Journal of Information
2015 Vol.1, No.2, pp.59-70
ISSN(e): 2520-7652
DOI: 10.18488/journal.104/2015.1.2/104.2.59.70

BIG DATA IN HOMELAND SECURITY

Lidong Wang[1]† --- Cheryl Ann Alexander[2]

[1]*Department of Engineering Technology, Mississippi Valley State University, USA*

[2]*Technology and Healthcare Solutions, Inc., USA*

ABSTRACT

Big Data predicts outcomes and has great impacts on knowledge discovery and value creation. It can be used to fight against terrorism and enhance Homeland Security by providing accurate predictions and patterns of terrorist activities. This paper introduces some methods and technologies used in Homeland Security. They are: biometrics, radio frequency identification (RFID), data mining, cloud computing, and Big Data. Big Data applications in Homeland Security are presented. These applications include Big Data in general security and public safety, crime prediction and aviation security, disasters, and cybersecurity and cyber defense. Big Data challenges in security are also discussed.

Keywords: Big data, Homeland security, Information technology, Information security, Data mining, Cybersecurity, Cyber defense, Cloud computing.

Contribution/ Originality

This study contributes in the existing literature and presents technology progress and applications of Big Data in Homeland Security, especially in cybersecurity and cyber defense.

1. INTRODUCTION

Homeland Security has gained much attention since the tragic events of September 11, 2001. Critical mission areas, as suggested by the U.S. Office of Homeland include border and transportation security, intelligence and warning, protecting critical infrastructure (including cyberspace), domestic counter-terrorism, defending against catastrophic terrorism, and emergency preparedness and response [1].

Critical infrastructure protection is the foundation of national security. Critical infrastructure is systems and assets, whether physical or virtual, so vital to a country that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters [2]. The

† Corresponding author

critical infrastructures include [3]: (1) administration (basic services, facilities, information networks, assets, important places, and national monuments); (2) transportation (airports, ports, intermodal facilities, railways, mass transit networks, and traffic control systems); (3) production, storage and transport of dangerous goods (chemical, biological, and radiological and nuclear materials); (4) food (food security, means of production, distribution and food industry); (5) installations and networks in the energy sector; (6) technologies for communications and information; (7) the health care sector; (8) the financial sector; and (9) water supplies.

In order to protect critical infrastructure from different cyber-attacks, system administrators can use many technologies and tools. Current technologies, like secure access control, remote system management and checking system integrity help administrators and security experts to avoid unauthorized access to information and data inside such infrastructures [4].

It is also necessary to improve the resilience of critical infrastructure, i.e. the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions (e.g., all hazard events including a terrorist attack, a natural hazard, or a technological failure) [5].

Sharing data and information between countries is a major challenge, as shown by the terrorist bombing attack on the Boston Marathon in April 2013. The Boston Marathon tragedy might have been prevented if the Russian secret services had shared critical information about the terror suspects with U.S. intelligence agencies. National governments must be prepared and willing to share data and build systems for crime prevention and fighting [6].

2. SOME METHODS AND TECHNOLOGIES IN HOMELAND SECURITY

Biometrics can be used in visas and e-passports for border security, identity verification at airports, access control and safety for personnel in basic military training, and security for facilities in troops. Radio frequency identification (RFID) technology speeds the movement of people crossing borders, tracks baggage and polices airport access, provides better management of wounded soldiers and supply chains in military, detects unauthorized shipments for marine security, and improves disaster tracking, response and relief operations [7].

Biometric identification and authentication are increasingly used due to the advanced devices that can extract biometric information from a multitude of sources such as voice, fingerprints, and iris. While biometry serves as an excellent mechanism for identification of individuals, biometric data is extremely sensitive and must be subject to minimal exposure. As a result, biometric data must be protected from arbitrary disclosure. Consider, for instance, an agency that needs to determine whether a given biometric appears on a government watch-list. As agencies may have different clearance levels, privacy of biometrics owner needs to be preserved if no matches are found; unrestricted access to the watch-list cannot be granted. There are many legitimate scenarios where biometric data should be shared, in a controlled way, between different entities [8]. Advances in biometric recognition enable the use of biometric data as a practical mean of authentication and identification. Today, several governmental agencies around the world

perform large-scale collections of different biometric features. As an example, the US Department of Homeland Security (DHS) collects face, fingerprint and iris images, from visitors within its US-VISIT program [8].

Facial analytics is a biometric technology that examiners can use to contextualize images of people without encroaching on their privacy. Facial analytics can add powerful capabilities to existing technology used to tackle big data, for example, to better identify child pornographers [9]. Facial recognition software has been used to compare faces in photographs and video against visas, passports, drivers' licenses and other databases [10].

Based on fingerprints, retina scans, and the DNA, a lot of data can be collected. Once the data is used for a common good, a flag that that marks a terrorist as dangerous could be placed in a national database system, which warns users to watch out for their families and other affiliates. The terrorist would then be unable to open a bank account or have a job in government organizations. Big data can certainly play a very important role in predictive analytics and counterterrorism. Immigration records and biometric data are present in different databases. It is necessary to have centers of excellence on big data for terrorism [11].

Extremist and terrorist groups often use the Internet for the dissemination of propaganda and the development of operational plans. Online activity is an important part of almost every national security investigation. The following methods [12] can be used for counter-terrorism:

- Data mining and predictive analytics: the statistical mining or analysis of large datasets or big data.
- Event detection: the statistical detection analysis of social media streams to identify offline events.
- Natural language processing (NLP): the computational analysis (often using machine learning methods) of natural language as it is found on social media.

NLP for countering terrorism is to use algorithmic models as 'classifiers'. The earliest application area of NLP is called sentiment analysis, wherein classifiers make decisions on whether a piece of social media data is positive or negative in tone. NLP can be used to identify some types of risky behavior or criminal intent. Certain structural and underlying features of a sentence and related syntax can be broadly correlated to general behavior types, such as anger, frustration, and subconscious states of mind [12]. Terrorists leave digital traces with much of what they do, whether using e-mail, cell phones or credit cards. This data can be mined to fight terrorism [10]. The Global Terrorism Database is an open source collection of terrorism events across the globe from 1970s to 2013. This unclassified database is a collection of over 125,000 terrorist attacks with detailed records including the country, type of attacks, targets – civilian, military, business, and weapon type, etc. The decision tree classifier and the ensemble classifier were used on the Global Terrorism Database and their performance was analyzed, respectively. The results show that the ensemble method outperforms for the given dataset [13]. The following sections will introduce Big Data applications in Homeland Security.

3. BIG DATA APPLICATIONS IN HOMELAND SECURITY

3.1. Big Data Characteristics, Analytics and Impacts

Business intelligence and analytics (BI&A) and the related field of Big Data analytics have become important in security and public safety. Table 1 summarizes some BI&A features and capabilities in this area, including applications, data characteristics, analytics, and potential impacts [1].

Recognizing the challenges presented by the complexity and volume of defense-related big data, the U.S. Defense Advanced Research Project Agency (DARPA) within Department of Defense (DOD) initiated the XDATA program in 2012. The program is to develop big data analytics and usability solutions for warfighters [1].

Table-1. BI&A and Big Data in Security and Public Safety

Applications	• Crime analysis • Computational criminology • Terrorism informatics • Open-source intelligence • Cyber security
Data	• Criminal records • Crime maps • Criminal networks • News and web contents • Terrorism incident databases • Viruses, cyber-attacks, and botnets *Characteristics*: Personal identity information, incomplete and deceptive content, rich group and network information, multilingual content
Analytics	• Criminal association rule mining and clustering • Criminal network analysis • Spatial-temporal analysis and visualization • Multilingual text analytics • Sentiment and affect analysis • Cyber-attacks analysis and attribution
Impacts	Improved public safety and security

3.2. Big Data in Crime Prediction and Aviation Security

Big Data is capable of handling all data types with extremely large, flexible and scalable storage capability. It has great potential to predict crime, crime hot spots and criminal trends. The New York Police Department, in partnership with Microsoft, launched crime prevention and counter-terrorism technology based on big data mining, and developed a system called the Domain Awareness System [10].

Big Data and analytics hold the keys to shifting the security procedures of Transportation Security Administration (TSA) from a reactive posture to a more holistic approach to security.

Big Data will revolutionize aviation security. More and more people will go through some form of expedited screening process. Future models would leverage the developing world of big data analytics to help TSA know more about travelers before they arrive at the airport [14].

3.3. Big Data and Cloud Computing in Disasters

Big Data delivers the cost-effective prospect to improve decision-making in critical development areas such as health care, crime and security, and natural disaster. One of the biggest sources of uncertainty is nature. Reducing this uncertainty through data analysis can quickly lead to tangible impacts. A recent project by the United Nations University uses climate and weather data to analyze "where the rain falls" in order to improve food security [15].

A large quantity of disaster-related data is available, including response plans, records of previous incidents, simulation data, and the data at Web sites or from social media. However, data management solutions in the past offered few or weak integration capabilities. Cloud computing, big data, and NoSQL have opened the door for new solutions in disaster data management. A Knowledge as a Service (KaaS) framework has been proposed for disaster cloud data management (Disaster-CDM) to facilitate search and support interoperability and integration. Data are stored in a cloud environment using a combination of relational and NoSQL databases [16].

A solution to store disaster related data in a cloud computing environment can provide the following benefits to disaster management [16]:

- High availability: Within the cloud environment, data are automatically replicated, often across large geographic distances.
- Scalability and elasticity: The amount of disaster-related data is immense, and a cloud solution can adapt storage resources based on real time needs and priorities. Data can be automatically redistributed to take advantage of heterogeneous servers.
- No need for a large initial investment: The system can start small and be expanded by adding heterogeneous nodes as needed.

3.4. Big Data in Cybersecurity and Cyber Defense

The information about the terrorists' operations is highly voluminous and is increasingly becoming multidimensional, therefore pushing the analysis of big data into new frontiers. As new terror outfits spring up consistently, applying suitable approaches to such big data has a great impact on counter-terrorism measures and understanding the pattern of attacks [13]. In the information security area, virus characteristics, attack characteristics, and loophole characteristics, etc. may be identified easily through Big Data analytics on big data in the form of log files of an intrusion detection system [17].

Big Data can improve agency cybersecurity through the continuous monitoring of data streams. Agencies are taking numerous steps toward continuous monitoring, but big data analytics has not been widely used to increase cybersecurity [18]. A survey showed this state of

Big Data. Only 26 percent of managers indicated that their agencies used big data to improve their cybersecurity posture. However, several opportunities existed for expansion in this area. Of those who used big data for cybersecurity purposes, three fourths of respondents used it to conduct threat and vulnerability assessments. The survey indicated that Big Data could assist in preventative cybersecurity efforts. The survey result about this is shown Table 2 [18].

Table-2. How Agencies Use Big Data to Improve Cybersecurity

Items	Percentage (%)
Conduct threat and vulnerability assessments	75
Detect intruders	73
Detect anomaly and changes in network usage	60
Investigate incidents	59
Don't know	16
Other	3

Another survey was conducted among 706 IT and IT security (also called cybersecurity) practitioners in December 2012. Survey results are shown in Table 3 and Table 4 [19]. According to Table 3, the greatest areas of cyber security risk are mobile access (either through mobile device such as smartphones and mobile/remote employees), lack of system connectivity/visibility and multiple global interconnected network systems. To make their organizations more secure, the survey respondents would most like big data analytics to be combined with anti-virus/anti-malware, anti-DoS/DDoS, security intelligence systems (SIEM) and content aware firewalls as shown in Table 4. Big Data analytics in security involves the ability to gather massive amount of information to analyze, visualize and draw insights that can make it possible to predict and stop cyber-attacks. Security technologies with Big Data analytics shape stronger cyber defense posture [19].

Table-3. Greatest Areas of Potential Cyber Security Risk within IT (Three choices permitted)

Areas of Potential Cyber Security Risk	Percentage (%)
Mobile access (mobile devices/remote employees)	44
Lack of system connectivity/visibility	42
Multiple global interconnected network systems	40
Cloud computing infrastructure providers	30
Insiders (whether malicious or negligent)	29
Fragmented compliance solutions	26
Network infrastructure environment	2
Virtual computing environments	18
Desktop or laptop computers	16
Removable media (USB devices) and/or media (CDs, DVDs)	15
Across 3rd party applications	9
Within operating systems	7
Server environment & data centers	2
Other	1

Table-4. Enabling Technologies Combined with Big Data Analytics for Better Security (More than one response permitted)

Enabling Technologies	Percentage (%)
Anti-virus/anti-malware	82
Anti-DoS/DDoS (denial of services & distributed denial of services)	80
Security intelligence systems including security intelligence systems (SIEM)	73
Content aware firewalls including next generation firewalls (NGFW)	70
Intrusion detection systems (IDS)	69
Web application firewalls (WAF)	67
Intrusion prevention systems (IPS)	67
Endpoint security systems	60
Identity and authentication systems	54
Mobile device management	51
Secure coding in the development of new applications	41
Data loss prevention systems	29
Secure network gateways including virtual private networks (VPN)	20
Enterprise encryption for data in motion	19
Enterprise encryption for data at rest	17
ID credentialing including biometrics	16
Other crypto technologies including tokenization	4
Other	3

Analyzing logs, network flows, and system events for forensics and intrusion detection has been used in the information security for decades. Conventional technologies aren't always adequate to support large-scale analytics. Performing analytics and complex queries on large, unstructured datasets with incomplete and noisy features was inefficient. Big Data can help clean, prepare, and query data in heterogeneous, incomplete, and noisy formats efficiently. Big data technologies are also suited to become fundamental for advanced persistent threat (APT) detection and forensics [20].

Usable security is a field of study that examines the interrelation between security, usability, and scalability in software systems. It is a combination of multiple domains including information security, user-centered design, and system development. All of these areas work together and provide a framework for usable security [21]. Usable security for Big Data software and systems is an important research topic.

Big data analysis has been used in cyber defense. Big Data analytics helps provide insights for deep packet inspection on the net-flow to identify anomalies or unfamiliar patterns. A lot of the critical infrastructure responsible for basic facilities such as water, energy, food, gas and electricity has become integrated with cyberspace. Securing cyberspace has become an issue of high national priority. Cyberspace has been identified as the fifth domain of warfare [22].

Securing cyberspace has been achieved much through passive cyber defense strategies. Unfortunately, these strategies have proved ineffective in a lot of situations, requiring a strategy shift from passive to active cyber defense [23].

Active cyber defense has synchronized and real-time capabilities to discover, detect, analyze, and mitigate threats and vulnerability. It operates at network speed by using sensors, software, and intelligence to detect and stop malicious activity. As intrusions may not always be stopped at the network boundary, it is necessary to continue to operate and improve upon advanced sensors to detect, discover, map, and mitigate malicious activity on the networks [22].

Approaches to active cyber defense have three categories: detection and forensics, deception, and attack termination. Detection and forensics uses honeypots to attract potential adversaries (detection) and then look for behavior patterns (forensics). Permitting a cyber-adversary to steal false or misleading information involves deception. Attack termination can include actions such as launching Denial of Service (DoS) attacks against attackers [23].

4. BIG DATA CHALLENGES IN SECURITY

Big data has the following security related challenges [17]:

4.1. Big Data Privacy

Big data privacy includes two aspects: (1) protection of personal privacy during data acquisition; (2) personal privacy data leak during storage, transmission, and usage, even if acquired with the permission of users.

4.2. Big Data Safety Mechanism

The performance of previous encryption methods for small and medium-scale data could not meet the requirements of big data due to its high diversity and large scale, so efficient cryptography methods for big data should be developed. Effective schemes for access control, safety communications, and safety management should be studied for structured, semi-structured, and unstructured data.

4.3. Data Quality

Generation, acquisition, and transmission may all influence data quality. Data quality is mainly manifested in accuracy, completeness, consistency and redundancy. Effective methods for automatically detecting data quality and repairing some damaged data need to be studied and developed.

Big data is possibly dirty data, or is the data with potential errors, incompleteness, or inaccuracy. Artificial Intelligence (AI) can be used to identify and clean dirty data or use dirty data as a means of establishing context knowledge for the data. AI can further facilitate additional development in data visualization, which makes intelligent data visualization applications available, possibly for particular types of data. Big data will include more audio- and video-based information. Natural language processing, natural visual interpretation and visual machine

learning will become increasingly important forms of AI for big data. AI-structured versions of audio and video will be integrated along with other forms of data [24].

Security and privacy of big data online applications is a major concern. The scale of data and applications grow exponentially, which brings big challenges for dynamic data monitoring and security protection. Traditional technologies of privacy protection are mainly for static data sets, while big data is often dynamically varied, including data pattern, variation of attribute, and addition of new data. Therefore, it is a challenge to implement effective privacy protection in big data online applications [25].

Homeland Security agencies are increasingly making use of the cloud in order to make use of key characteristics such as on-demand self-service, broad-network access, resource pooling, rapid elasticity, and measured service. However, these advantages also create a single point where adversaries may try to attack the confidentiality, integrity and/or availability of sensitive information stored or being processed [26].

Data security and privacy is a challenge in cloud computing. One critical aspect in cloud competing security is protecting data integrity, availability, and confidentiality. Sharing the cloud resources with protecting customers' privacy is a big challenge. Other security challenges or security issues include monitoring, heterogeneity, virtualization, compliance, service level agreement, security in the web browser, risk analysis and management, access controls and identity management, cross-organizational security management, and extensibility and shared responsibilities [27]. Virtualization is a key element in cloud computing, but it brings its unique vulnerability and has a number of security concerns such as Hypervisor security. Encryption is often used to secure data in untrusted storage environment such as cloud computing. However, it can be a time and cost consumer and could cause additional storage and bandwidth usage. Key management is another complicated problem, which needs more attention [27].

There is growing need to improve the security of big data stored in the cloud. The sensitivity of data being processed in the cloud is increasing; and it is possible to make use of cryptographic advances to secure processing in the cloud to address a growing veracity of big data [26].

5. CONCLUSIONS

Biometrics and RFID have been used in border security, airports, marine security, supply chain management in the military, and disaster tracking and operations. Big Data can work with biometric technologies and RFID to facilitate Homeland Security.

Big Data can analyze the social networks and financial transactions of possible criminals and terrorists; predict crime, crime hot spots, and criminal trends. Big Data will revolutionize aviation security. Big Data and cloud computing deliver the prospect to improve decision-making in disasters.

Cybersecurity is a pillar of national security strategy. Big Data improves cybersecurity through continuously monitoring data streams. Big Data with security technologies help predict

and stop cyber-attacks. Active cyber defense can provide better cyberspace security because of its synchronized and real-time capability to analyze, detect, and mitigate threats and vulnerability.

Big Data has challenges such as data privacy, confidentiality, integrity, and availability of sensitive information. These can be future research topics.

6. ACKNOWLEDGMENT

This study was supported in part by Technology and Healthcare Solutions, Inc. in Mississippi, USA. No conflict of interest to disclose.

REFERENCES

[1] H. C. Chen, R. H. L. Chiang, and V. C. Storey, "Business intelligence and analytics: From big data to big impact," *MIS Quarterly*, vol. 36, pp. 1165-1188, 2012.

[2] K. M. Deitz, "Critical infrastructure protection," *Journal of Healthcare Protection Management*, vol. 28, pp. 101-113, 2012.

[3] M. M. Neag, "Critical infrastructure protection-the foundation of national security 2," *Buletin Stiintific*, vol. 19, pp. 126-132, 2014.

[4] A. Pătrascu and E. Simion, "Critical infrastructures cyber protection using kernel based supervised learning techniques," *MTA Review, Military Technical Academy (MTA) Publishing House*, vol. 24, pp. 59-66, 2014.

[5] B. Thomas, S. Fernandez, and T. Wilbanks, "Perspectives on improving resilience for critical infrastructures," The Global Forum on Urban and Regional Resilience at Virginia Tech: New Perspectives on Resilience, Blacksburg, Virginia, USA, October 12-14, 2014.

[6] G. H. Kim, S. Trimi, and J. H. Chung, "Big-Data applications in the government sector," *Communications of the ACM*, vol. 57, pp. 78-85, 2014.

[7] L. D. Wang, "Enhanced homeland security based on biometrics and RFID," *International Journal of Computer Applications in Technology*, vol. 44, pp. 37-45, 2012.

[8] C. Blundo, E. D. Cristofaro, and P. Gasti, "Espresso: Efficient privacy-preserving evaluation of sample set similarity," *Journal of Computer Security*, vol. 22, pp. 355–381, 2014.

[9] R. Karl and B. Chris, "Facial Analytics: From Big Data to Law Enforcement, IEEE COMPUTER, Sept. 2012, at 95; see also Evgeny Morozov, Requiem for Our Wonderfully Inefficient World, SLATE, Apr. 26, 2013." Available http://www.slate.com/articles/technology/future_tense/2013/04/senor_based_dynamic_pricing_may_be_efficient_but_it_could_create_inequality.html, 2012.

[10] W. Jeberson and L. Sharma, "Survey on big data for counter terrorism," *International Journal of Innovations & Advancement in Computer Science*, vol. 4, pp. 197-205, 2015.

[11] Z. U. H. Usmani, "Predictive modeling to counter terrorist attacks," *Brown Journal of World Affairs*, vol. 20, pp. 277-284, 2014.

[12] J. Bartlett and C. Miller, "The state of the art: A literature review of social media intelligence capabilities for counter-terrorism," Demos, Technical Report, London, UK, 2013.

[13] S. R. Srinivasan and S. R. M. Chandrasekeran, "Big data on terrorist attacks: An analysis using the ensemble classifier approach," presented at the International Conference on Inter Disciplinary Research in Engineering and Technology, New Delhi, India, 2015.

[14] D. Verton, "How data will revolutionize aviation security," *Homeland Security Today Magazine*,vol. 5, pp. 30-33, 2013.

[15] M. Hilbert, "Big data for development: From information- to knowledge societies (January 15, 2013)." Available http://ssrn.com/abstract=2205145 or http://dx.doi.org/10.2139/ssrn.2205145 [Accessed October 30, 2014], 2013.

[16] K. Grolinger, E. Mezghani, M. A. M. Capretz, and E. Exposito, "Knowledge as a service framework for disaster data management," *Electrical and Computer Engineering Publications*, vol. 25, pp. 1-6, 2013.

[17] M. Chen, S. W. Mao, and Y. H. Liu, "Big data: A survey," *Mobile Netw Appl.*, vol. 19, pp. 171–209, 2014.

[18] D. Grinshpan, "Live streaming: Powering continuous monitoring through big data - A candid survey of federal employees," