The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence

Conference Paper · July 2016

DOI: 10.1109/CEC.2016.7743900

CITATIONS
58

READS
957

7 authors, including:

Hongmei He
De Montfort University
79 PUBLICATIONS **513** CITATIONS
SEE PROFILE

Tim Watson
The University of Warwick
49 PUBLICATIONS **673** CITATIONS
SEE PROFILE

Jorn Mehnen
University of Strathclyde
142 PUBLICATIONS **2,130** CITATIONS
SEE PROFILE

Bogdan Gabrys
University of Technology Sydney
197 PUBLICATIONS **4,492** CITATIONS
SEE PROFILE

The Security Challenges in the IoT enabled Cyber-Physical Systems and Opportunities for Evolutionary Computing & Other Computational Intelligence

Hongmei He*, Carsten Maple †, Tim Watson †, Ashutosh Tiwari*, Jörn Mehnen*, Yaochu Jin ‡, Bogdan Gabrys§
*Department of Manufacturing, Cranfield University, Cranfield, MK43 0AL, UK
Email: h.he@cranifeld.ac.uk
†Cyber Security Centre - WMG, University of Warwick, UK
‡Department of Computer Science, University of Surrey, UK
§School of Design, Engineering & Computing, Bournemouth University, UK

***Abstract*—Internet of Things (IoT) has given rise to the fourth industrial revolution (Industrie 4.0), and it brings great benefits by connecting people, processes and data. However, cybersecurity has become a critical challenge in the IoT enabled cyber physical systems, from connected supply chain, Big Data produced by huge amount of IoT devices, to industry control systems. Evolutionary computation combining with other computational intelligence will play an important role for cybersecurity, such as artificial immune mechanism for IoT security architecture, data mining/fusion in IoT enabled cyber physical systems, and data driven cybersecurity. This paper provides an overview of security challenges in IoT enabled cyber-physical systems and what evolutionary computation and other computational intelligence technology could contribute for the challenges. The overview could provide clues and guidance for research in IoT security with computational intelligence.**

I. Introduction

Internet of Things (IoT) has given rise to the fourth industrial revolution (Industrie 4.0) by connecting the factories and plants to the Internet. Industrie 4.0 presented a new concept of "Smart Factory". Such smart factories, connected with supply chains, are much more efficient and productive than traditional factories. In the connected manufacturing processes and supply chains, data flows from the machines and factory floor to the top level of cloud, and the information exchange occurs in all stakeholder (floor workers, managers), software systems and many aspects of supply chains, so that there is visibility across the entire process, which enables centralised control. Therefore, IoT and our cyber-physical environment bring great benefits by connecting people, processes and data. They offer an easier, safer, smarter, more productive and more prosperous lifestyle for everyone with real-time information and real-time management.

However, the increasing use of Internet and mobile devices means that the boundary of an enterprise is disappearing, and as a result, the risk landscape becomes unbounded. IoT enabled cyber-physical systems (CPS) are facing vulnerabilities and threats from the Internet. This has attracted much attention from researchers. For example, the European project E-CRIME provided cyber crime inventory and networks in non-ICT sectors. It is shown that the causes of system interference could be a virus, worm, trojan horse, software bomb, disrupting computer services, Denying Computer Services, and sabotage [17].

Advanced manufacturing systems are not secure like traditional systems now. Cybersecurity has become a critical challenge in IoT enabled CPS, which could be threatened by a wide variety of cyber-attacks from criminals, terrorists and hacktivists. As a consequence, Cybersecurity is critical for the success of smart manufacturing. Cyber threats to the Industrial IoT are real, global and growing, including theft of trade secrets and intellectual property, hostile alterations to data, and disruptions or denial of process control [6]. Now the public and senior decision-makers become ever more aware of the security threats caused by the malicious exploitation of poorly-secured systems.

To secure smart manufacturing systems, Industrie 4.0 raised two demands for cybersecurity: "Security Architecture" and "Security by Design" in future smart systems [22]. This will require systems to have automatic detection of malware, threats and attacks with zero-installation. Computational intelligence will play important roles for cyber intelligence - tracking, analysing, identifying digital security threats to combat viruses, hackers and terrorists that exist on the Internet for different purposes, apart from the cyber threats to Industrial IoT mentioned above, including cyberstalking and harassment, extortion, blackmail, stock market manipulation, complex corporate espionage, and planning or carrying out terrorist activities.

Evolutionary Computation and other Computational Intelligence techniques (EC&CI) have been successfully applied in various areas, such as computational biology, medical science, finance, engineering, etc. Cybersecurity is another key area where we can exploit the power of EC&CI. Unlike other problem domains, the design of intelligent solutions for Cybersecurity has to be resilient in the face of determined, sophisticated attackers who may target any adaptive cyber-physical systems. Cyber Intelligence is expected to be able to secure the benefits to all from our cyber-connected world. Combining EC&CI with Cybersecurity will help underpin our safe, secure and prosperous connected future.

In the following sections, we will overview the security challenges in IoT enabled cyber-physical systems, and explore what Evolutionary Computation & other Computational Intelligence techniques can contribute for the challenges.

II. Security Challenges for IoT Enabled Manufacturing

A. Challenges in Supply Chains

Supply chain is the network of organisations that are involved through upstream and downstream relationships in the different processes and activities that produce value in the form of products and services in the hands of the ultimate customer, defined in [16]. A distinct feature of Smart Manufacturing is that the manufacturing processes are connected to the suppliers through the Internet. All people within the connected supply chains are aware of the dependencies, flow of inventory (raw materials, parts and products) and production cycles instantly. Hence, IoT enables real-time monitoring of shipment through using a combination of sensors and communication channels to produce real-time information. Such real-time information will help manufacturers reduce inventory costs and identify/resolve issues before they happen. Suppliers will have increased visibility of material consumption on the plant floor and can replenish stock just-in-time. IoT will enable manufacturers to automatically recognise the need to order and restock materials and products on a "machine-to-machine" basis, reducing the need for human interaction. Such proactive replenishment will ensure that the production line does not stop due to lack of spares or parts in the inventory. Pervasive visibility and proactive replenishment are the two major benefits of IoT to the Manufacturing Supply Chain [2] (Fig. 1).

However, organisations or enterprises within the connected supply chain will have different levels of security. A determined aggressor, e.g. an advanced persistent threat (APT), usually identifies the organisation with the weakest cyber-security within the supply chain, and uses these vulnerabilities presented in their systems to gain access to other members of the supply chain. The smaller organisations within a supply chain, due to more limited resources, often have the weakest cyber-security arrangements [12]. It is reported that small organisations account for 92 percent of the total number of cyber incidents [3].

Recently identified supply chain compromises were approached in the following ways [12]:

(1) The third party software provider: In mid-2014, the cyber-espionage group, Dragonfly, had allegedly been targeting companies across Europe and North America, mainly in the energy sector, since 2011. This group has a history of targeting companies through their supply chains. In the latest campaign, Dragonfly was able to "trojanise" legitimate industrial control system (ICS) software. They were able to compromise the websites of the ICS software suppliers and replace legitimate files in their repositories with those that had malware added to them. The ICS software could then be downloaded from the suppliers' websites and install the malware alongside the ICS software. The malware included additional remote access functionalities that could be utilised to take control of the systems where it was installed.

(2) Website builders: The Shylock banking Trojan is a good example. The Shylock attackers compromised legitimate websites through website builders used by creative and digital agencies and employed a redirect script sending victims to a malicious domain owned by the Shylock authors. From there, the Shylock malware was downloaded and installed onto the systems of those browsing the legitimate websites.

(3) Third party data stores: In Sept 2013, a number of networks belonging to large data aggregators were reported as having been compromised. A small botnet was observed exfiltrating information through an encrypted channel from the internal systems to a botnet controller on the public Internet.

(4) Watering hole attacks: The attacker identifies weaknesses in cybersecurity of the main target, and then manipulates the website chosen as a watering hole to deliver the malware that will exploit these weaknesses onto the target's system.

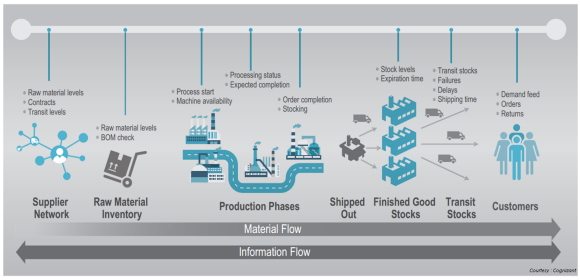

Fig. 1. IoT Manufacturing Supply Chains [2]

B. Challenges in Big Data

It is estimated that the number of connected devices will increase to 40 billion by 2020 [10]. A huge number of connected devices (including sensors) will produce huge amount of data. The amount of data generated by machines will be orders of magnitude greater than that generated by humans in future, and data generated by sensors is different to that generated by human. The storage of Big Data is a challenge. Real-time response to health diagnosis or to natural disaster is critical for data processing and analysis. Asynchronisation of temporal and spatial information could bring challenge in data analysis. As the uncertainty of the data may be unpredictable, data retrieval and feature extraction are critical components in data analysis. The goal of data mining/fusion is to make decision for the actions of machines or humans. Therefore, accurate and timely decision making is a tremendous challenge for data mining or fusion. Many analytic algorithms are running with the data on a server, requiring both power and bandwidth to communicate the data to the server. Intelligent computation should be distributed across both the devices and the cloud. Although IoT devices have now become more powerful, high performance intelligent computation is still desired, especially in memory use and running time.

Koster [26] presented a reference model of IoT infrastructure (Fig. 2) when discussing data models for IoT. Every interface between components in the IoT stack will produce information exchange (denoted as an arrow). Every point that has information exchanges could be a cyber vulnerability.

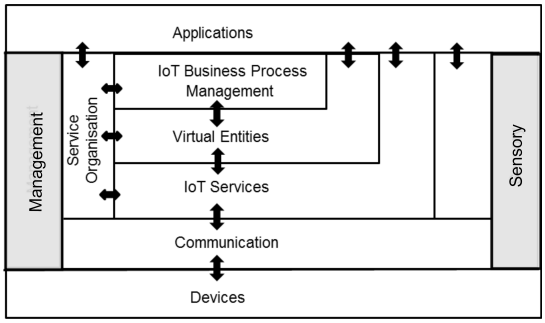

Fig. 2. A Reference Model for IoT Infrastructure [26]

Regarding data flow from bottom to top, Chen [13] simplified IoT system structure to four levels: Sensors collect data, communication units relay the information collected, computing units analyse the information, and service layers take action, and summarised the challenges in each layer. These four levels could be the classic vulnerabilities in the whole IoT infrastructure. It is notable that Chen introduced a new level of computation, which is the new property of IoT enabled systems with Big Data Analytics to guide machine or human action. The level of computation is corresponding to the level of IoT business processing and management in the IoT stack (Fig. 2). Data protection and privacy is one of IoT challenges as Chen suggested.

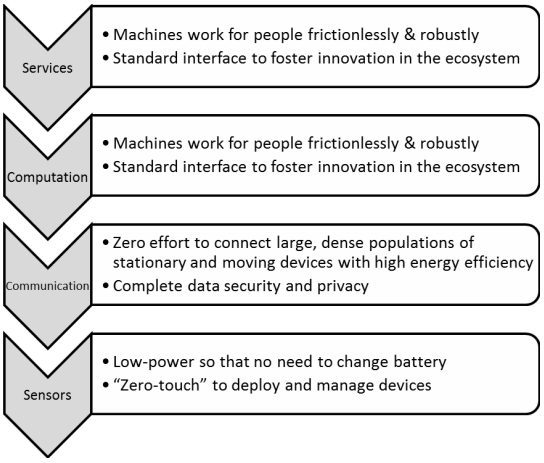

Fig. 3. IoT Challenges [13]

Fig. 1 presents the horizontal information flow in manufacturing supply chain, while Fig. 2 presents the vertical information flow in an IoT system. Both data flows form the IoT data network. Attackers could steal data from any possible point in the IoT data network. Hence, data protection is a major task in Cybersecurity. The protection of data flow in supply chains is critical for the success of different sectors enabled by IoT. For example, smart city could be the most beneficial to our life, brought by the IoT technology. However, one of challenges to make smart city towards reality is the public - private and privacy issues of connecting travellers, cities and transport providers in IoT enabled smart cities [18]. The construction sector is rapidly evolving due to the need to reduce the cost of public sector assets. In future, the close connection between stakeholders of construction will form a more transparent, open and cross-sector collaborative digital built environments, sharing of both detailed models and large amounts of digital information to implement real-time information and real-time management in the life-cycle of construction. Therefore, appropriate and proportionate countermeasures are needed to reduce the risk of loss or disclosure of information, which could impact on the safety and security of personnel and other occupants or users of the built asset and its services [1].

All industries are affected by privacy and data protection requirements, and protecting sensitive data is an objective that governments and business share. According to Verizon's 2015 report [3], the estimated $400 million financial loss from 700 million compromised records, conducted by Verizon with contributions from 70 organisations around the world, shows the real importance of managing data breach risks. Many industry associations, such as the Payment Card Industry (PCI), the Healthcare Information Trust Alliance (HITRUST), Telecommunications Service Company Privacy Regulation (Germany), Information Commissioners Office (UK), and Privacy and Electronic Communication Regulation (UK) have issued their own standards to supplement existing laws and regulations [35].

More than ever, intangible assets, such as customers, systems, and data form the foundation, on which corporate value is built in IoT enabled manufacturing. The new concept of "Security by Design" in Industrie 4.0 requires that security risks should be addressed at every level and across all interfaces, horizontally and vertically, while the system is being built.

C. Challenges in Industry Control Systems

The IoT is where the Internet meets the physical world. This has some serious implications on security as the attack threat moves from manipulating information to controlling actuation (i.e, moving from the digital to the physical world). Consequently, it drastically expands the attack surface from known threats and known devices, to additional security threats of new devices, protocols, and work-flows. Many manufacturing systems are moving from closed systems (e.g., SCADA, Modbus, CIP) into IP-based cyber-physical systems, which further expand the attack surface. Fig. 4 shows the evolution from a legitimate Industry Control System (ICS) to a modern ICS. Cybersecurity risks are brought to the modern ICS while a legitimate ICS is incorporated with IT capacity. Hence, cybersecurity is critical for the success of modern ICS enabled by IoT. The state of vulnerability is exacerbated by the fact that legitimate ICS is typically older equipment and isn't well secured against modern networked environments [25]. This is because the components of a traditional ICS are communicated with specific protocols without any security concern. For example, a malicious actor can attack a connected automatic car through the wireless network, and directly intrude the control system. The focus in automotive industry is now starting to

shift from the physical protection of vehicles, drivers and passengers to the security protection against cyber-attacks and intrusions [4]. Therefore, a big challenge is how to protect legitimate ICS from attacks when they are connected to the Internet.

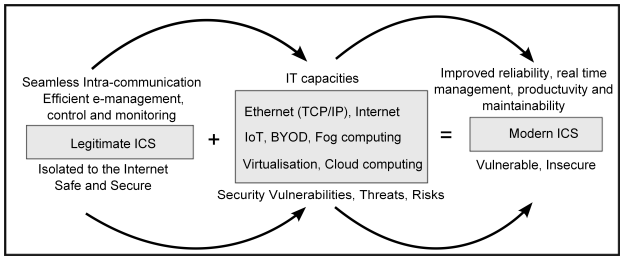

Fig. 4. Evolution from Legitimate ICS to Modern ICS [8]

Cyber threats to modern ICS are globally increasing. It is reported that attacks specifically targeting SCADA industrial control systems rose 100 percent in 2014 compared to the previous year, and countries most affected were Finland, the UK and the US [25]. Such attacks are trying to overwhelm SCADA systems and can cause a disruption or denial of service. For example, a malicious actor had infiltrated a German steel facility in 2014. The adversary used a spear phishing email to gain access to the corporate network and then moved into the plant network. The adversary showed knowledge in ICS and was able to cause multiple components of the system to fail. This specifically impacted critical process components to become unregulated, which resulted in massive physical damage [28].

In Fiscal Year 2014, the US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) received and responded to 245 incidents, reported by asset owners and industry partners. The Energy Sector led all others again in 2014 with the most reported incidents, and the critical manufacturing was at the second most place. Fig. 5 shows FY 2014 incident distribution in different sectors in total 245 incidents [34].

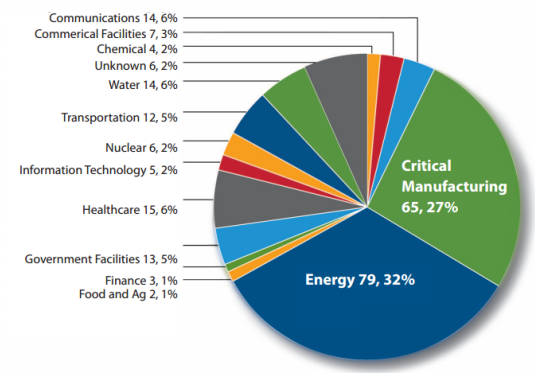

Fig. 5. FY 2014 incidents reported by sector (245 total) [34]

III. Opportunities for EC&CI

A. Cybersecurity architecture

Security is critical for the success of smart manufacturing in Industrie 4.0. A good "Security Architecture" will make it easy to implement "Security by Design" for future cyber-physical systems. IoT security architecture should be featured with feasibility, robustness and extendibility under the goal of cybersecurity to make the availability, integrity, confidentiality and accountability of the protected systems and data. To fulfil the target of fastest Time-to-market, highest Quality, lowest Cost, best Service, cleanest Environment and high Knowledge (TQCSEK), many manufacturing models and technologies have been investigated [42]. However, few investigations were conducted on security architecture for IoT. Cisco [32] generalised the IoT architecture to four levels.

- Embedded systems layer: comprised of embedded systems, sensors and actuators,
- Multi-service edge layer (multi-modal): to support both wired and wireless connectivity, security and scalability),
- Core Network Layer: to provide paths to carry and exchange data and network information between multiple sub-networks. It is corresponding to the level of the business process and management in the IoT stack (Fig. 2),
- Data Centre Cloud layer: to host applications that are critical in providing services and to manage the end-to-end IoT architecture.

Cisco enriched the meaning of each level in the IoT architecture, comparing to the four levels of IoT architecture in [13]. Security should be a major concern crossing all levels of IoT. As illustrated in Fig. 6, Cisco proposed four components: Authentication, Authorisation, Network Enforced Policy, and Secure Analytics: Visibility and Control, to secure the IoT environment.

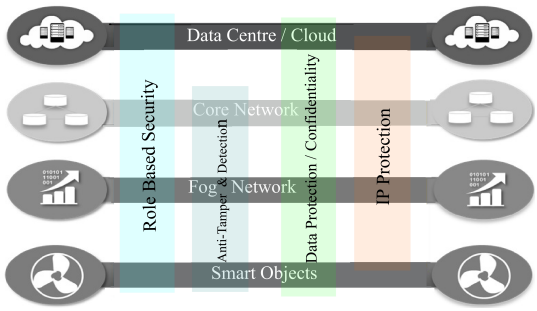

Fig. 6. IoT Security Environment [32]

Fig. 7 shows the Cisco's framework with the four components. It could be the foundation to the execution of security in IoT environments. However, a mechanism is needed to allow the security components to be seamlessly integrated into the IoT architecture, and thus to implement "Security by Design", demanded by Industrie 4.0. Also, an automatic security incident response mechanism for IoT is needed, thus to improve incident response when an IoT enabled system is attacked. An artificial immune mechanism for IoT is worthy to investigating. The IoT immune system should be adaptive and self-learning. Liu et al. [30] proposed an artificial immunity-based security response model for IoT.

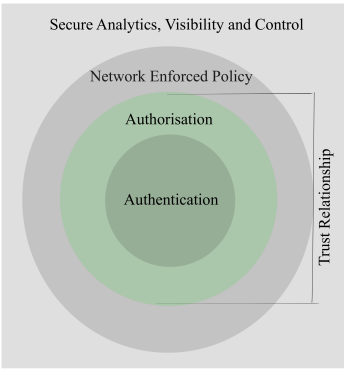

Fig. 7. IoT Security Framework [32]

B. Data mining

In the IoT paradigm, enormous amounts of data have to be stored, processed and presented in a seamless, efficient, and easily interpretable form [19]. Therefore, evolutionary computation and other computational intelligence techniques, such as neural networks, fuzzy logic & systems, and semantic computing will help meet the requirements. "Turn Data to Opportunities" is the goal of business intelligence (BI). Advanced analytics with EC&CI will provide the edge in extracting insights from data, identifying risk, capitalising on opportunities and gaining a deep understanding of a business with reports, dashboards, visualisations and analysis of information.

With IoT equipped with computational intelligence, better, faster decisions are coming to manufacturing shop floors. In the supply chain networks, data flows are actively influence the whole manufacturing processes and materials flows. Better decisions mean fewer mistakes and less waste. The payoff for manufacturers who implement Industrial IoT solutions lies in better decision-making, for which computation intelligence will be the cutting-edge techniques of Knowledge Discovery in Databases (KDD). Tsai et al. [41] generalised an architecture of IoT with KDD (Fig. 8).

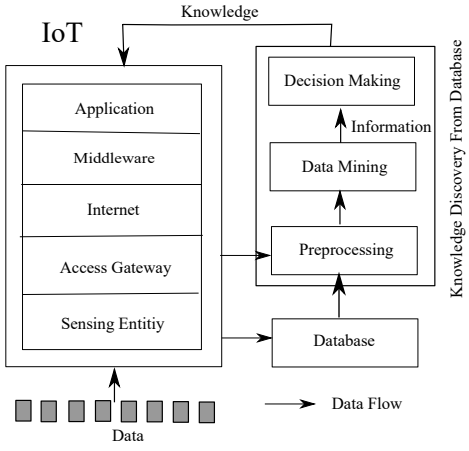

Fig. 8. An architecture of IoT with KDD [41]

Evolutionary computation is useful for optimising the parameters of manufacturing processes. A just-in-time adaptable system will also be useful for automatically updating parameter settings, thus to maximise productivity, minimise energy consumption and promote safety. Briefly, Computational Intelligence for collecting, analysing and managing data from devices and sensors is a core element in the IoT data-information-decision-action loop, where 'SMART' comes from.

The capacity of the cloud to store and process data is virtually unlimited. Storing and processing data remotely is generally more economical, flexible and secure than on-site alternatives. The cloud is also more readily scalable, that is, its capacity can be expanded rapidly to meet growing demand. However, network data flow and bandwidth are challenges for transferring huge amount of data from connected devices. Fog computing provides a new concept, to allow intelligence to down to the devices. This requires computational intelligence algorithms to use small size of memory with real-time performance. Therefore, high performance of computational intelligence algorithms for IoT devices is another topic that is worthy to investigation.

C. Data Driven Cybersecurity

Cyber intelligence is to track, analyse and identify digital security threats. Since data from IoT devices or in the cloud provide various clues of cybersecurity threats, data-driven cybersecurity has great potentials for protecting IoT assets. Hence, computational intelligence will have the power to support data driven cybersecurity. In the four security components of the IoT security framework, proposed by Cisco [20], identity authentication and secure analytics will be better powered by computational intelligence techniques on pattern recognition and data mining/fusion.

