Situation-Aware Deep Reinforcement Learning Link Prediction Model for Evolving Criminal Networks

Marcus Lim 1, Azween Abdullah 1, NZ Jhanjhi 1 and Muhammad Khurram Khan 2
1School of Computing and IT (SoCIT), Taylor’s University, Malaysia; infinity3098@gmail.com
2Center of Excellence in Information Assurance, King Saud University, Kingdom of Saudi Arabia; mkhurram@ksu.edu.sa

Corresponding Author: noorzaman.jhanjhi@taylors.edu.my;

ABSTRACT Evidently, criminal network activities have shown an increasing trend in terms of complexity and frequency, particularly with the advent of social media and modern telecommunication systems. In these circumstances, law enforcement agencies have to be armed with advance criminal network analysis (CNA) tools capable of uncovering with speed, probable key hidden relationships (links/edges) and players (nodes) in order to anticipate, undermine and cripple organised crime syndicates and activities. The development of link prediction models for network orientated domains is based on Social Network Analysis (SNA) methods and models. The key objective of this research is to develop a link prediction model that incorporates a fusion of metadata (i.e. environment data sources such as arrest warrants, judicial judgement, wiretap records and police station proximity) with a time-evolving criminal dataset in order to be aware of real-world situations to improve the quality of link prediction. Based on the review of related work, most of the models are constructed by leveraging on classical machine learning (ML) techniques such as support vector machine (SVM) without metadata fusion. The problem with the use of classical ML techniques is the lack of available domain dataset which is sufficiently large for training purpose. Compared to social network, criminal network dataset by nature tends to relatively much smaller. In view of this, deep reinforcement learning (DRL) technique which could improve the training of models with the self-generated dataset is leveraged upon to construct the model. In this research, a purely time-evolving DRL model (TDRL-CNA) without metadata fusion is designed as a baseline for comparison with the metadata fusion model (FDRL-CNA). The experimental results show that the predictive accuracy of new and recurrent links by the FDRL-CNA model is higher than the baseline TDRL-CNA model that does not factor data fusion from different data sources.

INDEX TERMS Data Fusion, Time-evolving network, Criminal Network Analysis, Deep reinforcement Learning, Node similarity.

I. INTRODUCTION
Syndicated criminal activities usually involve key leaders (actors) who coordinate their members in expanding their network to carry out their unlawful operations in a stealthy and coherent manner [1]. Social Network Analysis (SNA) is a well-recognised technique applied on such criminal syndicates to uncover the key actors and relationships between them from the network topological configurations [2,3]. SNA incorporates the knowledge from the field of graph theory, network analysis and social science [4] from which the development of SNA methodologies was pioneered. Graph analysis is based on the graph theory constructs, methods and techniques. The SNA tools and techniques which incorporate graph theory, analytical methods and visualisation applications, are developed to perform the analysis of social networks and other domains which can be modelled in a network structure [5]. The CNA methodologies are usually developed by adapting models and metrics from the field of SNA [6]. A number of social media networks, such as Wechat and Facebook, refer friends of similar interests based on the link prediction techniques of SNA models [7].

In CNA, the topological structures, environmental variables and parameters that influence the evolution of links or relationships between actors within the network need to be considered [8]. Environmental factors referred to as metadata such as criminal convictions, arrest warrants, wiretap records and juvenile crime rates within the community (Fig.1), provide additional information on the domain network data which influence the change in network characteristics over time [9].

In particular, criminal networks display a high probability of having hidden or missing links due to the characteristics of criminal activities which tend to operate covertly and with stealth [10]. This characteristics of criminal networks is usually caused by the captured data...
being incomplete, entered inconsistently or wrongly, either intentionally by the criminals or due to human error during the law enforcement process [11]. As a result, the usual practices and methods of predicting probable links (edges) that may or may not exist between the nodes in social networks are pertinent and crucial to the identification of hidden or missing relationships in criminal networks (Fig.1).

A. STRUCTURE OF PAPER
This paper is organised as follows: In Section II, the related works in the field of a time-evolving criminal network, DRL and the influence of factoring in metadata fusion are reviewed. In Section III, the models were developed to compare the performance of the models are described. In Section IV, which is the experimental set-up, characteristics of the dataset and experimental results are explained. Section V summarises the conclusion of the research, and Section VI provides the direction for future work.

