, stochastic gradient descent, and ridge regression classifiers. The fake news is classified into true or fake news. The ensemble model was built on Blending. Blinding is a variation of stacking. In Stacking, each classifier is trained based to pool the prediction of other classifiers and all classifiers are trained on the whole data. The combine algorithm in Stacking approach learns how to best combine the predictions of the base classifiers while in blending is based on a holdout dataset validation [44].

Iftikhar Ahmad et. al (2021). used three different classifiers using three different data sets then built an ensemble model to detect fake news based on these three individual classifiers. The data sets are ISOT Fake News Dataset, and another two data sets exported from Kaggle. The individual classifiers are Logistic Regression, Support Vector Machine and multilayer perceptron (MLP). To achieve the highest possible accuracy, they used LIWC2015 tool. This tool can extract 93 different features from a given text They extracted the following features function words, punctuation, percentage of words percentage of stop words, percent of words implying positive or negative emotions, informal language; and percentage of certain grammar. The training process for the individual classifiers was repeated several times. In each time different set of features using a grid search to optimize the model for the best outcome. For merging the results, two different voting approaches were used XGBoost and AdaBoost. A k-fold (k = 10) cross validation model was implemented for all ensemble learners [45].

Based on a data set borrowed from Kaggle 2019, Mohammad Zubair Khan and Omar Hussain Alhazmi (2020), developed an ensemble learning model to detect unreliable news based on content acquired. The data were pre-processed through eliminating stop words, deleting single characters and punctuation, lowercasing the whole texts. For each article, a 300- length vector of comma separated vector is presented to be embedded using Doc2Vec borrowed from google. The used individual classifiers are Decision Tree, Naïve Bayes, SVM and Random-Forest. Each classifier was trained based on the whole data set. The applied ensemble strategies are AdaBoost-LinearSVM and AdaBoost-Random Forest were applied to choose the ensemble model with the highest accuracy [46].

For the sake of populating their products, to increase the products sales and to gain more profit, many companies add spam reviews of products. One of the hardest tasks in natural language processing is to detect spam reviews. Muhammad Fayaz et. al. (2020) proposed an ensemble method to classify products reviews into spam and non-spam. In their method, they used Yelp to train the base classifiers. The base classifiers are Random Forest (RF), multilayer perceptron (MLP) and K-Nearest Neighbour (KNN). The data was pre-processed to reduce the number of features to get 25 optimal features. The ensemble mode used the regular voting majority to combine the results of the individual classifiers [47].

4.3 Theft of identity and ensemble learning

Assessing the default customer is one important problem related to theft identity. Depending on personal credit issuance as a data source, Gang Li et. al, (2021) proposed an ensemble classifier for personal credit default discrimination. From Kaggle, they borrowed the UCI database of German, Australia, Japanese, and the GMSC data set. The base learners are logistic regression, SVM and random forest classifiers. Each individual trainers were trained using the whole data. To enhance the accuracy of each trainer a 10-fold scheme was applied during the training of each individual trainer The combining method was done through designing a loss function that depending on the loss of each individual learners and the weights corresponding to each individual trainer's loss was optimized [48].

Since insider has a legitimate privilege to access the system. It will be difficult to detect attacks designed by insiders. Chen Xiaojun et. al. (2013) proposed ensemble method to detect theft through insiders. To determine whether the current operations belong to the real legitimate user or not a re-authentication system that combines the classification of keystroke-classifier and mice-classifier. Data Manipulator is responsible to target the correct data to the correct classifier. In this work two different types of data are collected: Keystroke classifier and mice classifier. A software named KM was designed to collect keyboard and mice events then those events within a fixed time window are calculated to be recorded as one behaviour record. A set

of different classifiers for each type were Assigned to classify the corresponding records. The classical majority voting was used as a combination method [49].

4.4 Adware

Jin-A Choi and Kiho Lim proposed that target advertising is done by firstly identifying the target audience by precisely measuring the best performing platform for advertising; also, low obtrusiveness and personalization upgrading of advertising messages makes marketing efficiencies maximum and improve investment returns. After target identification, the user-centric approach or context-centric approach is used for advertisement. One way of the user-centric approach is behavioral targeting, which takes into account consumers' behavior like searches, visited pages, and links viewed. The other way to apply a user-centric approach is User profiling, which calculates patterns that aid in discovering consumer links likely to be interesting from the consumer perspective. Both these techniques are helpful in enhancing the user experience. The content-centric approach is the second method, in which contextual advertisement is a placement method that uses a machine learning approach to identify whether the advertisement is close to the contents of the page, such as blogs, web docs, and vehicle ads. On the other hand, real-time bidding compels the machine learning method to take rapid action about displaying specific advertisements by obtaining consumers' past history like clicks and searches. The third method is the detection of fraud clicks, which is also done by making the use of machine learning procedures to ensure that the click by the user is felonious or not, i.e., the consumer is really interested in the advertisement or clicking for any other purpose. The efficiency and optimization of this proposed method can be enhanced [50].

4.5 Bot

Silvia Garcia-Méndez et al. [51] published a simulation, modeling, and classification technique to automatically distinguish between benign and malignant contributors as well as between human and non-human (bot) contributors. They used data generation to equalize the classes in experimental data sets. They employed data stream modeling to produce and manage contributor profiles. They found that using a class-balanced data stream made up of both real and fake data considerably increased the confidence and quality of the classifier when tested using the free, public, international wiki travel guide WikiVoyage. According to the researchers' actual data, the suggested method reliably distinguishes between good and bad bots as well as human contributions with an accuracy of up to 92 percent.

4.6 Fraud

Xinke Zhan et al. [52] proposed a novel computation model which detects drug target interaction on a large scale, using target protein sequence information and drug substructure fingerprints; afterward, PSSM will provide a GIST feature vector, which is then provided to RF classifier to get prediction result. The proposed model, when performed on the enzyme, ion channels, GPCRs, and nuclear receptors, yields an average accuracy of 89.20%, 85.93%, 82.36%, and 73.89%.

Sumaya Sanober et al. [53] put forward an Enhanced Secure Deep Learning Algorithm for Fraud Detection in the field of Wireless Communication. The model makes use of the card purchases dataset by European Cardholders in September 2013. The dataset is provided to Auto encode AE, which makes the input data displayed in a smaller representation. An unsupervised learning algorithm AE consists of two main networks, Encoders and Decoders, with backpropagation. Autoencoder will classify the alert as fraudulent or authorized by using the Random Forest (RF) Algorithm of Regression to ensemble optimal alternatives to reduce overfitting [54]. Afterward, KNN is applied to evaluate data. Decision trees like GINI and Split Index are applied to split candidates. Logistic Regression will predict the likelihood of an adjustable goal, which is then inputted to SVM to detect fraud. The proposed system will result in a fraud prevention system in the future.

4.7 Malware

Yakub Kayode Saheed et al. proposed an Intrusions Detection System (IDS) to detect application attacks on the Internet of Things (IoT) [55]. They used the UNSW-SB15 dataset that was issued recently and comprised of up-to-date attack types. In the first step, the min-max concept of normalization feature scaling was made on the dataset to restrict information leakage. After procuring and loading the dataset, Data preprocessing is applied as the first analysis, in which outlier elimination is done, and redundant attributes are excluded. In the next step, PCA is used to carry out dimensionality reduction. The result of normalization is passed as input to the feature selection algorithm PCA. PCA picks ten important components out of forty-nine attributes. In this machine learning-based IDS, security detection tasks are manipulated. Moreover, F1, MCC, and accuracy are calculated to be 99.99% [56].

P Mohan Anand et al. [57] proposed Domain Generation Algorithm (DGA) Detection System using an ensemble approach. To construct the dataset, features were procured from domain names. Prior to earlier versions of DGA, when malware had hardcoded commands and controlled (C C) IP addresses, the proposed DGA followed the traditional cryptographic principles of a Pseudo-random number generator to create a domain names list with whom malware

communicates [57-59]. Lexical and statistical altogether, 44 features were established, and then grouping methods like the random forest, gradient boosting, C 5.0, and CART were utilized to classify DGA Domains in which C 5.0 performed great with the accuracy of 97.04%. Character-based DGA Malware Domain names were classified by this proposed method, but word-based DGAs are still not worked upon.
Yalong Xie et al. [60] proposed a Heterogeneous Ensemble Learning Model Based on Data Distribution (HELMDD), comprised of two steps; resampling Method based on Data Distribution (RMDD) is the first step in which balanced training subsets are formed by making the use of KNN and Kmeans [62]. The heterogeneous ensemble learning model (HELM) is the second step that groups up several classification models into one bagging model. RMDD maintains the classification boundaries and makes the sample information loss low; that is why the recall rate of majority and minority classes is improved. Both the proposed models are beneficial for fraudulent transaction inspection [63].

Ahmed S. Shatnavi et al. [64] submitted a paper for Malware Detection Android based on Hybrid Analysis. Using dynamic and static analysis, features are extracted from the dataset [65, 66]. Features from the static analysis are extracted directly from the source code, while dynamic analysis addresses features that are extracted upon implementation. Feature selection is performed by collecting the features from the pool that improve accuracy and results in complexity reduction. The accuracy results were 94%.

4.8 Phishing

H. S. Hota et al. suggested phishing attacks with remove-replace feature selection (RRFST) by emphasizing making a grouped Machine Learning (ML) [67-69]. RRFST reduces feature space by randomly including features, ensuring accuracy increases or remains unchanged. The classifier uses two decision trees, with final accuracy of 99.27% by 11 features [70-72].

A. Orunsolu et al. [72] proposed a model for phishing detection in which the feature selection module contains the URL features, web document properties, and webpage behavior. These components make a filter that produces a system based on the incremental construction of a component-based system. For an efficient detection approach, these components can be used as unit components and as composite ones. URL feature uses web address characteristics for the retrieval of a particular page from the internet. A classification algorithm does an identity, feature set, and task of determining transaction genuineness. To make a prediction of unknown instances accurately, the algorithm automatically learns based on past or trained experience. To estimate the probabilities of categories, the Naive Base Classifier is an efficient text classification algorithm that uses joint probabilities of words and categories. The support vector machine classifier is a learning algorithm that efficiently categorizes the text. The incremental construction of component-based systems provides an advantage that gives a practical solution for managing scale and complexity in system development. The proposed model was evaluated on NB and SVM classifiers with 2541 phishing pages and 25,000 legitimate pages dataset. The result indicates 99.96 true positives and 99.96 true negatives, and 0.04 False Positive and 0.04 False Negatives. Moreover, the result showed this scheme to be superior to anti-phishing as compared to existing ones. Exploration of this design as a mobile app and design appropriateness investigation in emerging IoT-based phishing attacks can be done in to extend it.

According to research by Qussai Yaseen and Isra'a Abdul Nabi [73], word embedding is crucial for spotting fraudulent emails. To successfully separate spam from authentic emails, they enhanced the BERT (Bidirectional Encoder Representations from Transformers) pre-trained transformer model. The context of the text is explained by BERT using attention levels. They compared their results to a conventional DNN model composed of a Belts (bidirectional long, short-term memory) layer and two stacked dense layers. Additionally, the outcomes were compared to several well-known classifiers, such as k-NN and NB. The second of two open-source data sets, which were also used to train the model, was utilized to assess the model's resilience and durability. Their suggested strategy delivered the most accurate results, with F1 scores of 98.67 and 98.66.

Fig. 5 illustrates the distribution of works using ensemble models in social domain risks. The top risks came from fraud with 32% and the lowest risks came from identity theft with percent 5% then adware with 1%. The individual models used in these works are illustrated in table 1. Most of the works used heterogenous models to guarantee the diversity. The works that used homogenous individual learners tends to use different features schemes to distribute the features for each individual learner. The common combining method is the majority voting or simple weighting scheme or naïve bayes approach.

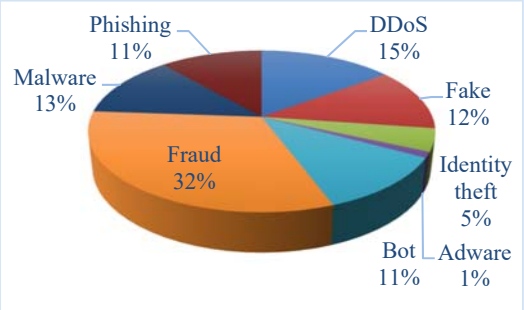

Fig. 5 Distribution of works in social media domain risks

5. Conclusion

In this work a review of ensemble methods used in various social media risks was explored. The common security risks on social media are fraud risk then malware and DDoS. Bot attacks are supposed to be the highest attacks however, ensemble methods were used to solve few percent of Bot attacks. Ensemble-based systems provide intuitive, simple, elegant, and powerful solutions to a variety of social media security problems. The effectiveness of ensemble learning was proved mainly in solving classification problem. Some problems in security include classifying the type of packets in networking routing to decide if they are a part of probable attack. Due to the diversity of features, simple model cannot properly classify such attacks, however, based on the diversity of simple learning models, ensemble models achieved a tangible result in improving the accuracy of detection and preventing attacks especially in DDoS. The most common method in selection of simple methods is random approach, as in bagging, or adopting a dynamically updated distribution, as in boosting. For combining strategies most works depended basically on simple majority voting, sum rule, and weighted majority voting. Using more complex ensemble methods is expected to give more better results. Checking and credibility assessment of news is a promising field for using machine learning techniques especially ensemble learning methods. Based on incremental ensemble learning can be used to check news quality based on time, location and distribution manner of the fake news. Fake new might be the source of all fraud and information theft attacks. So, based on combination of knowledge engineering and artificial intelligence especially deep learning and ensemble learning, fake news detection and other security tools will the most challenging area of research in coming years.

References

[1] Caleb T. Carr & Rebecca A. Hayes (2015) Social Media: Defining, Developing, and Divining, Atlantic Journal of Communication, 23:1, 46-65, DOI: 10.1080/15456870.2015.972282

[2] José Luis Lalueza, Isabel Crespo and Marc Bria, Microcultures, Local Communities, and Virtual Networks, Chapter IX in Handbook of Research on Digital Information Technologies: Innovations, Methods, and Ethical Issues , Copyright: © 2008 |Pages: 14 DOI: 10.4018/978-1-59904-970-0.ch009

[3] Nyagadza, Brighton, and Brighton Nyagadza. “Search Engine Marketing and Social Media Marketing Predictive Trends.” Journal of Digital Media & Policy, 2020. doi:10.1386/jdmp_00027_1.

[4] Ravneet Singh Bhandari1 , Ajay Bansal2, Sanjeela Mathur3 and Harikishni Nain, Privacy Concern Behaviour on Social Media Sites: A Comparative Analysis of Urban and Rural Users, FIIB Business Review, 1-13, 2022, https://doi.org/10.1177%2F23197145221078106

[5] A. Badawy, E. Ferrara and K. Lerman, "Analyzing the Digital Traces of Political Manipulation: The 2016 Russian Interference Twitter Campaign," 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), 2018, pp. 258-265, doi: 10.1109/ASONAM.2018.8508646.

[6] Mingmin Zhang, Ping Xu, Yinjiao Ye, Trust in social media brands and perceived media values: A survey study in China, Computers in Human Behavior, Volume 127, 2022, 107024, ISSN 0747-5632, https://doi.org/10.1016/j.chb.2021.107024.

[7] Dwivedi, Yogesh K., Kawaljeet Kaur Kapoor, and Hsin Chen. "Social media marketing and advertising." The Marketing Review 15.3 (2015): 289-309.

[8] Chris Norval, Heleen Janssen, Jennifer Cobbe and Jatinder Singh, Data protection and tech startups: The needfor attention, support, and scrutiny, Policy Internet. 2021;13:278–299, https://doi.org/10.1002/poi3.255

[9] Jeffrey A. Hall, Dong Liu, Social media use, social displacement, and well-being, Current Opinion in Psychology, Volume 46, 2022, https://doi.org/10.1016/j.copsyc.2022.101339.

[10] Chetioui K, Bah B, Alami AO, Bahnasse A. Overview of Social Engineering Attacks on Social Networks. Procedia Computer Science. 2022 Jan 1;198:656-61. https://doi.org/10.1016/j.procs.2021.12.302

[11] Irshad S, Soomro TR. Identity theft and social media. International Journal of Computer Science and Network Security. 2018 Jan 30;18(1):43-55

[12] Treyger E, Cheravitch J, Cohen R. Russian Disinformation Efforts on Social Media. RAND CORP SANTA MONICA CA; 2022 Jun 7.

[13] Barbier G, Liu H. Data mining in social media. InSocial network data analytics 2011 (pp. 327-352). Springer, Boston, MA.

[14] Tharani JS, Arachchilage NA. Understanding phishers' strategies of mimicking uniform resource locators to leverage phishing attacks: A machine learning approach. Security and Privacy. 2020 Sep;3(5):e120, DOI: 10.1002/spy2.120

[15] Le Page S, Jourdan GV, Bochmann GV, Flood J, Onut IV. Using url shorteners to compare phishing and malware attacks. In2018 APWG Symposium on Electronic Crime Research (eCrime) 2018 May 15 (pp. 1-13). IEEE, DOI: 10.1109/ECRIME.2018.8376215

[16] Kumar S, Carley KM. Understanding DDoS cyber-attacks using social media analytics. In2016 IEEE Conference on Intelligence and Security Informatics (ISI) 2016 Sep 28 (pp. 231-236). IEEE, DOI: 10.1109/ISI.2016.7745480

[17] Derhab A, Alawwad R, Dehwah K, Tariq N, Khan FA, Al-Muhtadi J. Tweet-based bot detection using big data analytics. IEEE Access. 2021 Apr 22;9:65988-6005, DOI: 10.1109/ACCESS.2021.3074953

[18] Zhang C, Ma Y, editors. Ensemble machine learning: methods and applications. Springer Science & Business Media; 2012 Feb 17, https://link.springer.com/content/pdf/10.1007/978-1-4419-9326-7.pdf

[19] B. V. Dasarathy and B. V. Sheela, “Composite classifier system design: concepts and methodology,” Proceedings of the IEEE, vol. 67, no. 5, pp. 708–713, 1979, DOI: 10.1109/PROC.1979.11321

[20] Y. Freund and R. E. Schapire, “Decision-theoretic generalization of on-line learning and an application to boosting,” Journal of Computer and System Sciences, vol. 55, no. 1, pp. 119–139, 1997, https://doi.org/10.1006/jcss.1997.1504
[21] L. Breiman, “Bagging predictors,” Machine Learning, vol. 24, no. 2, pp. 123–140, 1996, https://doi.org/10.1007/BF00058655
[22] Jacobs RA, Jordan MI, Nowlan SJ, Hinton GE. Adaptive mixtures of local experts. Neural computation. 1991 Mar;3(1):79-87, DOI: 10.1162/neco.1991.3.1.79
[23] Jordan MI, Jacobs RA. Hierarchical mixtures of experts and the EM algorithm. Neural computation. 1994 Mar;6(2):181-214, DOI: 10.1162/neco.1994.6.2.181
[24] Benediktsson JA, Swain PH. Consensus theoretic classification methods. IEEE transactions on Systems, Man, and Cybernetics. 1992 Jul;22(4):688-704, DOI: 10.1109/21.156582
[25] Xu L, Krzyzak A, Suen CY. Methods of combining multiple classifiers and their applications to handwriting recognition. IEEE transactions on systems, man, and cybernetics. 1992 May;22(3):418-35, DOI: 10.1109/21.155943
[26] Ho TK, Hull JJ, Srihari SN. Decision combination in multiple classifier systems. IEEE transactions on pattern analysis and machine intelligence. 1994 Jan;16(1):66-75, DOI: 10.1109/34.273716
[27] Rogova, G. (2008). Combining the Results of Several Neural Network Classifiers. In: Yager, R.R., Liu, L. (eds) Classic Works of the Dempster-Shafer Theory of Belief Functions. Studies in Fuzziness and Soft Computing, vol 219. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-44792-4_27
[28] Lam L, Suen CY. Optimal combinations of pattern classifiers. Pattern Recognition Letters. 1995 Sep 1;16(9):945-54, https://doi.org/10.1016/0167-8655(95)00050-Q
[29] Woods K, Kegelmeyer WP, Bowyer K. Combination of multiple classifiers using local accuracy estimates. IEEE transactions on pattern analysis and machine intelligence. 1997 Apr;19(4):405-10, DOI: 10.1109/34.588027
[30] Wolpert DH. Stacked generalization. Neural networks. 1992 Jan 1;5(2):241-59. https://doi.org/10.1016/S0893-6080(05)80023-1
[31] Ho TK. The random subspace method for constructing decision forests. IEEE transactions on pattern analysis and machine intelligence. 1998 Aug;20(8):832-44, DOI: 10.1109/34.709601
[32] Kuncheva LI. Combining pattern classifiers: methods and algorithms. John Wiley & Sons; 2014 Sep 9, https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.365.2334&rep=rep1&type=pdf
[33] Banfield RE, Hall LO, Bowyer KW, Kegelmeyer WP. Ensemble diversity measures and their application to thinning. Information Fusion. 2005 Mar 1;6(1):49-62, https://doi.org/10.1016/j.inffus.2004.04.005
[34] Kuncheva, L.I., Whitaker, C.J. Measures of Diversity in Classifier Ensembles and Their Relationship with the Ensemble Accuracy. Machine Learning 51, 181–207 (2003). https://doi.org/10.1023/A:1022859003006
[35] Kuncheva, L.I. (2003). That Elusive Diversity in Classifier Ensembles. In: Perales, F.J., Campilho, A.J.C., de la Blanca, N.P., Sanfeliu, A. (eds) Pattern Recognition and Image Analysis. IbPRIA 2003. Lecture Notes in Computer Science, vol 2652. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-44871-6_130
[36] Dietterich, T.G. (2000). Ensemble Methods in Machine Learning. In: Multiple Classifier Systems. MCS 2000. Lecture Notes in Computer Science, vol 1857. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45014-9_1
[37] E. Filippi, M. Costa and E. Pasero, "Multi-layer perceptron ensembles for increased performance and fault-tolerance in pattern recognition tasks," Proceedings of 1994 IEEE International Conference on Neural Networks (ICNN'94), 1994, pp. 2901-2906 vol.5, doi: 10.1109/ICNN.1994.374692.
[38] Healey SP, Cohen WB, Yang Z, Brewer CK, Brooks EB, Gorelick N, Hernandez AJ, Huang C, Hughes MJ, Kennedy RE, Loveland TR. Mapping forest change using stacked generalization: An ensemble approach. Remote Sensing of Environment. 2018 Jan 1;204:717-28, https://doi.org/10.1016/j.rse.2017.09.029
[39] Zhang B, Luo L, Liu X, Li J, Chen Z, Zhang W, Wei X, Hao Y, Tsang M, Wang W, Liu Y. DHEN: A Deep and Hierarchical Ensemble Network for Large-Scale Click-Through Rate Prediction. arXiv preprint arXiv:2203.11014. 2022 Mar 11, https://doi.org/10.48550/arXiv.2203.11014
[40] S. Haider et al., "A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks," in IEEE Access, vol. 8, pp. 53972-53983, 2020, doi: 10.1109/ACCESS.2020.2976908.
[41] Osanaiye, O., Cai, H., Choo, KK.R. et al. Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing. J Wireless Com Network 2016, 130 (2016). https://doi.org/10.1186/s13638-016-0623-3
[42] S. Das, D. Venugopal, S. Shiva and F. T. Sheldon, "Empirical Evaluation of the Ensemble Framework for Feature Selection in DDoS Attack," 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), 2020, pp. 56-61, doi: 10.1109/CSCloud-EdgeCom49738.2020.00019.
[43] Jia B, Huang X, Liu R, Ma Y. A DDoS attack detection method based on hybrid heterogeneous multiclassifier ensemble learning. Journal of Electrical and Computer Engineering. 2017 Mar 15;2017, https://doi.org/10.1155/2017/4975343
[44] Hansrajh A, Adeliyi TT, Wing J. Detection of online fake news using blending ensemble learning. Scientific Programming. 2021 Jul 29;2021, https://doi.org/10.1155/2021/3434458
[45] Ahmad I, Yousaf M, Yousaf S, Ahmad MO. Fake news detection using machine learning ensemble methods. Complexity. 2020 Oct 17;2020, https://doi.org/10.1155/2020/8885861
[46] Khan, M.Z., Alhazmi, O.H. Study and analysis of unreliable news based on content acquired using ensemble learning (prevalence of fake news on social media). Int J Syst Assur Eng Manag 11, 145–153 (2020). https://doi.org/10.1007/s13198-020-01016-4
[47] Fayaz M, Khan A, Rahman JU, Alharbi A, Uddin MI, Alouffi B. Ensemble machine learning model for classification of spam product reviews. Complexity. 2020 Dec 18;2020, https://doi.org/10.1155/2020/8857570

[48] Li G, Shen M, Li M, Cheng J. Personal Credit Default Discrimination Model Based on Super Learner Ensemble. Mathematical Problems in Engineering. 2021 Mar 31;2021, https://doi.org/10.1155/2021/5586120
[49] Xiaojun C, Zicheng W, Yiguo P, Jinqiao S. A continuous re-authentication approach using ensemble learning. Procedia Computer Science. 2013 Jan 1;17:870-8, https://doi.org/10.1016/j.procs.2013.05.111
[50] Choi, J. A., & Lim, K. (2020). Identifying machine learning techniques for classification of target advertising. ICT Express, 6(3), 175-180, https://doi.org/10.1016/j.icte.2020.04.012
[51] García-Méndez S, Leal F, Malheiro B, Burguillo-Rial JC, Veloso B, Chis AE, González–Vélez H. Simulation, modelling and classification of wiki contributors: Spotting the good, the bad, and the ugly. Simulation Modelling Practice and Theory. 2022 Nov 1;120:102616, https://doi.org/10.1016/j.simpat.2022.102616
[52] Zhan, X., You, Z., Yu, C., Li, L., & Pan, J. (2020). Ensemble learning prediction of drug-target interactions using GIST descriptor extracted from PSSM-based evolutionary information. BioMed Research International, 2020, https://doi.org/10.1155/2020/4516250
[53] Sanober, S., Alam, I., Pande, S., Arslan, F., Rane, K. P., Singh, B. K., ... & Shabaz, M. (2021). An enhanced secure deep learning algorithm for fraud detection in wireless communication. Wireless Communications and Mobile Computing, 2021, https://doi.org/10.1155/2021/6079582
[54] Mao, Z., Fang, Z., Li, M., & Fan, Y. (2022). EvadeRL: Evading PDF Malware Classifiers with Deep Reinforcement Learning. Security and Communication Networks, 2022, https://doi.org/10.1155/2022/7218800
[55] Anand, P. M., Kumar, T. G., & Charan, P. S. (2020). An ensemble approach for algorithmically generated domain name detection using statistical and lexical analysis. Procedia Computer Science, 171, 1129-1136, https://doi.org/10.1016/j.procs.2020.04.121
[56] Chen, Y., Chen, H., Zhang, Y., Han, M., Siddula, M., & Cai, Z. (2022). A survey on blockchain systems: Attacks, defenses, and privacy preservation. High-Confidence Computing, 2(2), 100048, https://doi.org/10.1016/j.hcc.2021.100048
[57] Saheed, Y. K., Abiodun, A. I., Misra, S., Holone, M. K., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. Alexandria Engineering Journal, 61(12), 9395-9409, https://doi.org/10.1016/j.aej.2022.02.063
[58] Bijalwan, A., Chand, N., Pilli, E. S., & Krishna, C. R. (2016). Botnet analysis using ensemble classifier. Perspectives in Science, 8, 502-504, https://doi.org/10.1016/j.pisc.2016.05.008
[59] Tebenkov, E., & Prokhorov, I. (2021). Machine learning algorithms for teaching AI chat bots. Procedia Computer Science, 190, 735-744, https://doi.org/10.1016/j.procs.2021.06.086
[60] Suchacka, G., Cabri, A., Rovetta, S., & Masulli, F. (2021). Efficient on-the-fly Web bot detection. Knowledge-Based Systems, 223, 107074, https://doi.org/10.1016/j.knosys.2021.107074
[61] Xie, Y., Li, A., Gao, L., & Liu, Z. (2021). A heterogeneous ensemble learning model based on data distribution for credit card fraud detection. Wireless Communications and Mobile Computing, 2021, https://doi.org/10.1155/2021/2531210
[62] Yan, J., Qi, Y., & Rao, Q. (2018). Detecting malware with an ensemble method based on deep neural network. Security and Communication Networks, 2018, https://doi.org/10.1155/2018/7247095
[63] Xu, H., Fan, G., & Song, Y. (2022). Application Analysis of the Machine Learning Fusion Model in Building a Financial Fraud Prediction Model. Security and Communication Networks, 2022, https://doi.org/10.1155/2022/8402329
[64] Shatnawi, A. S., Jaradat, A., Yaseen, T. B., Taqieddin, E., Al-Ayyoub, M., & Mustafa, D. (2022). An Android Malware Detection Leveraging Machine Learning. Wireless Communications and Mobile Computing, 2022, https://doi.org/10.1155/2022/1830201
[65] Martín, I., Hernández, J. A., Muñoz, A., & Guzmán, A. (2018). Android malware characterization using metadata and machine learning techniques. Security and Communication Networks, 2018, https://doi.org/10.1155/2018/5749481
[66] Xiao, F., Lin, Z., Sun, Y., & Ma, Y. (2019). Malware detection based on deep learning of behavior graphs. Mathematical Problems in Engineering, 2019, https://doi.org/10.1155/2019/8195395
[67] Gera, T., Singh, J., Mehbodniya, A., Webber, J. L., Shabaz, M., & Thakur, D. (2021). Dominant feature selection and machine learning-based hybrid approach to analyze android ransomware. Security and Communication Networks, 2021, https://doi.org/10.1155/2021/7035233
[68] Park, S., & Choi, J. Y. (2020). Malware detection in self-driving vehicles using machine learning algorithms. Journal of advanced transportation, 2020, https://doi.org/10.1155/2020/3035741
[69] Lu, T., Du, Y., Ouyang, L., Chen, Q., & Wang, X. (2020). Android malware detection based on a hybrid deep learning model. Security and Communication Networks, 2020, https://doi.org/10.1155/2020/8863617
[70] Subasi, A., Balfaqih, M., Balfagih, Z., & Alfawwaz, K. (2021). A Comparative Evaluation of Ensemble Classifiers for Malicious Webpage Detection. Procedia Computer Science, 194, 272-279, https://doi.org/10.1016/j.procs.2021.10.082
[71] Hota, H. S., Shrivas, A. K., & Hota, R. (2018). An ensemble model for detecting phishing attack with proposed remove-replace feature selection technique. Procedia computer science, 132, 900-907, https://doi.org/10.1016/j.procs.2018.05.103
[72] Orunsolu AA, Sodiya AS, Akinwale AT. A predictive model for phishing detection. Journal of King Saud University-Computer and Information Sciences. 2019 Dec 24, https://doi.org/10.1016/j.jksuci.2019.12.005
[73] AbdulNabi, I., & Yaseen, Q. (2021). Spam email detection using deep learning techniques. Procedia Computer Science, 184, 853–858, https://doi.org/10.1016/j.procs.2021.03.107

Mahmoud B. Rokaya was born in Tanta city, Egypt in 1971. He received the B. S and M.S. degrees in mathematics from Tanta University, Egypt in 2003 and the Doctor of Engineering in information science From Tokushima University, Japan in 2009. From 1997 to 2003, he was assistant of teaching in department of mathematics, Tanta University, Egypt. From 2003 to 2009, he was a researcher in the advanced engineering institute, Tokushima University, Japan. Since 2009-2020, he was assistant professor in information technology, Taif University, KSA. Currently, he is associate professor in informatics, Taif University. His research interests related to AI, information retrieval, natural language processing and data science. Dr. Rokaya was a recipient of the outstanding in scientific research from Taif University for 5 subsequent years from 2010 to 2016. He also was the chair of the committee that got the ABET accreditation in the college of computers and information technology, Taif University, KSA from 2018 to 2025.

Sana Al Azwari received her PhD degree in Computer and Information Sciences in June 2016 from the University of Strathclyde, UK. She also completed her master's degree in computer and Internet Technologies in 2010 from the University of Strathclyde, UK. She is an associate professor and the vice dean of the Computer and Information Technology College at Taif University. Her research focuses on minimizing the number of updates (deltas) necessary for updating Semantic Web data. This work leads to the introduction of a new updating method that exploits implicit information to produce sound and small in size deltas, which are both important properties for a sufficient delta. Dr. AL Azwari won the best paper Award in SEMANTiCS15 in Vienna and the best paper Award in the 8th Saudi Conference in London. During her PhD studies she won a number of prizes for the Best Student Award from the Saudi Cultural Bureau in London. Before that, in 2006, she awarded the King Abdulaziz and His Companions Foundation for the Gifted Award. She is now an International Science Ambassador for the University of Strathclyde.