Authentication: Authentication is the process of an individual claiming to have a certain identity, and then biometrically validating the users' identity is what they claim it to be. Genetic algorithms have been used for identification in software or computer forensics [27], [9]. From fingerprints, to facial scanning, to voice, biometrics are the unique parts of a human body that identifies an individual person. These have been leveraged by law enforcement for years. Biometrics authentication involves confirming or denying a person's claimed identity based on his/her physiological or behavioral characteristics [15]. Fujitsu developed the world's first authentication technology to extract and match 2,048-bit feature codes from palm vein images [23]. However, it is possible to fake a single fingerprint or wave a photo of an individual in front of an unsophisticated finger or facial recognition program, then the device could be accessed. No single method of access is ever going to be completely secure. Multi-modality biometrics identification has attracted much attention [14], [15], [31], [33]. Moreover, now online identity is not limited to electronic usernames, passwords, or online responses. There is a significant evolution from traditional concepts of self-identity to new digital identity management approaches. Now identity is a complex concept, reflecting issues of stability, context, privacy and ownership, across cyber and physical domains. The concept of cyber-identity is important in this regard, and it could be represented by how individuals choose to present themselves in an online forum, or what they decide to self-disclose in a chat room. Cyber-metrics captures aspects of these cyber-identities, and

provides additional information to identity authentication [11]. Computational intelligence particularly works for the fusion of identity modalities across cyber and physic domains.

Secure Analytics Manufacturing industry should consider how to protect their data, their systems and their networks at every step toward becoming part of the Industrial IoT. Connecting machine tools to a network or cloud-based application creates a number of vulnerabilities, which are often overlooked. For example, network connections installed in a CNC machine may require a firewall to block unauthorised access while permitting outward communication. Machine tool data is especially sensitive because it involves critical information about product design. CNC tool paths and inspection routines for measurement probes represent the dimensions and attributes of the intended component, and are thus a tempting target for hackers. Data-driven approach to network security can identify hackers in the network before essential systems have been breached and the reputation of an organisation is compromised. In-depth understanding of hacker behaviors and methods is helpful for identification of cybersecurity risks. Therefore knowledge-based Computational Intelligence will be a good approach to identifying hacker's behaviours from Big Data. This could provide a sophisticated protection of IoT systems through identifying breaches, insider threat, and vulnerabilities in networks, and warn users to intrusions before they reach critical data or impact business' operations and reputation.

There has been a lot of research on cybersecurity with evolutionary computation and other computational intelligence techniques. For example, Akyaz and Uyar [5] proposed an Artificial Immune System-inspired multi-objective evolutionary algorithm to detect DDoS attacks; Genetic Algorithms can be used to evolve the rules that determine whether the network connections and related behaviours are intrusions or not [29], [7]; Computational Intelligence techniques have been widely used for spam detection. For example, Kolari et al [24] used SVM-based approach for blog spams; Tran et al. [39] proposed a domain-feature based approach to detecting advertisement spam; Jindal and Liu [21] investigated review spam by detecting duplicated review and classifying review with machine learning technology; Shirani-Mehr [37] investigated SMS Spams with Naive Bayes algorithm; Sharifi et al. [36] used Logistic Regression approach to detecting Internet scam; and Tretyakov [40] used the combination of the most classic machine learning techniques (Bayesian classifier, k-NN, ANNs, SVMs) for the problem of email spam-filtering.

Data should be protected in static and communication. Except data encryption, secure communication protocol is very important. There has been some research on it. For example, Szałachowski et al. [38] proposed an adaptable security model to optimise the TLS security protocol. Evolutionary Computation is powerful for optimisation problems, and many classification or decision making problems can be transferred to optimisation problems for improving accuracy, reducing error rates, or obtaining a tradeoff of multi-objectives. Hence, Evolutionary Computation combining with other computational intelligence techniques will be powerful for cybersecurity in the identification of risks, the detection of intrusion or attacks, and the optimisation of secure protocol, etc.

IV. Conclusions

The overview of security challenges in IoT and opportunities of EC&CI was based on a survey on the latest investigation on IoT and industrie 4.0. Cybersecurity is critical for the success of Industrie 4.0 enabled by IoT. Three aspects of IoT were be viewed. One of important features of IoT enabled smart manufacturing lies in that manufacturing processes are connected manufacturing supply chains. There exist many vulnerabilities in the connected supply chains. Huge amount of data will be produced by IoT devices. Big Data retrieving, storage, processing and fusion, as the core of intelligence, are challenge issues. Especially the introduction of Fog Computing will require improving the performance of computational intelligence algorithms in memory use and running time. More importantly, the legitimate ICS with poor security protection when they are incorporated with modern IT technology will face great security challenge.

IoT brings exciting benefits, but faces great security challenges at the same time. To achieve the success of smart manufacturing, Evolutionary Computation and other Computational Intelligence techniques will play important roles in cybersecurity and business intelligence. An IoT security architecture with immune mechanism is demanded to implement zero installation of cybersecurity tools, and thus to support the demand of Industrie 4.0 for "Security by Design". Data Mining is important for business intelligence in Industry IoT or Cloud Manufacturing, and Computational Intelligence provides cutting-edge techniques for business intelligence and cyber intelligence, which are core elements in the smart cyber-physical systems.

References

[1] Digital built assets and environments. CPNI,Centre of the Protection of National Infrastrucutre, www.cpni.gov.uk/advice/Cross-cutting-advice/Digital-built-assets-and-environments. Accessed on 25 Mar 2016.

[2] Smart manufacturing - iot enables fourth industrial revolution. www.smarttechforyou.com/2015/03/smart-manufacturing-iot-fourth-industrial-revolution.html, Feb 2005.

[3] Verizon 2015 data breach investigations report. www.verizonenterprise.com/DBIR/2015/, 2015.

[4] ABIresearch. Connected car cybersecurity. www.abiresearch.com/market-research/product/1017985-connected-car-cybersecurity. Accessed on 25 Mar 2016.

[5] U. Akyaz and A. Uyar. Detection of ddos attacks via an artificial immune system-inspired multiobjective evolutionary algorithm. In Cecilia Di Chio et al., editor, *EvoApplications 2010*, volume Part II of *LNCS 6025*, pages 1–10, Istanbul, Turkey, Apr. Springer-Verlag Berlin Heidelberg.

[6] M. Albert. Seven things to know about the internet of things and industry 4.0. *Modern Machine Shop Magazine*, 88(4):74, Sept 2015.

[7] S. Al amro, D. A. Elizondo, A. Solanas, and A. Martnez-Ballesté. Evolutionary computation in computer security and forensics: An overview. In D.A. Elizondo et al., editor, *Computational Intelligence for Privacy and Security*, SCI 394, pages 25–34. Springer-Verlag Berlin Heidelberg, 2012.

[8] U. P. D. Ani. Cyber security assurance in critical manufacturing infrastructure. first year phd report, Cranfield University, Nov. 2015.

[9] L. Ballerini, O. Cordon, J. Santamaria, S. Damas, I. Aleman, and M. Botella. Craniofacial superimposition in forensic identification using genetic algorithms. In *The Third International Symposium on Information Assurance and Security*, pages 429–434. IEEE Computer Society, California, 2007.

[10] R. J. Baxter. Bluemix and the internet of things. developer.ibm.com/bluemix/2014/07/16/bluemix-internet-things/, July 2014. Accessed in Jan 2016.

[11] S. Black, S. Creese, R. Guest, B. Pike, S. Saxby, D. Stanton Fraser, S. V. Stevenage, and M. T. Whitty. Superidentity: Fusion of identity across real and cyber domains. In *ID360 - The Global Forum on Identity*, Austin, US, 23 - 24 Apr 2012.

[12] CERT-UK. Cyber-security risks in the supply chain. www.cert.gov.uk/wp-content/uploads/2015/02/Cyber-security-risks-in-the-supply-chain.pdf, FEb 2015.

[13] Y.-K. Chen. Challenges and opportunities of internet of things. In *2012 17th Asia and South Pacific Design Automation Conference (ASP-DAC)*, pages 383 – 388, Sydney, Australia, 30 Jan -2 Feb 2012.

[14] G. Chetty and M. Wagner. Audio-visual multimodal fusion for biometric person authentication and liveness veriftion. In *Proceedings of the 2005 NICTA-HCSNet Multimodal User Interaction Workshop*, volume 57, pages 17–24. Australian Computer Society, Inc., 2005.

[15] G. Chetty and M. Wagner. Audio-visual multimodal fusion for biometric person authentication and liveness veriftion. *International Journal of Advanced Science and Technology*, 48:23–60, Nov. 2012.

[16] M. Christopher. Logistics and supply chain management - creating value-adding networks. Prentice Hall, London, 2005.

[17] EU FP7 E-Crime. The economic impacts of cyber crime, d2.2 executive summary and brief: Cyber crime inventory and networks in non-ict sectors. ecrime-project.eu/wp-content/uploads/2015/02/E-CRIME-Deliverable-2.2.pdf. Accessed, 25 Mar 2016.

[18] EU FP7. Petra project (01-02-2014 - 31-01-2017). petraproject.eu/index.php. Accessed, 25 Mar 2016.