B. DATASET
The Caviar drug import syndicate dataset from UCINET [30], contains the historical evolution of a criminal network over a 2-year period involving 11 arrest operations where imported drugs were seized. The number of active nodes at the end of the 2-year period is 110.

II. RELATED WORK
In research conducted by Budur et al. [12], a link prediction model was developed using SNA metrics and leveraging on ML to predict hidden links in criminal networks. The ML techniques there were used were the GBM supervised learning model to improve the accuracy in the prediction of a hidden link of a large dataset. The experiment used a dataset with about 1.5 million nodes and 4 million edges which were at a scale of a thousand times larger in size than other samples used in prior research works. A large dataset was used as it was expected to precisely reflect real-world properties of criminal syndicates. The large dataset used in the experiment managed to enhance the performance of the trained gradient boosting machine(GBM) model in this research, as evidenced by the improvement in the predictive accuracy of the links by the model which achieved a higher scoring of the area under curve (AUC) metric. However, the research methodology had some limitations as the dataset was a snapshot of a specific timestamp. Therefore, the dataset was not fully representative of the real-world criminal networks, which evolve over time [19,20].

Berlusconi et al. [21] proposed a method of identifying the probable hidden links between key players (actors) in the Italian mafia network. In their research, the individuals denoted as nodes are found to be related by analysing the frequency of telephone calls between them. Three sub-networks were investigated which are wiretap record, arrest warrant and judicial judgement networks. The strength of the links between actors in the wiretap record network is found to be in proportion to the frequency of telephone calls made. The arrest warrant network is
formulated from the wiretap record network and the judicial judgement network is formulated from the arrest warrant network. These networks are derived by eliminating the links between criminals if the frequency of telephone calls is insignificant. The link was eliminated as it indicates insignificant betweenness of node pair in the network. This means that the presence of these links have minimal impact in the link prediction model as the respective nodes are found to be related indirectly in some other way.

A definitive milestone was achieved in the research work by Silver et al. when a program they developed know as AlphaGo, with DRL and Monte Carlo Tree Search (MCTS) algorithm, replicated human cognitive intuition and super intelligence in mastering the ancient strategic game of Go[22]. The game of Go is considered a holy grail of artificial intelligence (AI) as the possible permutation of moves are more than the number of atoms in the observable universe. AlphaGo exhibited extraordinary cognitive capability by overcoming the world’s top-ranking Go grandmaster in 2017 with a dominating result.

Anthony et al. [23] combined imitation learning techniques into the MCTS function within the RL model to optimise the RL algorithm to play Hex, a board game with perfect information. Research work by the team was conducted with reference to the definitive work on DRL by Silver et al. and supported the application of DRL in the advancement of artificial general intelligence (AGI).

Silver et al. contributed in a far-reaching way to the development of AGI when they subsequently developed AlphaGo Zero. AlphaGo Zero was not only able to self-learn by playing against a version of itself but was able to master other board games such as Chess and Shogi [24] after being provided with just the basic legal moves of the games. This achievement had reduced the reliance on specific human hand-crafted domain-related patterns in the construction of ML models.

AlphaGo Zero trained itself with a self-generated dataset simulated over 3 days and was able to defeat AlphaGo. DRL incorporates neural networks which usually rely heavily on the availability of large dataset in order to achieve more precise representation learning. Therefore, the DRL technique has various possible applications in other domains where large datasets are not available to train ML models to achieve an acceptable level of accuracy.

The review of the research journals seems to indicate little evidence that the combination of DRL and metadata fusion methods have been investigated in the development of ML models for the prediction of links in evolving criminal networks. In this research work, the investigation and experiments were conducted to address the gaps by constructing a DRL link prediction model trained on an evolving criminal network dataset with metadata fusion. The proposed model was expected to perform better than classical ML models in terms of predictive accuracy.

![Proposed FDRL-CNA link prediction model with SNA and metadata metrics](image-url)
III. MODELS AND METHODOLOGY

A. PROPOSED FDRL-CNA MODEL

The proposed metadata fusion DRL link prediction criminal network analysis model (FDRL-CNA) (Fig. 2), which is constructed with reference to the work conducted by Marcus Lim et al. on criminal network link prediction [25], incorporates the MCTS algorithm.

Notes (Fig. 2):

[a] The feature matrix formulated from the SNA metrics is extracted from the criminal network dataset.

[b] Feature extraction of metadata to formulate the metadata feature matrix.

[c] The SNA link prediction which features a matrix of the criminal network dataset, is processed by the value network.

[d] The feature matrix extracted from metadata sources such as the number of wiretaps, arrest warrants and judicial judgement are processed by the metadata fusion neural net.

[e] The neural net SNA function approximator computes the node pairs with the highest likelihood of link formation.

[f] The SNA link predictions metrics such as the Katz index and Rooted Pagerank is factored both as weights in the value network and into the metadata fusion formulation process.

[g] The metadata feature matrix is factored into the Metadata fusion formulation process by the metadata fusion neural net.

[h] The Monte-Carlo Tree Search (MCTS) initiated the link prediction simulation process on the node-pairs ranked by the highest probability of hidden links ($P_0$, $P_1$) computed by the both the SNA Function Approximator and Metadata Fusion Neural Net.

[i] The criminal network states simulated, $S_0$ to $S_N$, represents the predicted rollout of network instances based on the predicted links between node pairs. The simulated network instances are compared with the 10 sets of test dataset ($T_1$ to $T_{10}$) to determine the predictive accuracy.

[j] The result of link prediction from the prior instance of iteration is fed back to the RL agent to calibrate the hyper-parameters of both the SNA Function Approximator and Metadata Fusion Neural Net to achieve better accuracy in subsequent link prediction.

[k] Representation learning of metadata feature matrix such as the number of wiretaps, arrest warrants and judicial judgements is formulated as weights for the Metadata Fusion Neural Net.

[l] The performance indices derived from the evaluation against the 10 sets of test dataset ($T_1$ to $T_{10}$) are feedback to calibrate the hyper-parameters of the value network.

The DRL technique involves incorporating the ML techniques of DL (multilayered neural networks) and RL. The integration of DL will have an impact on the performance of the link prediction model as it is dependent on a few factors such as optimising the use of graphics processing unit (GPU) and parallel processing. The accuracy of the DRL-CNA model in the prediction of links is evaluated using the AUC scores [26].

The value network of the DRL-CNA model (neural net function approximator) (Fig.2) is a DNN with weights formulated from SNA metrics which are represented as probability distributions over node pairs and edges. In representation learning of the metadata feature matrix, the number of wiretaps, arrest warrants and judicial judgement are formulated as the weights for the metadata fusion neural network. The formulation process of data fusion weighted edges will compute the neural network output values which will rank node pairs on the basis of the probability of links being formed. The MCTS search is initiated from the node pair with the highest combined weights estimated from the value network and metadata fusion neural net. The aggregated scores of the RL agent from every simulation of network instance are then applied to calibrate the hyper-parameters of the DRL model to achieve a better predictive accuracy (Fig. 3).

FIGURE 3. The methodology of proposed FDRL-CNA link prediction model construction with SNA and metadata metrics
The link prediction problem of identifying the probable existence or disappearance of edges between the nodes are usually computed as a binary classification problem using supervised ML technique. In this research, the feature matrix formulated from the metrics of SNA models, computed based on each node pair and the topology of the network, are input into the DRL model for link prediction for training purposes.

**B. METHODOLOGY**

The features matrix formulated from SNA metrics based on the topology of a network dataset were processed by the RL policy network to compute the score during the link prediction process in the simulation of each instance of the network. The SNA metrics identified for the feature matrix formulation includes common neighbour, Adamic-Adar, Jaccard, Katz and random-walk indices [27]. For each node pair, the SNA metrics is computed as an array of features and stored as a data record. This feature matrix is then used to train the neural net to identify the edges of node pairs as a binary class of either positive or negative labels. The edge which exists between the nodes is labelled as positive, and it is labelled as negative if it is found to be non-existent.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common neighbour</td>
<td>$S_{xy} =</td>
</tr>
<tr>
<td>Jaccard Index</td>
<td>$S_{xy} = \frac{</td>
</tr>
<tr>
<td>Hub Index</td>
<td>$S_{xy} = \frac{</td>
</tr>
<tr>
<td>Preferential Attachment index</td>
<td>$S_{xy} = k_x \times k_y$</td>
</tr>
<tr>
<td>Adamic-Adar Index</td>
<td>$S_{xy} = \sum_{z \in \varphi(x) \cap \varphi(y)} \frac{1}{\log k_z}$</td>
</tr>
<tr>
<td>Katz</td>
<td>$S_{xy} = \sum_{t \in \varphi(x) \cap \varphi(y)} \beta^t \cdot S_{w^t}$</td>
</tr>
</tbody>
</table>

The formulation of the feature matrix is derived from the SNA link prediction metrics (Table I) for every node pair and edge of a network where $\varphi(i)$ is the nodes of a network which are neighbours of node $i$. $k_i$ is the degree in respective to each node $i$. $n_{ij}^{(t)}$ is the number of walks of length $t$ node-pairs $i$ and $j$. $\beta$ is the discount factor computed on the walks of a longer length.

At the training stage of the DRL model, a dataset is generated by the link prediction algorithm where each array of features indicates either the existence of an edge between a node pair or the absence of an edge. The features array comprises of the SNA link prediction metrics computed for each node pair. As the training model is constructed from the binary classified feature matrix, the class label will indicate the existence or non-existence of an edge between the nodes. At the testing stage, each sample node pair used is computed as an array with multiple SNA feature metrics, from which the model will predict the existence of an edge (Fig. 3).

During the MCTS network traversal process, each probable link formation between the nodes simulated by the policy network will generate an instance of the network. The MCTS process initiated at the root node represents the initial network state, $S_0$, and the traversal to the following node, guided by the likelihood of a positive or negative link formation, represents the simulation of the subsequent network state.

The probable prediction of a new link from the current state, $S_1$ to $S_2$, corresponds to an RL agent’s action traversing to $S_2$ from $S_1$ in accordance with the default policy. The generation of the new network instance after each simulation of a probable link formation is guided by the highest-ranking scores calculated from SNA link prediction metrics. On each completion of a simulation process, each simulated network state is compared with the actual network to ascertain the predictive accuracy of the model. Any errors detected from the comparison is then processed by a loss function to calibrate the hyper-parameters of the value and policy network to improve the predictive accuracy of the link prediction model. The hyper-parameters that have been calibrated will be factored in the next network state simulation in the link prediction process by means of self-simulation (Fig. 2).

The predictive accuracy of link prediction models constructed on the classical supervised ML and DRL techniques are assessed by comparing the AUC metric of each model. The AUC metric of the link prediction model is indicative of the predictive accuracy of each ML model with a value that ranges from 0 to 1. A model with a higher AUC metric will produce a more accurate prediction.

**C. TIME-EVOLVING GRAPH**

For the purpose of this research, the proposed FDRL-CNA model and the baseline time-evolving DRL link prediction criminal network analysis (TDRL-CNA) model incorporated the concepts of the Rooted PageRank [26] where the node pairs are sorted on the basis of the weights computed according to the time that elapsed at the current instance, $t$, of the network topology and the instance at the time of prediction, $t'$. If nodes $x$ and $y$ are neighbours, with $z$ being any node that may exist between the two nodes, then the probability of the walk going from $x$ to $y$ can be denoted as follows [28]:

$$P(x, y) = (1 - \alpha) \sum_{z \in \varphi(x)} \frac{w(x, y)}{w(x, z)} + \alpha \begin{cases} 1 & \text{if } y \text{ is the central node} \\ 0 & \text{otherwise} \end{cases}$$ (1)
The time dimension is factored as a weight in Rooted PageRank with the time elapsed as a probability proportional to the distance between a node pair. The time-evolving graph can be used to model the dynamic nature of social groups, such as social media or criminal networks, whose structure varies over time [28]. Each individual, represented by a node, may join or leave the network at any point of time. At the same time, each relationship represented by an edge may increase or decrease in strength. In a majority of network growth models, global properties are represented but not specific local properties, such as which individual will be connected to another over time. In the link prediction for an evolving criminal network, the objective is to identify probable future edges at time \( t' (t' > t) \) that might emerge from the snapshot of the network at time \( t \). The link prediction problem for a given instance of a network at time \( t \), \( G_t = (V, E_t) \), where \( V \) represents the nodes in existence across all-time series and \( E_t \) represents the edges at time \( t \). The objective is to predict the most likely edges to arise in the next time step, \( t' \).

D. METADATA FUSION
Metadata fusion is an evolving technology related to the technique of how to fuse multiple data sources obtained from the variables and parameters of the environment, which may influence the change in the attributes or features of a dataset [29]. In the context of criminal networks, metadata refer to data sources, such as wiretap records, arrest warrants and judicial judgement that influence the topological and node attributes of an evolving network in the form of link formation and disappearance over time [28]. In the proposed FDRL-CNA model (Fig. 2), the number of wiretaps and arrest warrants issued is formulated as a feature matrix and processed by the metadata fusion neural network. Then, the output of the metadata fusion neural network is merged with the output of the SNA metric neural network to compute the weights required to identify the node pairs with edges which are most probable to alter in the future. These nodes will be used to initiate the network traversal search process by the MCTS policy network. Each metadata feature is extracted and formulated as the weight to be processed by the metadata fusion neural network as follows [29]:

\[
V_{k+} = \sum_{i} w_i x_i + b
\]

where \( v \) the vector of neurons within the neural network, \( w \) is the weight of each time step, \( k \), of node \( i \) and \( b \) is the corresponding bias, which will be calibrated at each iteration of the training process of the neural network.

IV. EXPERIMENT AND RESULTS
The Caviar drug import syndicate dataset from UCINET [30], which contains the historical evolution of a criminal network over a 2-year period involving 11 arrest operations where imported drugs were seized. The predictive performance of both the proposed FDRL-CNA and baseline TDRL-CNA link prediction models were both assessed using the AUC metric as it is unaffected by class imbalance.

A. EXPERIMENT SET-UP
For the purpose of training the classical and DRL-CNA link prediction models, a multidimensional feature matrix is formulated from SNA metrics feature selection extracted from the criminal network dataset. The formulation utilises SNA link prediction metrics to compute the likelihood of the formation or cessation of links between nodes at each time-step of the evolving criminal network dataset (Fig. 2).

The Caviar dataset used is randomly segregated into a training dataset and a test dataset at a ratio of 75%:25% respectively. The first part is used as the training set from which the features matrix for link prediction is derived. From the 11-time steps of arrest operations, 10-time steps are used for training from which the positive edges are randomly selected. The negative edges are then selected by random until the number of negative edges is equal to the positive edges. The link prediction models are used at each time step to predict the probable network instances from the test dataset.

The second part of the Caviar dataset represents the 11th time step, which is used as the test dataset to assess the predictive accuracy of both the classical and DRL models.

B. RESULTS AND DISCUSSION
The FDRL-CNA model managed to correctly predict more edges (Fig. 5(a)), which were supposed to exist within the network structure at the 11th time step, compared to the TDRL-CNA model (Fig. 5(b)) when measured against the actual criminal network structure at \( T_{11} \) (Fig.4).

The FRDL-CNA model did not manage to correctly predict eight node pairs, i.e. node pairs (83,86), (46,96), (81,87), (37,93), (84,85), (24,58), (72,79) and (11,94) (Fig. 5(a)). The TDRL-CNA model did not manage to correctly predict an additional seven node pairs, i.e. node pairs (13,41), (27,41), (14,58), (101,102), (59,102), (72,79) and (76,85) compared with the FRDL-CNA model (Fig. 5(b)).

Based on the comparison of the predicted criminal network topology at the 11th time step, \( T_{11} \), the empirical results do indicate that the metadata fusion with weights incorporated into the FDRL-CNA model (Fig. 5(a)) achieved a performance accuracy higher than the TDRL-CNA model (Fig. 5(b)).

A better predictive performance of the FRDL-CNA model than the TDRL-CNA model is most likely due to the metadata fusion data sources formulated as additional node similarity attributes, which are reflective of the real-world properties of the criminal network.

Additional experiments were also conducted where the proposed FDRL-CNA model was compared with three
classical ML models commonly used in link prediction, i.e. GBM, random forest (RF) and SVM (Figs. 6 and 8(a) to 8(c)).

The AUC scores of the classical link prediction models based on GBM, RF and SVM (Fig. 6) that incorporate metadata fusion as the edge weights are higher than the AUC scores achieved by link prediction models based on the classical ML techniques of GBM, RF and SVM (Fig. 7) that omit the factoring of metadata fusion by 0.11, 0.14 and 0.04, respectively (Tables II and III).

