IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON SECURITY AND TRUSTED COMPUTING FOR INDUSTRIAL INTERNET OF THINGS

Received April 7, 2018, accepted May 24, 2018, date of publication June 7, 2018, date of current version July 6, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2844794

A New Threat Intelligence Scheme for Safeguarding Industry 4.0 Systems

NOUR MOUSTAFA, (Member, IEEE), ERWIN ADI, (Member, IEEE), BENJAMIN TURNBULL, (Member, IEEE), AND JIANKUN HU, (Senior Member, IEEE)

School of Engineering and Information Technology, University of New South Wales at ADFA, Canberra, ACT 2612, Australia

Corresponding author: Nour Moustafa (nour.moustafa@unsw.edu.au)

This work was supported in part by UNSW at ADFA Project OP001 under Grants 1Z6300PS4 and Z6300PS45623, and in part by the Australian Department of Defence under Grant DST-CERA 135.

ABSTRACT Industry 4.0 represents the fourth phase of industry and manufacturing revolution, unique in that it provides Internet-connected smart systems, including automated factories, organizations, development on demand, and 'just-in-time' development. Industry 4.0 includes the integration of cyber-physical systems (CPSs), Internet of Things (IoT), cloud and fog computing paradigms for developing smart systems, smart homes, and smart cities. Given Industry 4.0 is comprised sensor fields, actuators, fog and cloud processing paradigms, and network systems, designing a secure architecture faces two major challenges: handling heterogeneous sources at scale and maintaining security over a large, disparate, data-driven system that interacts with the physical environment. This paper addresses these challenges by proposing a new threat intelligence scheme that models the dynamic interactions of industry 4.0 components including physical and network systems. The scheme consists of two components: a smart management module and a threat intelligence module. The smart data management module handles heterogeneous data sources, one of the foundational requirements for interacting with an Industry 4.0 system. This includes data to and from sensors, actuators, in addition to other forms of network traffic. The proposed threat intelligence technique is designed based on beta mixture-hidden Markov models (MHMMs) for discovering anomalous activities against both physical and network systems. The scheme is evaluated on two well-known datasets: the CPS dataset of sensors and actuators and the UNSW-NB15 dataset of network traffic. The results reveal that the proposed technique outperforms five peer mechanisms, suggesting its effectiveness as a viable deployment methodology in real-Industry 4.0 systems.

INDEX TERMS Industry 4.0, threat intelligence, cyber-attacks, cyber-physical systems (CPS), Internet of Things (IoT), cloud, fog, beta mixture-hidden Markov models (MHMM).

I. INTRODUCTION

The emerging Industry 4.0 represents the fourth phase of industry and manufacturing, promising to become the foundation of smart systems, automated factories, and intelligent buildings. Through data-driven decision-making and heavy use of Cyber-Physical Systems (CPS), Industry 4.0 has the potential to change many aspects of our daily lives. The term Industry 4.0 was proposed by the German government in 2011 as an impetus for shifting the manufacturing sector into the technological automation one [1], [2]. Earlier industrial phases are mechanisation, electricity and Information Technology (IT). The fourth phase of industry and manufacturing enables automation in manufacturing, through a combination of CPS, Cloud and Fog computing, Internet of Things (IoT), data exchanges, big data, and autonomous industrial techniques [3], [4].

The promise of change offered by Industry 4.0 is based on pervasive and heterogeneous sensor networks, computing devices, and ubiquitous internet connectivity. Industry 4.0 is also heavily linked to smart machines, especially in the area of manufacturing. Smart machines provide increased manufacturing speed, faster recalibration, and greater customisation, allowing for the development of new business and partnership models to meet individual customer requirements. This combination also increases profitability, flexibility and reduces waste. One example of current industrial development is the management of electricity storage [5], integrating renewable energy and electrical grid usage using

IoT technologies. Power balancing techniques have been proposed to address the problems of dynamic pricing and energy saving [1], [5]. Although Industry 4.0 systems have the opportunity to improve the productivity and profitability of organisations, they still face large challenges related to cybersecurity and privacy [1]–[4].

The core of these challenges comes from differing standards in manufacturing and technology specifications. To be successful, Industry 4.0 implementations require an architecture design capable of unifying industry-based operational technology platforms and traditional IT systems, each relying on different protocols, security models and expectations for confidentiality, integrity, and availability [2], [3], [5]. Securing Industry 4.0 demands proactive and reactive security across all aspects; from sensor fields, the data they produce, the 'big data' datasets and the systems that analyze them, the network traffic produced, the mobile and workstations interacting with them, and the actuators that interact with the environment, individually and at scale. "Security by design" must become an integral part of big data analytics to establish secure Industry 4.0 systems.

Industry 4.0 is a system-of-systems, and security issues in one area can detrimentally affect the system as a whole, often in ways that are non-trivial and non-obvious. Concepts such as data transparency must be developed into Industry 4.0 implementations at all levels of the design process. It is obvious that data transparency of Industry 4.0 faces open issues in cybersecurity and privacy. There are sophisticated attacking techniques that attempt to exploit Industry 4.0 environments by hacking their physical and network systems [3], [4]. Given the Industry 4.0 aims to universally integrate software and physical modules, there is a heavy requirement for CPS within Industry 4.0. There are potentially large consequences for successful cyber-attacks, as actuators control and alter aspects of the physical environment.

This introduces a contemporary cybersecurity issue: how can secure cyber systems for heterogeneous sensors and network traffic be designed [2], [4], [5]? To address this question, this paper proposes a new threat intelligence scheme based on Beta **M**ixture [6] and **H**idden **M**arkov **M**odels [7], [8] (MHMM) for discovering cyber adversaries that attempt to expose physical and network layers of Industry 4.0 systems. The novelty of the proposed scheme includes designing an architecture that shows how Industry 4.0 elements interact including CPS, IoT, and both Fog and Cloud computing paradigms. More importantly, since Industry 4.0 comprises different data sources of sensor/actuators and network nodes, we propose a data smart module that can process these data sources. For reducing the data dimensionality, we use the Independent Component Analysis (ICA) technique [9] for removing irrelevant features and improving the MHMM performance.

In addition to the use of ICA to reduce sensor and network dimensionality, this work proposes a Beta Mixture Model (BMM) for fitting multivariate time series of physical and network data. We propose using the BMM as it can solve the boundary issue of Gaussian Mixture Model (GMM) [6], [10]. The BMM is used as input of the HMM which is utilised for threat intelligence by learning legitimate and suspicious states and computing their posterior probabilities. The minimum and maximum posteriors of normal and suspicious states are used as baselines for identifying known and zero-day attacks. Thus, this mechanism solves the issue of anomaly methods being unable to define attack types and the issue of signature methods that cannot discover zero-day attacks [6], [8].

Due to the fact that there are no publically accessible Industry 4.0 datasets, this work trains and validates the proposed technique using a combination of the power system dataset of sensors and physical devices [11], [12] and UNSW-NB15 dataset of network traffic [13], [14], as in aggregate these forms of data are of the types that would be collected within an Industry 4.0 deployment to build threat intelligence, intrusion detection, and forensic systems.

The key contributions of the paper include the following.

- We propose a threat intelligence technique for recognising cyber threats in Industry 4.0 based on BMM and HMM, novel in this domain.
- We provide depth-statistical and mathematical theories and applications that demonstrate the applicability of the proposed mechanism in real-world Industry 4.0 systems.
- We evaluate the performance of the proposed mechanism using physical and network data with comparisons that reveal its superiority compared to five peer mechanisms.

The remainder of the study is structured as follows. Section II explains the background and related studies of threat intelligence and Industry 4.0. Section III discusses the proposed architecture of Industry 4.0 and how the heterogeneous data sources could be processed. The proposed MHMM mechanism is detailed in Section IV. Section V describes the empirical results and discussions. Finally, we conclude the study with future directions of research that are provided in Section VI.

II. BACKGROUND AND RELATED WORK

This section discusses the background of intelligent threat mechanisms that have been utilised in these paradigms. Moreover, the background and related studies discuss how CPS, IoT, Cloud and Fog paradigms integrate into Industry 4.0 systems. Each of these sections will be discussed separately.

A. THREAT INTELLIGENCE

Threat intelligence was defined as the process of obtaining many sources and knowledge about cyber threats that can be used for discovering malicious events for the purpose of protecting organisations' assets [15].

Threat Intelligence expands upon the concepts of intrusion detection, as it maintains the properties of monitoring

and analyzing platforms and network traffic using, either a signature or anomaly-based methodology, or a hybrid of the two [6], [8]. A signature-based methodology monitors events of host, mobiles, devices or network systems and matches against a predefined blacklist of attack signatures if any rule is fired. Signature-based methodologies can efficiently detect existing cyber-attacks, but consume a high processing time to check and update known attack rules and are inherently incapable of discovering zero-day attacks where there is no predefined rule [14], [16].

In contrast, an anomaly detection methodology creates a profile of normal events and considers any deviations as attacks. Although the methodology can detect known and zero-day attacks with some limitations of false positive rates (i.e., detecting normal instances as attacks), it cannot define attack types such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) [6], [8], [14], [16].

Given this need, this work proposes a threat intelligence architecture for Industry 4.0 systems, which learns statistical state transitions of normal and attack events from multivariate time series that can discover known and unknown attacks and their type based on estimating the posterior boundaries of normal and attack categories. This model solves the issues of existing anomaly and signature-based methods.

B. INDUSTRY 4.0 SYSTEMS

The components of Industry 4.0 are introduced in this section. Specifically, this work outlines the technology platforms that underpin Industry 4.0, which are Cyber-Physical Systems, IoT, Cloud Computing and Fog Computing. Existing work on threat intelligence at each component is presented and critically analyzed.

1) CYBER-PHYSICAL SYSTEMS

Industry 4.0 foresees that the operations of physical facilities are overseen by computing systems in the shape of Cyber-Physical Systems (CPS). The term denotes a revolution on how humans will interact with and control the physical world, from the nano to large-scale systems. Industry 4.0 has amazing potential [8], including zero-energy buildings, abundant agriculture yield, access to medical care, life assistance, and reliable electricity. CPS, therefore, must operate dependably, safely, and in real-time.

With the ubiquity of low-cost sensors and data storage, coupled with increases in the speed and reliability of Internet connectivity, the scale and breadth of data collection has dramatically improved. However, data collection does not itself provide meaning. There is a gap between the current manufacturing model and the use of CPS. Current manufacturing systems require cognition and intelligence to convert data into useful information for the right purpose.

For this reason, there is a need to open currently available systems and find mechanisms for integrating them into a CPS model. The shift from traditional manufacturing to CPS thereby presents a flow of smart sensors, data conversion, cyber systems, cognition, and configuration [17]. The challenge with this movement is, while accessibility to collect data increases, the cyber threat surface expands. CPS adds several factors to the threat surface through the integration of physical components and communication infrastructure, all running on common protocols and systems.

2) INTERNET OF THINGS

The manifestation when devices and appliances are connected to the Internet is termed as the Internet of Things (IoT). When the Internet began to proliferate through web services in the late 20^{th} century, it was envisaged that objects such as refrigerators would directly and automatically order food through e-commerce. Instead, the path of development for IoT has been built on the ubiquity of computing through the proliferation of workstations, laptops, tablets and mobile devices. Miniaturisation of computers, together with the advancement of wireless networks, formed the ingredients for the creation of new products.

Sensors became Internet-connected devices, such as IP cameras and wearable devices. These mobile devices and low-cost sensors are responsible for the growth of the IoT. Current work indicates that cyber threats in the IoT layer focuses on the authentication, authorisation and access control [21]. This study observed that heterogeneity [22] and large datasets are changing how cyber threats can be detected. The traffic pattern will continuously change, not only due to increasing use of applications and new network protocols [23], [24], but also malicious use of botnets [24], [25]. The uniqueness of this space when compared with existing systems means there is an identified need to develop machine learning, statistical learning, and deep learning techniques able to classify big data for analyzing IoT cyber threats [26], [27].

3) CLOUD COMPUTING

The term Cloud Computing is a network of networks linked using the internet, where virtual shared servers offer software, infrastructure, platforms, services and other resources accessible to customers anywhere at any time [28]. The Cloud comprises a set of applications, platforms, and infrastructure connected to each other by the Internet for providing them to customers on-demand. The Cloud offers an elastic computing model, which permits firms and organisations to use and adapt their IT needs over the Internet with a lower cost of use, without any liability toward IT infrastructure and maintenance [29].

Cloud Computing is one of the key drivers enabling Industry 4.0 [30]. As the Cloud offers flexible, on-demand centralized data storage and high-uptime services, it is a highly relevant technology for storing and handling big data. For example, storm forecasting was conducted in a short time through data collection from disparate sensors and previously developed datasets [31]. Data can be collected from geographically dispersed sensors into a pooled resource through publicly available APIs, via common network protocols.

One of the big challenges in contemporary threat detection techniques stems from those in processing heterogeneous data sources collected from software, platforms, and Fog and Cloud computing systems [32]. This is exemplified in recent studies of threat detection in Cloud computing which discuss the proposed solutions separately at the application, platform, and infrastructure layers [32]–[35]. For example, web application threat detection was proposed as part of software services [36], as detection at the application layer is very effective compared to when threat detections were deployed as other services. Delivering threat detection solutions at different layers highlights inconsistencies in coordinating these approaches and can also lead to incomplete coverage across various intelligent systems. For example, Iqbal *et al.* [37] [37] outline a system where threat detection is installed as a hypervisor on a virtual machine, enhancing the reliability of the computing systems being protected. However, when threat detection solutions were integrated at different layers as collaborating systems, they suffered from scalability issues as the performance dropped with the increased data volume [38]. On the other hand, scalable collaborative threat detection solutions [29] did not provide a centralized correlation handler to merge activities, and thereby failed to detect large-scale distributed anomalies. This is issue especially pertinent to Industry 4.0, given that it does not have standards or architectures that demonstrate how distributed nodes could be monitored.

4) FOG COMPUTING

While Cloud Computing places processing power, infrastructure, and software into central systems, Fog Computing (or Fog) locates these capabilities closer to end users [33]. The drive behind the technology is the needs for low latency services and mobility. With computing power geographically located closer to end users, Fog applications such as gaming and augmented reality can enjoy real-time services; and moving vehicles can make use of streaming facilities. These use-cases are not achievable with Cloud paradigms, given the latency induced.

It is not foreseen that Fog Computing will cannibalize Cloud Computing. Rather, there are mutual reciprocities between the two, especially when it comes to data management and analytics. The Fog focuses on localisation, Cloud computing provides centralisation; hence, the former enables low latency services, while the later administer globalization. Due to these reciprocities, threat intelligence in the Fog endows those issues that both the Cloud and the IoT faces [39], [40], such as authentication and access control at all different service layers. In addition, the Fog can be made responsible for preserving privacy, especially in preserving the usage and location of end devices [40]. For example, path trajectory of an end-device can be inferred through analyzing collective data, although a single location data was secured.

Because the Fog is well positioned to collect large amounts of data, recent studies in detecting cyber threats in the Fog employed machine learning techniques [41]. In addition, the use of Markov models has been shown as a powerful tool to detect threats in this problem area [42], [43], due to their abilities to model state transition with probabilities. A Markov model is used to predict cyber threat patterns based on the current known features [44].

III. INDUSTRY 4.0 SYSTEM ARCHITECTURE

This work proposes an Industry 4.0 architecture that clarifies the interconnections of CPS and IoT solutions and provides services to users and organisations, using both Cloud and Fog paradigms. Based on this, it also outlines how the proposed threat intelligence architecture can monitor and analyze Industry 4.0 systems, recognizing cyber-attacks that attempt to exploit their critical infrastructure and network communications. As shown in Figure 1, devices of sensors and actuators demand middleware tools that digitalise and connect those devices to the Internet.

Once the devices are connected to the Internet, they are transformed into IoT and/or CPS services that users and organisations can lease as necessary, as opposed to purchasing and maintaining their own physical systems. Cloud and Fog Computing are the current two paradigms that offer the services in terms of software, platforms, and infrastructures to users and organisations [34]. It is obvious that there are open-loop connections that link between physical and technological systems that have the potential to lead to cybersecurity and data privacy issues [3], [45]. For identifying cyber threats from Industry 4.0 environments, this work proposes a threat intelligence architecture that concurrently monitors Cloud and Fog destination nodes. The architecture includes three main components of smart data management and analysis, feature reduction, and new MHMM threat intelligence, as explained below.

SMART DATA MANAGEMENT

Industry 4.0 systems are comprised of four layers; the physical layer, the sensor/actuator layer, the control layer and the network layer [46]. The physical layer links directly to the sensor/actuator layer. Sensors are used for estimating the dynamics of the physical systems and capturing these systems into the digital systems, while actuators are used for modifying the environment to desired states and local controllers to take suitable actions when needed. The network layer is responsible for communicating sensor and actuator devices using various protocols and services, such as IP, TCP/IP, HTTP, and HTTPS.

Middleware tools, such as Zerynth Studio [47] and Node-Red [48], are the interpreter between these devices and their software to connect to the Internet and they offered as services to users and organisations, ensuring effective communications these layers. The middleware tools are utilised for remotely monitoring and managing Cloud and/or Fog services and recording the services' data in log files. Consequently, Industry 4.0 systems generate heterogeneous data sources collected from log files of these devices (e.g., temperature and power data using middleware) and network

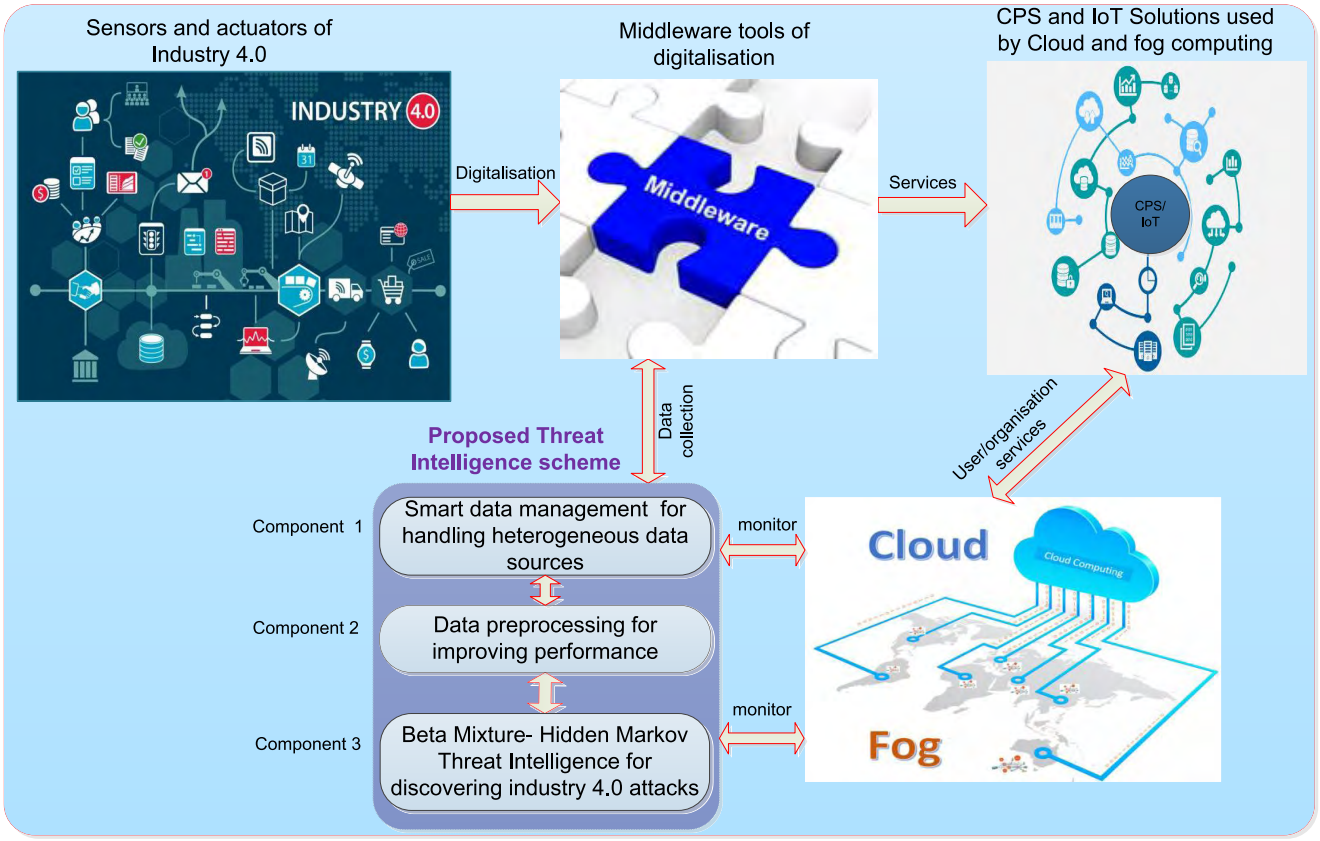

FIGURE 1. Proposed workflow for Industry 4.0 threat intelligence.

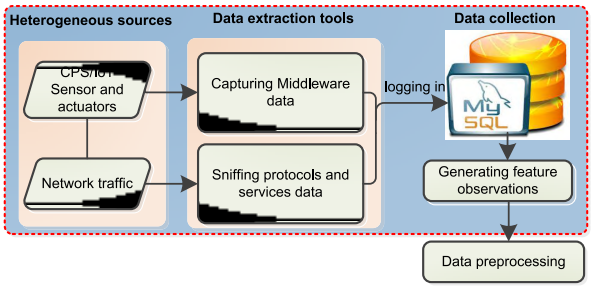

FIGURE 2. Proposed Smart data management.

traffic while providing these devices as services to users and organisations, as presented in Figure 2.

The data of sensors and actuators is captured from the log files of middleware tools, while network collection and Intrusion Detection System (IDS) tools (such as TCPDump and Bro-IDS, respectively) are employed for capturing network traffic and generating feature observations. For determining the reliability of our architecture, we used two publicly labelled datasets that include malicious activities of physical and network systems. The CPS power datasets [11], [12] were used for collecting multiclass physical attacks against collecting features of power sensors while the UNSW-NB15 [13], [14] are used for collecting features of network flows. This is discussed further in Section V. Therefore, the features of the two datasets can be recorded in a distributed and scalable database for handling their heterogeneity.

For the implementation of this work, a MySQL Cluster CGE [16] was utilised for the logging process due to the fact that it can process extremely scalable and real-time databases that allow a distributed architecture to handle intensive workloads while permitting the access by SQL or NoSQL APIs. It can also process memory-optimised and disk-based tubulars, data partitioning with load-balancing, and add nodes into a running cluster to process online big data, which is the goal of training and testing real-time threat intelligence for Industry 4.0 systems.

DATA PRE-PROCESSING

Once features have been extracted from the two datasets, they are then processed to be compatible input to the proposed threat intelligence mechanism. Three data pre-processing methods are applied to the two datasets to improve the performance and scalability of the proposed mechanism. These are feature conversion, feature reduction and feature normalisation, discussed below.

- **Feature conversion-** maps any categorical feature into numeric features, for example, the protocol values of TCP and UDP are converted into ordered numbers

of 1 and 2, respectively. This is because the proposed threat intelligence mechanism can only deal with numeric features [6], [49].

- **Feature reduction-** removes irrelevant and redundant features from the data collections. We utilise the ICA technique [9], as it mines unidentified hidden components from multivariate data, that is, linear mixtures of some latent variables, using only the assumption that the unknown components are mutually independent and non-Gaussian from a statistical perspective. The ICA is chosen, as it fits non-Gaussian data, which is the norm for CPS/IoT and network data. It converts original features into a set of independent attributes by maximising the non-Gaussian data of new components. The general ICA technique is given as [50]

$$x = As + n \tag{1}$$

where x is a m-dimensional feature observation, s is the vector of assumed n-dimensional independent components, A is a constant $m \times n$ mixing matrix with $m \geq n$ and n a noise term. As we assume that CPS/IoT and network data are logged and labelled in a noise-free environment, the ICA model can be reformulated as

$$x = As \tag{2}$$

and

$$s = Wx \tag{3}$$

where W is the un-mixing matrix, called a mapping function, for projecting x to s.
ICA makes the best guesses of A and s given x with the constraint of maximising the non-Gaussian data so that these independent components are suitable representations of the data. To solve (3), we describe the constraint of maximising the non-Gaussian data as minimising the mutual information (MI) between n variables (s_i), where $i = \{1, \ldots, n\}$, as

$$MI(s_1, s_2, \ldots, s_m) = \sum_i H(s_i) - H(s_d) \tag{4}$$

where H is the differential entropy. Although the mutual information is usually non-negative, if it is zero, (4) is expressed as

$$\begin{aligned} \sum_i H(s_i) &= H(s_o) \\ \Rightarrow \sum_i \int p(s_i) \log p(s_i) ds_i &= \int p(s_o) \log p(s_o) ds_o \end{aligned} \tag{5}$$

and

$$p(s_d) = p(s_1)p(s_1) \ldots p(s_m) \tag{6}$$

Since mutual information is the normal way of estimating the independence of variables, it could be used as the standard for determining the appropriate ICA transformation. This declares that the selected features are statistically independent by ranking the highest p(s) of the features. The steps for applying the ICA technique to choose the most relevant features of the CPS/IoT and network data are presented in Algorithm 1.

Algorithm 1 Steps for Applying Fast-ICA to Reduce CPS and Network Features

Input: Features (F) of CPS and Network data
Output: Relevant Features (RF)

1: set initial weight vector (W) to generate each RF
2: compute $w+ = Exg(wTx)–Eg\prime(wTx)w$
3: compute derivatives of contrast functions (G) for steps 4 and 5
4: $g1(u) = tanh(a_1.u)$
5: $g2(u) = u.\exp(-u^2/2)$
6: compute $w = w^+/||w^+||$(normalisation step)
7: if not converged, go to step 2
8: (converged if norm $(w_{new}–w_{old}) > \xi$ or norm $(w_{old} – w_{new}) > \xi$, where $\xi = 0.0001$)
9: apply above steps to generate K features of RF

- **Feature normalisation-** regulates features. After selecting the relevant features using the ICA technique, feature normalisation is essential for scaling the values of each feature into a certain range (e.g., [0, 1]) [6], [49]. This is for eliminating the bias from the raw CPS and network data without modifying their statistical characteristics. Since our proposed threat intelligence uses a Beta mixture model that which demands a certain interval for each feature (X) as input, the features of CPS and network are normalised into the interval of [0, 1] by the linear transformation in (7).

$$(X_{normalised}) = (x_i - min(X)/max(X) - min(X)) \tag{7}$$

IV. MIXTURE-HMM THREAT INTELLIGENCE TECHNIQUE

This section explains the mathematical theories behind the proposed Mixture-HMM mechanism. The training and testing phases for detecting Industry 4.0 threats are also described. Moreover, the dynamics of Industry 4.0 layers are described using the proposed mechanism.

A. BETA MIXTURE-HIDDEN MARKOV THREAT INTELLIGENCE

As CPS and network data are comprised of multivariate time series data, it is complex to build a learning model with these time series features given that they dynamically change over time. Mixture Hidden Markov Models (MHMM) are new variants that have been proposed for determining and visualising multiple parallel sequences for each label (e.g., normal and attacks). MHMM is usually applied to the Gaussian Mixture Model (GMM) when the number of mixture components is known, and edges of observed data are unbounded boundary (i.e., $]-\infty, \infty[$) [6], [10]. However, we statistically

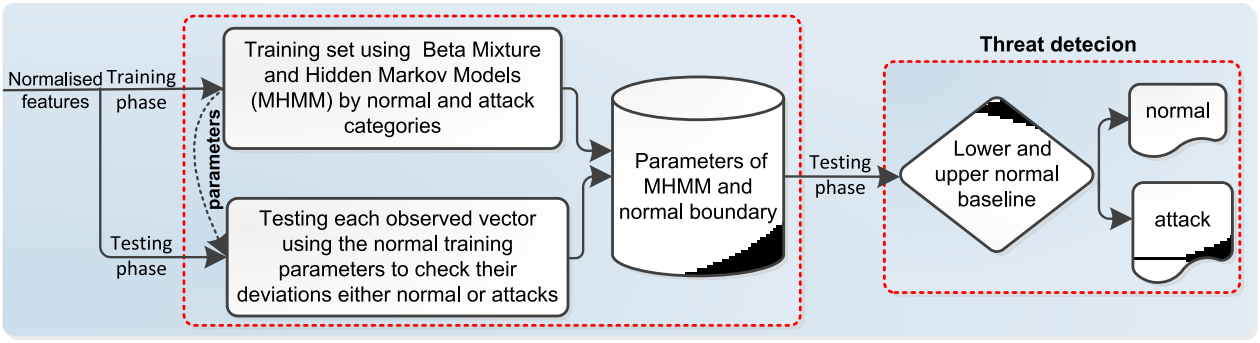

FIGURE 3. Proposed Mixture Hidden Markov mechanism for detecting Industry 4.0 threats.

observed that CPS and network data can be signified in a semi-bounded interval ($[0, N]$, N is an asymmetric number) for any feature in the datasets.

For solving the unbounded property of GMM, we propose using the BMM as BMM is more flexible than GMM and fits continuous variables that include a finite interval ($[a, b], a\ and\ b \in R$), such as [0, 1] which is the case for Industry 4.0 data. BMM has been previously used as a classifier, performing better than a GMM classifier in detecting human skin colors and speech spectra. The authors have used it in a previous study [6] to fit network data under bounded distributions and the results revealed that BMM can act better than GMM and Dirichlet Mixture Models (DMM). In this study, the BMM is used for clustering multivariate features of CPS and network data into a representative feature that has the potential characteristics of the raw feature vectors. After this has completed, the HMM is used the output of BMM as input for estimating the posterior probabilities and determining underlying latent structures for identifying unobservable states, either normal or abnormal, as shown in Figure 3.

For estimating the BMM for each feature vector, the Probability Density Function (PDF) is estimated by

$$f(X|\pi_k, v_k, \omega_k) = \sum_{k=1}^{K} \pi_k Beta(X, v_k, \omega_k) = \sum_{n=1}^{N} \pi_n \prod_{k=1}^{K} Beta(x_k, v_k, \omega_k) \quad (8)$$

Where X denotes feature vectors ($X = \{x_{11}, \ldots, x_{KN}\}$), such that N is the number of vectors and K is the number of components/relevant features selected by the ICA technique in Section III. ($\pi = \{\pi_1, \ldots, \pi_K\}$, $\upsilon = \{\upsilon_1, \ldots, \upsilon_K\}$, $\omega = \{\omega_1, \ldots, \omega_K\}$) are the three parameters of the BMM. π is the mixing weight, where $\sum_{k=1}^{K} \pi_k = 1,\ 0 < \pi < 1$), and υ_k and ω_k are the shape parameters of the beta distribution for each feature x_k. The EM algorithm is utilised for estimating these parameters as detailed in [10].

The HMM technique is widely used in the domains of speech recognition and network traffic, as it is a resilient discrete time-series technique that declares a probability distribution over vectors constrained on a particular number of hidden states [7], [8]. This study applies HMM under BMM for fitting and detecting abnormal behaviors of CPS and network features selected by the ICA technique and conditioned on two latent states of normal and attack. MHHM has two assumptions to be built on BMM; (1) the hidden state probability $p(s)$ at time (t) only relies on the previous state $(st - 1)$ at time $(t - 1)$, and (2) the feature vector $(x_{1:k}(t))$ under BMM represents one of the two hidden states: normal (SN) or attacks (SA). The joint probability of vectors and states is estimated by

$$P(S_{1:T}, X_{1:T}) = \prod_{t=1}^{T} P(x_t \mid s_t) \prod_{t=2}^{T} P(s_t \mid s_{t-1}) P(s_1) \quad (9)$$

The three HMM parameters of the initial, emission and transition probabilities are estimated based on the BMM, as follows.

- The initial vector ($I[1 : S]$) is the probabilities of starting hidden states, computed as

$$I[1 : S] = p(s_1, .., s_S) \quad (10)$$

  where s refers to the model states, as we have two states of normal and attack, we fairly initiate their probabilities as [0.5 (normal), 0.5 (attack)].
- The emission BMM matrix ($A[s_i, x_i]$) is the probabilities of the hidden state (s) emitting the observed feature vectors that are estimated using the PDF of BMM.

$$A[s_i, x_i] = p(f(x_i|\pi_i, v_i, \omega_i)|s_i) \quad (11)$$

  where $f(x_i|\pi_i, v_i, \omega_i)$ denotes the PDF of feature vectors using (8).
- The transition BMM matrix ($B[s_i, s_{i-1}]$)is the probability of moving from the state (s_{t-1}) to the coming state (s_t).

$$B[s_i, s_{i-1}] = p(s_t|s_{t-s}) \quad (12)$$

The posterior probability $(post)$ measure of each vector estimates the dependencies between prior and likelihood data distributions (i.e., $posterior \approx prior * likelihood$). This measure is applied to make a baseline the find the dynamic

changes of normal and attack states over time. It is computed with the following:

$$post = p(S_{1:N}|I_{1:N}, A_{1:N}) = p(s_1)p(f(x_i|\pi_i, v_i, \omega_i)|s_1) \times \prod_{i=1}^{I}(p(s_i|s_{i-1}) \times p(f(x_i|\pi_i, v_i, \omega_i)|s_i)) \quad (13)$$

B. TRAINING AND TESTING PHASES

In the training phase, the MHHM mechanism is learned using normal and attack vectors ($V_{1:N}^{training}$) in order to produce a threat model that includes wide variations of posterior probabilities of the two states of normal ($post^{normal}$) and attacks ($post^{attacks}$). The $prof^{training}$ includes the estimated parameters of the BMM (π_k, v_k, ω_k), and the minimum normal posterior ($min(post^{norml})$), and maximum normal posterior ($max(post^{norml})$) that will be used as a baseline of attack detection in the testing phase. The process of building the profile is described in Algorithm 2.

Algorithm 2 The Steps of the Training Phase

Input: training vectors ($V_{1:N}^{normal}$), class label= {*normal*/*attack*}
output: training profile ($prof^{training}$)

1: **for** each vector *i* all $V_{1:N}^{normal}$ **do**
2: **if** (class label == *normal*) **then**
3: BMM^{normal} ← estimate the BMM parametrs ($\pi_k, \upsilon_k, \omega_k$) for normal as in [10].
4: $post^{norml}$ ← compute the $post^{norml}$ using (13) based on step 2.
5: **else**
6: $BMM^{attacks}$ ← estimate the BMM parametrs ($\pi_k, \upsilon_k, \omega_k$) for attacks.
7: $post^{attacks}$ ← compute the $post^{attacks}$ using (13) based on step 2.
8: **end if**
9: **end for**
10: $[min(post^{norml}), max(post^{norml})]$ estimate the minimum and maximum $post^{normal}$.
11: $prof^{training}$ ← $\{\upsilon_k, \omega_k, \mu_k, min(post^{norml}), max(post^{norml})\}$
13: **return** ($prof^{training}$)

In the testing phase, the posterior probability ($post^{testing}$) of the observed vector ($V^{testing}$) is estimated using (13) with the same normal BMM parameters ($\upsilon_k, \omega_k, \mu_k$) of the $prof^{normal}$. The purpose of using the same normal parameters that if the value of $post^{testing}$ locates at the normal boundaries $[min(post^{norml}), max(post^{norml})]$, the observed vector will be a normal vector, otherwise an abnormal one, as the process of this phase is provided in Algorithm 3.

The proposed threat intelligence mechanism is more effective than the typical anomaly methodology, which creates a profile from normal activities only and considering deviations as attacks. The limitation of a typical anomaly methodology is unable to define attack types as there is no information

Algorithm 3 The Process of the Testing Phase

Input: observed vector ($v^{testing}$), *training profile* ($prof^{training}$)
output: normal or attack vector

1: $post^{testing}$ ←estimate the $post^{testing}$ using equation 13 based on the normal BMM parameters.
2: **if** ($post^{testing} \geq min(post^{norml})$) || ($post^{testing} \leq max(post^{norml})$) **then**
3: **return** normal
4: **else**
5: **return** attack
6: **end if**

about the types of attack in the training phase. However, the proposed method can estimate minimum and maximum posterior probabilities using steps 6 and 7 in algorithm 2 for each attack type. Thus, this mechanism can define zero-day attacks as anomaly methods and effectively detect existing attack types based on one condition of the minimum and maximum posterior of each attack types rather than many signature rules for each type, as in signature models that take a long processing time with regular updates.

C. INDUSTRY 4.0 DYNAMICS USING MHMM

As Industry 4.0 systems are comprised of several layers, this work presents a mathematical model based on MHMM for demonstrating the complexity of these systems. Mathematically speaking, to formulate the dynamic changes of the system states over time, this work assumes that network services should be monitored to recognise abnormal activities. Each of which is connected to a physical layer ($PL = \{PL_1, PL_2, \ldots, PL_N\}$), sensor/actuator layer ($SL = \{SL_1, SL_2, \ldots, SL_N\}$), network layer ($NL = \{NL_1, NL_2, \ldots, NL_N\}$) and control layer ($CL = \{CL_1, CL_2, \ldots, CL_N\}$, where N is number of states in the system), as presented in Figure 4.

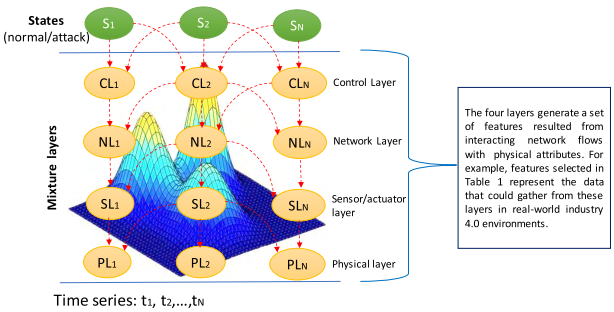

FIGURE 4. Modelling Industry 4.0 dynamics using MHMM.

These layers interact together to do a specific function over time, and the data collected from these layers can be represented using the proposed MHMM technique. For example, assume that there are two states in a system $S = \{SN, SA\}$, where SN refers to the normal state and SA refers to the attack

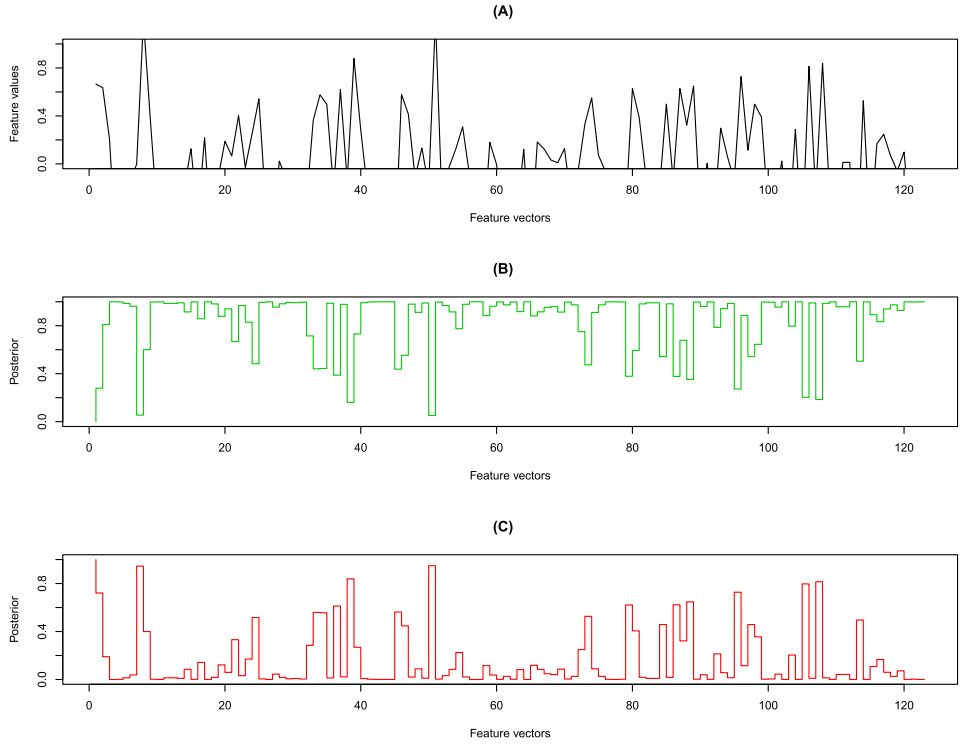

FIGURE 5. (A) shows 120 feature vectors from the CPS dataset, (B) and (C) represent the normal and attack posterior probabilities of the normal and attack states.

state. To represent the dynamics of normal and attack states, we compute the posterior probabilities for 120 samples from the power system dataset as plotted in Figure 5 (A, B and C). In Figure 5-(A), the normalised features for the 120 vectors are plotted. It is clear that the values of the features considerably vary in the normalised range of [0, 1]. The vectors include normal and attack states in which their posterior probabilities are computed using (13). It is observed that the majority of the normal posterior probabilities are located in the range of [0.5, 1] as shown in Figure 5-(B), whilst the he majority of the attack posterior probabilities are specified in the range of [0, 0.5], as presented in Figure 5-(C).

As shown, the MHMM mechanism makes considerable variations between normal and attack posterior probabilities. The reason behind these variations is that using BMM in a confidence interval of [0, 1] makes a clear difference in the normal boundaries. More importantly, fusing the relevant features using the PDF of BMM into one representative feature of the HMM technique leads to specify the normal variances which are too close from each other, while they considerably vary from attack vectors. This reveals that BMM and lower-upper normal posterior probabilities can improve the performance of detecting cyber-attacks from both CPS/IoT and network data, as explained in Section V-D.

V. EXPERIMENTAL RESULTS AND DISCUSSIONS

A. DESCRIPTION OF DATASETS

Two publicly available datasets were employed to evaluate the performance of the proposed threat intelligence architecture; the CPS power system dataset [11], [12] and the UNSW-NB15 dataset [13], [14]. The CPS power system dataset consists of 37 scenarios: natural events (8), no events (1) and intrusion events (28) that include Remote tripping, Relay, and Data injection attacks. The process of establishing this dataset is depicted in Figure 6. The figure shows two power generators, G1 and G2, connected to each other. There are four breakers in between these generators, BR1 to BR4. Each breaker is controlled by an IoT device R, hence, there are four devices labelled R1 to R4. They are responsible to provide remote protection mechanisms to control the breakers, such as automatically switch off the breaker it attaches to upon signs of faults. It is possible as well to manually override the program. All event detected by these R devices are sent to be saved as syslog in a logging system.

The UNSW-NB15 contains a large instance of recent, legitimate and malicious network features which allow sound analysis of the proposed technique. The UNSW-NB15 dataset contains about 100 Gigabytes of data representing 2,540,044 observations. Each observation is characterized through 47 features and a label signifying one of ten possible classes: a normal class and nine malicious categories (i.e., Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Fuzzers for anomalous activity, Shellcode, and Worms).

B. EVALUATION CRITERIA AND EXPERIMENTAL DESIGN

To measure the performance of the technique, the investigations on the two datasets employed Accuracy,

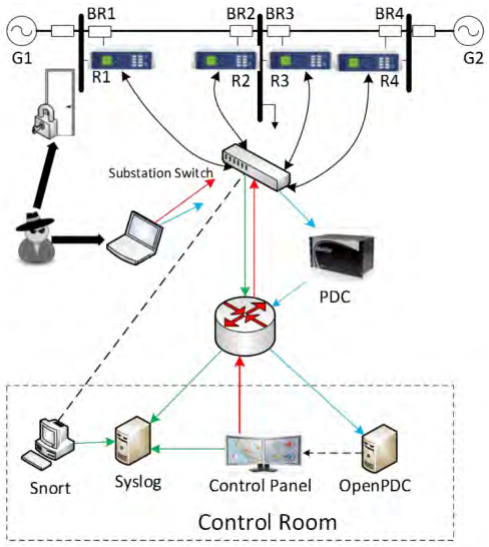

FIGURE 6. Testbed of generating CPS power system dataset.

Detection Rate (DR) and False Alarm Rate (FAR). These measures depend on four terms: True Positive (*TP*), True Negative (*TN*), False Negative (*FN*) and False Positive (*FP*). *TP* and *TN* are the number of suspicious and actual instances correctly classified as abnormal and normal, respectively. *FP* and *FN* are the numbers of actual and suspicious instances incorrectly defined as abnormal and normal, respectively. Henceforth, the performance metrics are defined as follows [6].

- The **Accuracy** is the percentage of all normal and attack vectors that are correctly classified, that is,

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)} \tag{14}$$

- The **detection rate (DR)** is the percentage of correctly detected attack vectors, that is,

$$DR = \frac{TP}{(TP + FN)} \tag{15}$$

- The **false positive rate (FPR)** is is the percentage of incorrectly detected attack vectors, that is,

$$FPR = \frac{FP}{(FP + TN)} \tag{16}$$

The proposed technique was developed using the 'R programming language' on Linux Ubuntu 16.04 LTS with 16 GB RAM on an i7 CPU processor. To conduct the experiments on each dataset, random samples were extracted from the two datasets with different sample sizes of between 100,000 and 300,000 (s). For each sample size, each normal sample is almost 60-70% of the total size, with some instances were used for training the technique and others were employed for testing it. The performance of the technique was obtained by averaging 5-fold cross-validation experiment results to correctly adapt the MHMM's parameters and measure its effectiveness for recognsinig attack observations.

C. ESTIMATION OF FEATURE REDUCTION

For evaluating the performance of the proposed mechanism, we selected the highest variances of nine features using the ICA technique explained in Section III from the power system and UNSW-NB15 datasets, as listed in Table 1.

TABLE 1. Features selected from the power system and UNSW-NB15 dataset.

Power system dataset		
No.	**Feature**	**Description**
F_1	PA1:VH – PA3:VH	Phase A – C Voltage Phase Angle
F_2	PM1:V – PM3:V	Phase A – C Voltage Magnitude
F_3	PA4:IH – PA6:IH	Phase A – C Current Phase Angle
F_4	PM4:I – PM6:I	Phase A – C Current Magnitude
F_5	PA7:VII – PA9:VII	Pos. – Neg. – Zero Voltage Phase Angle
F_6	PM7:V – PM9:V	Pos. – Neg. – Zero Voltage Magnitude
F_7	PA:Z	Apparent Impedance seen by relays
F_8	PM10:V – PM12:V	Pos. – Neg. – Zero Current Magnitude
F_9	PA:ZH	Apparent Impedance Angle seen by relays
UNSW-NB15 dataset		
F_1	ct_dst_sport_ltm	A number of connections containing the same destination address and source port in 100 connections
F_2	tcprtt	Round-trip time of TCP connection setup computed by the sum of 'synack' and 'ack-dat'
F_3	dwin	A value of destination TCP window advertisement
F_4	ct_src_dport_ltm	A number of connections containing the same source address and destination port in 100 connections
F_5	ct_dst_src_ltm	A number of connections containing the same source and destination address in 100 connections
F_6	ct_dst_ltm	A number of connections containing the same destination address in 100 connections
F_7	smean	Mean of flow packet sizes transmitted from source
F_8	dmean	Mean of flow packet sizes transmitted by destination
F_9	dtcpb	Source TCP base sequence number

The variation between features and their label is an accurate estimate, which assists the proposed MHMM mechanism in identifying the label either normal or attack. The box plot, which is a standardised representation of exhibiting the distribution of data using five statistical measures of minimum, first quartile, median, third quartile, and maximum values [51], can display the variations between feature values and their labels. As shown In Figures 7 and 8, the box plots for some samples from the power system and UNSW-NB15 datasets are presented, whereby there are clear variations between normal and abnormal feature values and their labels that extracted from the ICA technique. This is because the technique can find differences between non-linear and non-normal data distributions in which are the same characteristics of the power system and network data [6], [16].

D. EVALUATION OF MHMM ON POWER SYSTEMS AND NETWORK DATA

The performance of the proposed MHMM threat intelligence mechanism is assessed on the power system and

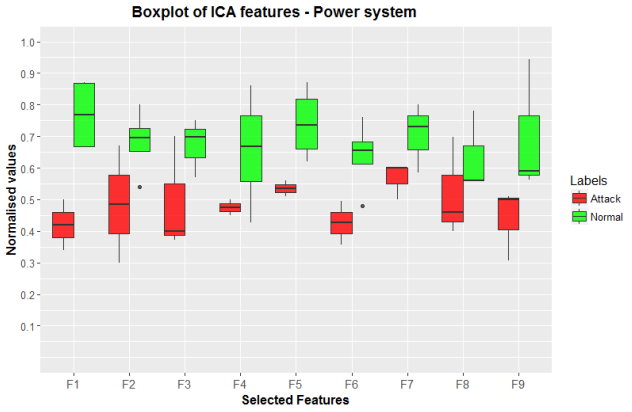

FIGURE 7. Box plots of features selected from power system dataset.

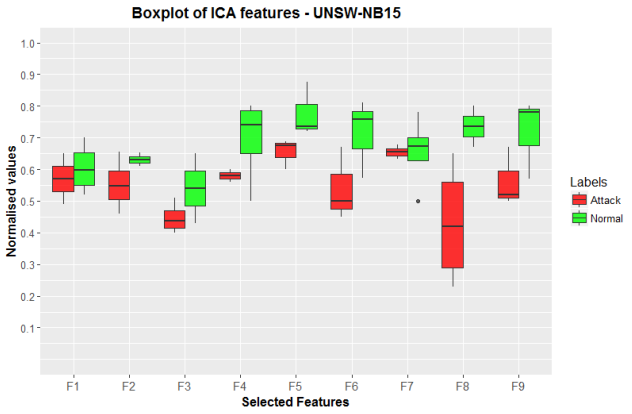

FIGURE 8. Box plots of features selected from UNSW dataset.

TABLE 2. Estimation of overall performances of six mechanisms on both datasets.

	Power Systems dataset			UNSW-NB15 dataset		
Mechanisms	DR (%)	Accuracy (%)	FPR (%)	DR (%)	Accuracy (%)	FPR (%)
Cart [52]	93.62	94.62	6.58	88.67	90.23	8.51
KNN [53]	89.57	89.94	9.54	85.35	86.64	11.48
SVM [54]	91.6	93.36	8.79	91.82	92.6	8.73
RF [55]	94.14	95.06	5.83	92.84	93.72	6.56
OGM [16]	96.23	97.18	3.75	94.76	95.19	4.72
MHMM	98.12	98.45	2.21	95.89	96.32	3.82

UNSW-NB15 datasets in terms of DR, accuracy, and FPR. The mechanism is compared with five peer techniques, named Cart [52], KNN [53], SVM [54], RF [55] and OGM [16] for demonstrating its effectiveness in identifying cyber adversaries that attempt to exploit Industry 4.0 systems within their sensors, actuators and network activities, as listed in Table 2. Moreover, the Receiver Operating Characteristics (ROC) curves that display the relation between the DR and FAR are presented in Figures 9 and 10 to clarify the inherent process of implementing the mechanisms.

It is obvious that the performance of the proposed MHMM technique is better than the other techniques, when applied to the two datasets. On the power systems dataset, the proposed mechanism gets the best outcome of a 96.23% DR and 98.45% accuracy and the lowest FPR of 2.21% technique achieves the best output of a 97.28% DR and 2.72% FAR, whereas the rest mechanisms attain on an average of 93-96% DR, 94-97% accuracy and 6-3% FPR. Similarly, on the UNSW-NB15 dataset, the proposed MHMM mechanism produces better than others, where it obtains a 95.89% DR, 96.32% accuracy and 3.82% FPR, whereby the others get in an average of 88-94% DR, 90-95% accuracy and 8-4% FPR.

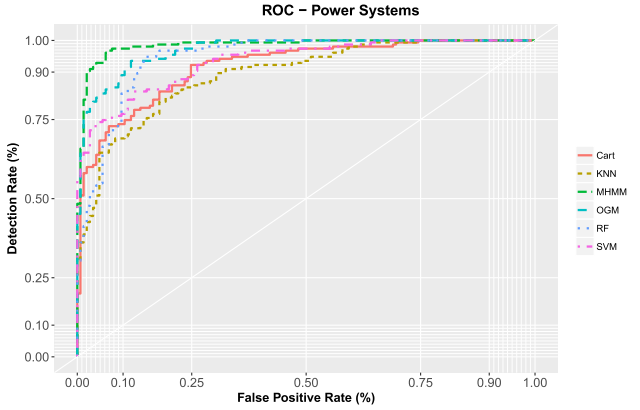

FIGURE 9. ROC curves of power system dataset compared five techniques with MHMM.

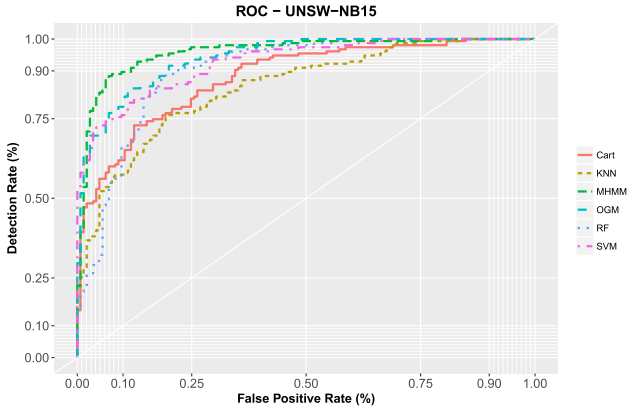

FIGURE 10. ROC curves of UNSW-NB15 dataset compared five techniques with MHMM.

The proposed MHMM mechanism can efficiently recognise different normal and abnormal records on both datasets. In Table 3, when the number of instances used to train and validate the mechanism increases (i.e., 100,000 to 300,000), the DRs gradually improve by well-fitting the parameters of BMM and HMM. On the power systems dataset, the mechanism can detect normal vectors with about a 98.05% DR and 1.95% false negative rate. Moreover, it can discover remote striping, reply, and data injection attacks that penetrate physical systems in an average of 97.69-99.36%.

On the UNSW-NB15 dataset, the mechanism can identify normal instances with approximately a 95.68% DR and

TABLE 3. Estimation of overall performances of six mechanisms on both datasets.

	Number of records		
Record types	**100,000**	**200,000**	**300,000**
Power system dataset			
Normal	97.62%	97.91%	98.05%
Tripping attack	98.92%	99.01%	99.01%
Relay attack	99.20%	99.26%	99.36%
Injection attack	97.69%	98.34%	98.47%
UNSW-NB15 dataset			
Normal	94.25%	94.38%	95.69%
Analysis	87.58%	87.87%	89.75%
Backdoor	81.83%	83.56%	87.58%
DoS	98.79%	98.80%	99.64%
Exploits	94.34%	96.49%	98.80%
Fuzzers	89.85%	92.83%	94.56%
Generic	93.93%	95.46%	96.87%
Reconnaissance	86.82%	87.89%	90.75%
Shellcode	99.24%	99.45%	99.37%
Worms	87.82%	87.56%	89.62%

4.32% false negative rate. Additionally, DoS, fuzzers, reconnaissance, and shellcode abnormal events are detected in an average of 90.75-99.64% DRs while the others are identified in an average of 89.62-89.75% due to their variances that are slightly similar to normal activities. But, these abnormal events do not appear in real-productions systems with the massive instances that found in the UNSW-NB15 dataset. The proposed mechanism can detect different normal and abnormal events using physical systems and network data that can be collected in Industry 4.0 systems. Based on that, the proposed MHMM mechanism can precisely model and classify the normal and attack states of real Industry 4.0 systems, as explained below.

E. DISCUSSION

The empirical results of the proposed MHHH mechanism, compared with the peer mechanisms, reveal its superiority in detecting different legitimate and malicious vectors on both physical and network data. The underlying reasons for this performance are twofold: the use of the ICA technique extracting for relevant features; and the utilisation of BMM for fitting multivariate time series physical and network data to construct threat intelligence by the HMM. Since physical and network data are not linearly and normally represented as presented in the boxplots of Figures 7 and 8, extracting important features demands the ICA technique which can deal with non-linear and non-Gaussian data distributions.

The ICA technique reduced the number of features into lower dimensional space (i.e., nine features from each dataset) with higher variances between them, including the impending characteristics of legitimate and attack observations. This improves the performance of MHMM. Using the experimental equipment, it takes approximately 55 seconds for processing 10,000 vectors if ICA is used, an improvement over the approximately 87 seconds it takes using the entire features of each dataset. Comparing our mechanism with the five compelling ones, it is observed that our mechanism runs faster than them with about 6-15 seconds for every 10,000 vectors, due to the complexity of building their potential process explained below.

In the HMM mechanism, fitting data distributions using the BMM solves the unbounded problem of mixture models, where the feature values are specified into a specific range that estimated based on the actual values of features into a finite range of $]-\infty, \infty[$. This enables the elimination of noise occurring in the lower and upper boundaries of mixture distribuends; thus, while estimating normal and suspicious states of vectors using the HMM, it improves computing different posterior probabilities of these states. Moreover, the posterior boundaries of each state can be used to be the threshold that discriminates between normal posterior probabilities and any abnormal ones. As a result, the MHMM threat intelligence could tackle the complexity of fitting and modelling Industry 4.0's data extracted from physical, sensor/actuator, control and network layers using estimating HMM parameters based on the BMM parameters in real-time for each specific time window.

The other mechanisms tested can not accurately fit and model the data produced by Industry 4.0 systems, like the MHMM. Additionally, their capability for recognising normal and attack categories are lower than the proposed methodology. There are several reasons for this, based on their underlying mathematical design. The Cart and RF mechanisms classify normal and attack data based on creating a recursive binary splitting method that differentiates between normal and attack values. These values could be relatively similar to mimicry attacks that try to mimic normal activities. The variations in the posterior probabilities of MHMM improves the detection accuracy for different attack categories compared with this mechanism. SVM requires an accurate determination of choosing a kernel function and its parameters. This leads to issues of over-fitting that can occur when learning normal observations that dynamically change over time. KNN and OGM cannot perfectly handle soft boundaries of training data, and therefore solved this challenge by estimating the actual feature vector boundaries using the BMM.

Despite some abnormal events, in particular backdoors and worms, analysis of UNSW-NB15 dataset are identified with low DRs in some runs using MHHM, and the results are better than the competing algorithms. This is due to the fact that this dataset was generated in a complex simulated environment that produces large numbers of abnormal traces that are unlikely to be found in real systems or other datasets. This also shows the proposed mechanism could effectively detect different abnormal activities in real Industry 4.0 environments compared with the peer machine learning techniques. It is important to note that there are no datasets specifically for Industry 4.0 systems, and the testing mechanisms are based on two benchmark datasets: power systems of physical data (i.e., sensors/actuators and devices) and UNSW-NB15 of network traffic that include data that should be collected from

any Industry 4.0 environment. This limitation highlights the need for the development of datasets encompassing different Industry 4.0 systems, including the connection of physical systems, IoT solutions, and both Fog and Cloud computing paradigms. Such datasets are needed to improve the fidelity of threat intelligence and intrusion detection systems.

Based on the above discussion, the MHMM technique has several advantages that enable monitoring and detecting threats that attempt to exploit Fog and Cloud computing. MHMM technique solves the main problem of anomaly detection by learning only on normal data, thus it can professionally detect both known and zero-day attacks. Moreover, it solves the problem inherent in rule-based detection systems in the requirement to develop and deploy signatures for all attack types. Instead, the MHMM technique estimates the lower and upper posterior probabilities of normal and existing attacks, bypassing the need for any signature. The MHMM technique is also designed to fit multivariate time series data that dynamically change over time, which is the norm of Industry 4.0 systems. It does this by accurately fitting data boundaries using the BMM, thus this improves estimating the posterior boundaries of normal and attack activities, especially mimicry attacks that cannot effectively detect using peer machine learning. However, this mechanism requires a huge number of normal and attack samples in order to accurately estimate the BMM and HMM parameters. It also needs a new function that enables running algorithm for adjusting the sliding window to be implemented real-world applications, as it is proven its capability of discovering physical and network attacks on both offline datasets.

VI. CONCLUSION

This paper has proposed a Beta Mixture-Hidden Markov Mechanism (MHMM) for designing threat intelligence that monitors and recognises cyber-attacks from Industry 4.0 systems. The mechanism was designed based on BMM for fitting physical and network data for addressing the problem of accurately estimating data boundaries of normal and attack data using HMM. It learns on normal and attacks data for discovering the posterior boundaries of normal and attack types, therefore it solves the issues of anomaly and signature-based detection. The performance of the proposed mechanism significantly improves while reducing and extracting important features through the ICA technique. This mechanism can competently discover physical and network attacks using the physical power system and UNSW-NB15 datasets. Its performance outnumbers five peer techniques in terms of detection rates, false positive rates and processing times deepening on its potential process of utilising BMM as the input of HMM for computing the posterior boundaries of normal and abnormal observations. Based on this, in future, we will extend this work for applying the mechanism on real Industry 4.0 systems that are in an early stage in the cybersecurity domain with architecture and data collections that validate threat intelligence, intrusion detection, and forensic systems in real-world applications.

REFERENCES

[1] H. Kagermann, J. Helbig, A. Hellinger, and W. Wahlster, *Recommendations for Implementing the Strategic Initiative INDUSTRIE 4.0: Securing the Future of German Manufacturing Industry; Final Report of the Industrie 4.0 Working Group*, document, Forschungsunion, 2013.
[2] L. Alonso and J. Barbarán, J. Chen, M. Díaz, L. Llopis, and B. Rubio, "Middleware and communication technologies for structural health monitoring of critical infrastructures: A survey," *Comput. Standards Interfaces*, vol. 56, pp. 83–100, Feb. 2018.
[3] P. Zheng *et al.*, "Smart manufacturing systems for industry 4.0: Conceptual framework, scenarios, and future perspectives," *Frontiers Mech. Eng.*, vol. 13, no. 2, pp. 137–150, Jun. 2018.
[4] P. O'Donovan, C. Gallagher, K. Bruton, and D. T. O'Sullivan, "A fog computing industrial cyber-physical system for embedded low-latency machine learning industry 4.0 applications," *Manuf. Lett.*, vol. 15, pp. 139–142, Jan. 2018.
[5] P. Harsha and M. Dahleh, "Optimal management and sizing of energy storage under dynamic pricing for the efficient integration of renewable energy," *IEEE Trans. Power Syst.*, vol. 30, no. 3, pp. 1164–1181, May 2015.
[6] N. Moustafa, J. Slay, and G. Creech, "Novel geometric area analysis technique for anomaly detection using trapezoidal area estimation on large-scale networks," *IEEE Trans. Big Data*, pp. 1–14, Jun. 2017, doi: 10.1109/TBDATA.2017.2715166.
[7] S. Helske and J. Helske. (2017). "Mixture hidden Markov models for sequence data: The seqHMM package in R." [Online]. Available: https://arxiv.org/abs/1704.00543
[8] W. Haider, J. Hu, Y. Xie, X. Yu, and Q. Wu, "Detecting anomalous behavior in cloud servers by nested arc hidden semi-Markov model with state summarization," *IEEE Trans. Big Data*, pp. 1–15, Aug. 2017, doi: 10.1109/TBDATA.2017.2736555.
[9] A. Hyvärinen and E. Oja, "Independent component analysis: Algorithms and applications," *Neural Netw.*, vol. 13, nos. 4–5, pp. 411–430, 2000.
[10] W. Fan, N. Bouguila, and D. Ziou, "Unsupervised anomaly intrusion detection via localized Bayesian feature selection," in *Proc. IEEE 11th Int. Conf. Data Mining (ICDM)*, Dec. 2011, pp. 1032–1037.
[11] U. Adhikari, S. Pan, and T. Morris. *Power System Datasets*. Accessed: Mar. 2018. [Online]. Available: https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets
[12] R. C. B. Hink, J. M. Beaver, M. A. Buckner, T. Morris, U. Adhikari, and S. Pan, "Machine learning for power system disturbance and cyber-attack discrimination," in *Proc. 7th Int. Symp. Resilient Control Syst. (ISRCS)*, 2014, pp. 1–8.
[13] N. Moustafa. (Mar. 2018). *UNSW-NB15*. [Online]. Available: https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/cybersecurity/ADFA-NB15-Datasets
[14] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection," in *Proc. MiLCIS-IEEE Stream, Military Commun. Inf. Syst. Conf.*, Canberra, ACT, Australia, Nov. 2015, pp. 1–6.
[15] M. Bromiley, "Threat intelligence: What it is, and how to use it effectively," SANS Inst., North Bethesda, MD, USA, Tech. Rep. 37282, 2016.
[16] N. Moustafa, G. Misra, and J. Slay, "Generalized outlier gaussian mixture technique based on automated association features for simulating and detecting web application attacks," *IEEE Trans. Sustain. Comput.*, pp. 1–13, Feb. 2018, doi: 10.1109/TSUSC.2018.2808430.
[17] J. Lee, B. Bagheri, and H.-A. Kao, "A cyber-physical systems architecture for industry 4.0-based manufacturing systems," *Manuf. Lett.*, vol. 3, pp. 18–23, Jan. 2015.
[18] S. Pan, T. Morris, and U. Adhikari, "Developing a hybrid intrusion detection system using data mining for power systems," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 3104–3113, Nov. 2015.
[19] R. Mitchell and I.-R. Chen, "Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 1, pp. 16–30, Jan./Feb. 2015.
[20] T. Marsden, N. Moustafa, E. Sitnikova, and G. Creech. (2017). "Probability risk identification based intrusion detection system for SCADA systems." [Online]. Available: https://arxiv.org/abs/1711.02826
[21] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of things security and forensics: Challenges and opportunities," *Future Generat. Comput. Syst.*, vol. 78, pp. 544–546, Jan. 2018.
[22] T. Qiu, N. Chen, K. Li, M. Atiquzzaman, and W. Zhao, "How can heterogeneous Internet of Things build our future: A survey," *IEEE Commun. Surveys Tuts.*, pp. 1–18, Feb. 2018, doi: 10.1109/COMST.2018.2803740.
[23] D. Shreenivas, S. Raza, and T. Voigt, "Intrusion detection in the RPL-connected 6LoWPAN networks," in *Proc. 3rd ACM Int. Workshop IoT Privacy, Trust, Secur.*, 2017, pp. 31–38.

[24] E. Adi, Z. Baig, and P. Hingston, "Stealthy denial of service (DoS) attack modelling and detection for HTTP/2 services," *J. Netw. Comput. Appl.*, vol. 91, pp. 1–13, Aug. 2017.
[25] E. Bertino and N. Islam, "Botnets and Internet of Things security," *Computer*, vol. 50, no. 2, pp. 76–79, 2017.
[26] S. Chawla, "Deep learning based intrusion detection system for Internet of Things," Ph.D. dissertation, 2017.
[27] D. Midi, A. Rullo, A. Mudgerikar, and E. Bertino, "Kalis—A system for knowledge-driven adaptable intrusion detection for the Internet of Things," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2017, pp. 656–666.
[28] M. P. K. Shelke, M. S. Sontakke, and A. Gawande, "Intrusion detection system for cloud computing," *Int. J. Sci. Technol. Res.*, vol. 1, no. 4, pp. 67–71, 2012.
[29] Z. Tan *et al.*, "Enhancing big data security with collaborative intrusion detection," *IEEE Cloud Computing*, vol. 1, no. 3, pp. 27–33, Sep. 2014.
[30] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST, Gaithersburg, MD, USA, Tech. Rep. SP 800-145, 2011.
[31] Q. Huang, C. Yang, K. Benedict, S. Chen, A. Rezgui, and J. Xie, "Utilize cloud computing to support dust storm forecasting," *Int. J. Digit. Earth*, vol. 6, no. 4, pp. 338–355, 2013.
[32] A. Patel, M. Taghavi, K. Bakhtiyari, and J. C. Júnior, "An intrusion detection and prevention system in cloud computing: A systematic review," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 25–41, 2013.
[33] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in *Proc. 1st Ed. MCC Workshop Mobile Cloud Comput. Conf.*, 2012, pp. 13–16.
[34] H. Liu, F. Eldarrat, H. Alqahtani, A. Reznik, X. de Foy, and Y. Zhang, "Mobile edge cloud system: Architectures, challenges, and approaches," *IEEE Syst. J.*, pp. 1–14, Feb. 2017, doi: 10.1109/JSYST.2017.2654119.
[35] B. Varghese and R. Buyya, "Next generation cloud computing: New trends and research directions," *Future Gener. Comput. Syst.*, vol. 79, pp. 849–861, Feb. 2018.
[36] G. Nascimento and M. Correia, "Anomaly-based intrusion detection in software as a service," in *Proc. IEEE/IFIP 41st Int. Conf. Depend. Syst. Netw. Workshops (DSN-W)*, Jun. 2011, pp. 19–24.
[37] S. Iqbal *et al.*, "On cloud security attacks: A taxonomy and intrusion detection and prevention as a service," *J. Netw. Comput. Appl.*, vol. 74, pp. 98–120, Oct. 2016.
[38] Z. Al Haddad, M. Hanoune, and A. Mamouni, "A collaborative framework for intrusion detection (C-NIDS) in cloud computing," *Int. J. Commun. Netw. Inf. Secur.*, vol. 8, no. 3, p. 130, 2016.
[39] S. Yi, C. Li, and Q. Li, "A survey of fog computing: Concepts, applications and issues," in *Proc. Workshop Mobile Big Data*, 2015, pp. 37–42.
[40] S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," in *Proc. Int. Conf. Wireless Algorithms, Syst., Appl.*, 2015, pp. 685–695.
[41] D. Kwon, H. Kim, J. Kim, S. C. Suh, I. Kim, and K. J. Kim, "A survey of deep learning-based network anomaly detection," *Cluster Comput.*, pp. 1–13, Sep. 2017, doi: 10.1007/s1058.
[42] R. Sandhu, A. S. Sohal, and S. K. Sood, "Identification of malicious edge devices in fog computing environments," *Inf. Secur. J. Global Perspective*, vol. 26, no. 5, pp. 213–228, 2017.
[43] A. S. Sohal, R. Sandhu, S. K. Sood, and V. Chang, "A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments," *Comput. Secur.*, vol. 74, pp. 340–354, May 2017.
[44] V. Balamurugan and R. Saravanan, "Enhanced intrusion detection and prevention system on cloud environment using hybrid classification and OTS generation," *Cluster Comput.*, pp. 1–13, Sep. 2017.
[45] G. Xu, P. Moulema, L. Ge, H. Song, and W. Yu, "Unified framework for secured energy resource management in smart grid," in *Proc. Smart Grid, Netw., Data Manage., Bus. Models*, 2017, pp. 73–96.
[46] S. Han, M. Xie, H. H. Chen, and Y. Ling, "Intrusion detection in cyber-physical systems: Techniques and challenges," *IEEE Syst. J.*, vol. 8, no. 4, pp. 1052–1062, Dec. 2014.
[47] *Zerynth*. Mar. 2018. [Online]. Available: https://www.zerynth.com/
[48] *Nodered*. Mar. 2018. [Online]. Available: https://nodered.org
[49] N. Moustafa, G. Creech, and J. Slay, "Big data analytics for intrusion detection system: Statistical decision-making using finite Dirichlet mixture models," in *Data Analytics and Decision Support for Cybersecurity*. Cham, Switzerland: Springer, 2017, pp. 127–156, doi: 10.1007/978-3-319-59439-2_5.
[50] A. Hyvärinen, "Fast and robust fixed-point algorithms for independent component analysis," *IEEE Trans. Neural Netw.*, vol. 10, no. 3, pp. 626–634, May 1999.
[51] M. Spitzer, J. Wildenhain, J. Rappsilber, and M. Tyers, "BoxPlotR: A Web tool for generation of box plots," *Nature Methods*, vol. 11, no. 2, pp. 121–122, 2014.
[52] R. Petersen, "Data mining for network intrusion detection: A comparison of data mining algorithms and an analysis of relevant features for detecting cyber-attacks," Ph.D. dissertation, Dept. Inf. Commun. Syst., Mid Sweden Univ., Sundsvall, Sweden, 2015.
[53] R. A. R. Ashfaq, X.-Z. Wang, J. Z. Huang, H. Abbas, and Y.-L. He, "Fuzziness based semi-supervised learning approach for intrusion detection system," *Inf. Sci.*, vol. 378, pp. 484–497, Feb. 2017.
[54] C. D. McDermott and A. Petrovski, "Investigation of computational intelligence techniques for intrusion detection in wireless sensor networks," *Int. J. Comput. Netw. Commun.*, vol. 9, no. 4, pp. 45–56, 2017.
[55] K. Singh, S. C. Guntuku, A. Thakur, and C. Hota, "Big data analytics framework for peer-to-peer botnet detection using random forests," *Inf. Sci.*, vol. 278, pp. 488–497, Sep. 2014.

NOUR MOUSTAFA received the bachelor's and master's degrees in computer science from the Faculty of Computer and Information, Helwan University, Egypt, in 2009 and 2014, respectively, and the Ph.D. degree in the field of cyber security from the University of New South Wales-Canberra in 2017. In 2011, he joined the Faculty of Computers and Information, Helwan University, as an Assistant Lecturer. He was a Senior Developer in the development field for developing .NET Web and desktop applications for seven years. He is currently a Post-Doctoral Fellow with the Australian Centre for Cyber Security, UNSW. His areas of interests include cyber security, in particular, network security, host- and network-intrusion detection systems, statistics, deep learning, and machine learning techniques. He is interested in designing and developing threat detection and forensic mechanisms to the Industry 4.0 technology for identifying malicious activities from cloud computing, fog computing, Internet of Things (IoT), and industrial control systems over virtual machines and physical systems.

ERWIN ADI received the B.Sc. degree in computer science from State of New York at Stony Brook, NY, USA, in 1992, the M.Sc. degree in communications technology from the University of Strathclyde, Glasgow, U.K., in 1998, and the Ph.D. degree in computer science from Edith Cowan University, Perth, Australia, in 2017. He was a Lecturer in network and Web security with Bina Nusantara University, Jakarta, Indonesia, for six years. He is currently a Post-Doctoral Researcher with the Research Group UNSW Canberra Cyber, University of New South Wales, Australia. He had shown to be dedicated in teaching: his supervised student received the best thesis award and a team of students under his coaching program went to the final stage of a national hacking competition. He received the Best Lecturer Award at an annual event and the Dean's List Award (top 2% student of the university) for three semesters from the State of New York at Stony Brook. He was invited to join the Golden Key National Honor Society.

BENJAMIN TURNBULL is currently a Senior Lecturer with UNSW Canberra Cyber, University of New South Wales. His research interests include novel cyber-security defense strategies, cyber simulation, and understanding the physical impact of cyberattack. As part of this, he investigates the nexus of cyber security and kinetic effect to understand the true impacts of cyberattack, best-practice automated analysis, and visual techniques to aid decision support. This involves research in the fields of digital forensics, cyber security, knowledge representation, and visual analytics domains. He was with the Defence Science and Technology Organisation, initially for the Computer Network Defense and Forensics Group and later for Automated Analytics and Decision Support.

JIANKUN HU received the Ph.D. degree in control engineering from the Harbin Institute of Technology, China, in 1993, and the master's degree in computer science and software engineering from Monash University, Australia, in 2000. He was a Research Fellow with the Delft University of Technology, The Netherlands, from 1997 to 1998, and also with Melbourne University, Australia, from 1998 to 1999. He is currently with Ruhr University, Bochum, Germany. He is a Full Professor and the Research Director of the Cyber Security Laboratory, School of Engineering and Information Technology, University of New South Wales, Australia. His main research interests are in the field of cyber security, including biometrics security. He has authored many papers in high-quality conferences and journals, including the IEEE Transactions on Pattern Analysis and Machine Intelligence in the abovementioned fields. He was a recipient of seven Australian Research Council (ARC) grants. He received the prestigious German Alexander von Humboldt Fellowship from Ruhr University from 1995 to 1996. He serves with the prestigious Panel of Mathematics, Information and Computing Sciences and the ARC Excellence in Research for Australia Evaluation Committee. He served on the Editorial Board for up to seven international journals, including the IEEE Transactions on Information Forensics and Security. He served as the Security Symposium Chair for the IEEE ICC and the IEEE Globecom.