[19] J. Gubbia, R. Buyyab, S. Marusica, and M. Palaniswamia. Internet of things (iot): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7):1645–1660, 9 2013.

[20] J. Jacobs and B. Rudis. *Data-Driven Security: Analysis, Visualization and Dashboards*. ISBN: 978-1-118-79372-5. WILEY, 2014.

[21] N. Jindal and B. Liu. Review spam detection. In *WWW 2007*, ACM 978-1-59593-654-7/07/0005, Banff, Alberta, Canada, 8-12 May 2007.

[22] 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. Forschungsunion, Apr 2013.

[23] Kawasaki. Fujitsu develops world's first authentication technology to extract and match 2,048-bit feature codes from palm vein images. Fujitsu Laboratories Ltd, Aug. 2013. accessed in Jan 2016.

[24] P. Kolari, A. Java, T. Finin, T. Oates, and A. Joshi. Detecting spam blogs: a machine learning approach. In *Proceeding of AAAI'06 proceedings of the 21st national conference on Artificial intelligence*, volume 2, pages 1351–1356, 2006.

[25] M. Korolov. Dell report: Attacks against industrial control systems double. powermore.dell.com/technology/dell-report-attacks-against-industrial-control-systems-double/, 2015. accessed in Jan 2016.

[26] M. J. Koster. Data models for the internet of things. iot-datamodels.blogspot.co.uk/2012/09/data-models-for-internet-of-things-5.html, Sept 2012. Accessed in Jan 2016.

[27] R. Lange and S. Mancoridis. Using code metric histograms and genetic algorithms to perform author identification for software forensics. In *Proceedings of the 9th Annual Conference on Genetic and Evolutionary Computation*, pages 2082–2089, 2007.

[28] R. M. Lee, M. J. Assante, and T. Conway. Ics defense use case (duc) : German steel mill cyber attack. Report, SANS, DEC 2014.

[29] W. Li. Using genetic algorithm or network intrusion detection. In *Proceedings of the United States Department of Energy Cyber Security Group*, pages 1–8, 2004.

[30] H.-C. Liu, L. Liu, and J. Wu. Material selection using an interval 2-tuple linguistic vikor method considering subjective and objective weights. *Materials and Design*, 52:158–167, 2013.

[31] S. Marcel, J. Mariethoz, Y. Rodriguez, and F. Cardinaux. Bi-modal face and speech authentication: A biologin demonstration system. In *Proceedings of the Second Workshop on Multimodal User Authentication*, Mar. 2006.

[32] M. Morrow. Securing the internet of things: A proposed framework. www.cisco.com/web/about/security/intelligence/iot_framework.html, May 2015.

[33] K. Nandakumar, Y. Chen, S. C. Dass, and A. K. Jain. Likelihood ratio based biometric score fusion. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 30(2):342–347, Feb 2007.

[34] NCCIC. Incident response / vulnerability coordination in 2014. ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf, Sept 2014. Accessed in Jan 2016.

[35] Protiviti. Intelligent computation. www.protiviti.co.uk/en-US/Documents/POV/POV-Privacy-and-Data-Protection-Protiviti.pdf. accessed in Jan 2016.

[36] M. Sharifi, E. Fink, and J. G. Carbonell. Detection of internet scam using logistic regression. In *2011 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pages 2168 – 2172, Oct 2011. 10.1109/ICSMC.2011.6083998.

[37] H. Shirani-Mehr. Sms spam detection using machine learning approach.

[38] P. Szałachowski, B. Księżopolski, and Z. Kotulski. Optimization of tls security protocol using the adaptable security model. *Annales UMCS, Informatica*, 9(1):59–75, Jan 2009.

[39] H. Tran, T. Hornbeck, V. Ha-Thuc, J. Cremer, and P. Srinivasan. Spam detection in online classified advertisements. In *Proceedings of the 2011 Joint WICOW/AIRWeb Workshop on Web Quality (WebQuality'11)*, ISBN: 978-1-4503-0706-2, pages 35–41. ACM New York, NY, USA, 2011. 10.1145/1964114.1964122.

[40] K. Tretyakov. Machine learning techniques in spam filtering. In *Data Mining Problem-oriented Seminar, MTAT.03.177*, pages 60–79, May 2004.

[41] C.-W. Tsai, C.-F. Lai, M.-C. Chiang, and L. T. Yang. Data mining for internet of things: A survey. *IEEE Coomunications Surveys & Tutorials*, 16(1):77–97, 2014.

[42] L. Zhang, Y. Luo, F. Tao, B. H. Li, L. Ren, X. Zhang, H. Guo, Y. Cheng, A. Hu, and Y. Liu. Cloud manufacturing: a new manufacturing paradigm. *Enterprise Information Systems*, 8(2):167–187, 2014.