These results indicate that the factoring of metadata fusion also improves the predictive accuracy of the trained classical ML models. The reason for the overall improvement of the ML models that incorporate metadata fusion as edge weights could be that the metadata provides additional information on the relationships and node attributes between node-pairs, which improves the identification of node-pairs which have a higher probability of a change in the links or edges in the future.

The identification of these node-pairs will also improve the network traversal search process from root to leaf by reducing the scope of the search process.

**TABLE II**

<table>
<thead>
<tr>
<th>Dataset</th>
<th>FDRL</th>
<th>GBM</th>
<th>RF</th>
<th>SVM</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUC</td>
<td>0.71</td>
<td>0.63</td>
<td>0.68</td>
<td>0.59</td>
</tr>
<tr>
<td>Iteration</td>
<td>1500</td>
<td>1500</td>
<td>1500</td>
<td>1500</td>
</tr>
</tbody>
</table>

**TABLE III**

<table>
<thead>
<tr>
<th>Dataset</th>
<th>TDRL</th>
<th>GBM</th>
<th>RF</th>
<th>SVM</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUC</td>
<td>0.59</td>
<td>0.52</td>
<td>0.54</td>
<td>0.55</td>
</tr>
<tr>
<td>Iteration</td>
<td>1500</td>
<td>1500</td>
<td>1500</td>
<td>1500</td>
</tr>
</tbody>
</table>

*True Positive (TP) Rate against the False Positive (FP) Rate
Overall, the link prediction results of the FDRL-CNA model, which leverages on the DRL technique, exhibit a higher predictive accuracy performance than the three classical ML models (Figs. 8(a) to 8(c) and 9(a) to 9(c)) when relatively smaller datasets were used to train the models because the DRL model can be trained on self-generated datasets.

This result is consistent with that of prior research conducted by Lim at al. on DRL link prediction based on a snapshot of a criminal network [26].

V. CONCLUSION
In this research, the experiments results demonstrated that the link prediction model developed with DRL that incorporates metadata fusion (FDRL-CNA model) has higher predictive accuracy than the TDRL-CNA model that does not involve metadata fusion. This finding is confirmed by the AUC scores of 0.71 and 0.59 of the FDRL-CNA model which is higher than the scores of the TDRL-CNA model (Tables 2 and 3). The experiments also indicated that the models developed with the DRL technique were able to exhibit better predictive performance than those developed with classical supervised learning techniques of GBM, RF and SVM, under the same hyper-parameter and relatively smaller dataset setting. The inclusion of metadata information sources, such as arrest warrants, judicial judgements and wiretap records, have enhanced the predictive accuracy of the model possibly because real-world activities that influence criminal network properties and behaviour have been factored into the construction of the model. Such a model can significantly strengthen the function of law enforcement agencies to disrupt criminal network activities by taking a fast pre-emptive strike against key actors.

VI. FUTURE WORK
The trajectory of future work will involve devising a specific indexed SNA metric to be factored as weights in the construction of the classification algorithms to enhance the sensitivity of the FDRL-CNA model. The indexed SNA metric, which incorporates metadata measurements, is expected to improve the accuracy of the link prediction model as this research has demonstrated that metadata fusion will enhance the model to be more reflective of real-world parameters and variables.

REFERENCES


FIRST A. MARCUS LIM received his M.S. degrees in Business Information System from the University of East London in 2016. Currently, he is pursuing his Ph.D. degree in Computer Science at Taylors University.

SECOND B. AZWEEN ABDULLAH is a professional development alumni of Stanford University and MIT and his work experience includes thirty years as an academic in institutions of higher learning and as director of research and academic affairs at two institutions of higher learning, vice-president for educational consultancy services, 15 years in commercial companies as Software Engineer, Systems Analyst and as a computer software developer and IT/MIS consultancy and training.

THIRD C. NOOR ZAMAN received the Ph.D. degree in IT from UTP, Malaysia. He has great international exposure in academia, research, administration, and academic quality accreditation. He was with ILMA University, KFU for a decade, and currently with Taylor’s University, Malaysia. He has 19 years of teaching & administrative experience. He has an intensive background of academic quality accreditation in higher education besides scientific research activities, he had worked a decade for academic accreditation, and earned ABET accreditation twice for three programs at CCISIT, King Faisal University, Saud Arabia. Dr. Noor Zaman has awarded as top reviewer 1% globally by WoS/ISI (Publons) recently. He has edited/authored more than 11 research books with international reputed publishers, earned several research grants, and a great number of indexed research articles on his credit. He has supervised several postgraduate students including master’s and Ph.D. Dr. Jhanjhi is an Associate Editor of IEEE ACCESS, Guest editor of several reputed journals, member of the editorial board of several research journals, and active TPC member of reputed conferences around the globe.

FOURTH D. MUHAMMAD KHURRAM KHAN is currently working as a Professor of Cybersecurity at the Center of Excellence in Information Assurance (CoEIA), King Saud University, Kingdom of Saudi Arabia. He is one of the founding members of CoEIA and has served as the Manager R&D from 2009-2012. He, along with his team, developed and successfully managed Cybersecurity research program of CoEIA, which turned the center as one of the best centers of excellence in the region. He is the founder and CEO of the “Global Foundation for Cyber Studies and Research” (http://www.gfcyber.org), an independent, non-profit, and non-partisan cybersecurity think-tank in Washington D.C., USA, which explores and addresses global cyberspace challenges from the intersecting dimensions of policy and technology. Prof. Khurram
is the Editor-in-Chief of a well-reputed International journal ‘Telecommunication Systems’ published by Springer for over 26 years with its recent impact factor of 1.707 (JCR 2019). Furthermore, he is on the editorial board of several international journals, including, IEEE Communications Surveys & Tutorials, IEEE Communications Magazine, IEEE Internet of Things Journal, IEEE Transactions on Consumer Electronics, Journal of Network & Computer Applications (Elsevier), IEEE Access, IEEE Consumer Electronics Magazine, PLOS ONE, Electronic Commerce Research, IET Wireless Sensor Systems, Journal of Information Hiding and Multimedia Signal Processing, and International Journal of Biometrics, etc. He has also played the role of a guest editor of several international journals of IEEE, Springer, Wiley, and Elsevier Science. Moreover, he is one of the organizing chairs of more than 5 dozen international conferences and member of technical committees of more than 10 dozen international conferences. In addition, he is an active reviewer of many international journals as well as research foundations of Switzerland, Italy, Saudi Arabia and the Czech Republic. Prof. Khurram is the recipient of the King Saud University Award for Scientific Excellence (Research Productivity) in May 2015. He is also a recipient of the King Saud University Award for Scientific Excellence (Inventions, Innovations, and Technology Licensing) in May 2016. He has secured “Outstanding Leadership Award” at the IEEE international conference on Networks and Systems Security 2009, Australia. Besides, he has received a certificate of appreciation for outstanding contributions in “Biometrics & Information Security Research” at the AIT International Conference, June 2010 in Japan. He has been awarded a Gold Medal for the “Best Invention & Innovation Award” at 10th Malaysian Technology Expo 2011, Malaysia. Moreover, in April 2013, his invention received a Bronze Medal at the ‘41st International Exhibition of Inventions’ at Geneva, Switzerland. In addition, he was awarded the best paper award from the Journal of Network & Computer Applications (Elsevier) in Dec. 2015. He has published more than 350 research papers in the journals and conferences of international repute. In addition, he is an inventor of 10US/PCT patents. He has edited 7 books/proceedings published by Springer-Verlag and IEEE. He has secured several national and international competitive research grants in the domain of Cybersecurity. He has played a leading role in developing “BS Cybersecurity Degree Program” and “Higher Diploma in Cybersecurity” at King Saud University. His research areas of interest are Cybersecurity, digital authentication, IoT security, cyber policy, and technological innovation management. He is a fellow of the IET (UK), fellow of the BCS (UK), fellow of the FTRA (Korea), senior member of the IEEE (USA), senior member of the IACSIT (Singapore), member of the IEEE Consumer Electronics Society, member of the IEEE Communications Society, member of the IEEE Technical Committee on Security & Privacy, member of the IEEE IoT Community, member of the IEEE Smart Cities Community, and member of the IEEE Cybersecurity Community. He is also the Vice-Chair of IEEE Communications Society Saudi Chapter. He is a distinguished Lecturer of the IEEE. His detailed profile can be visited at http://www.professorkhurram.com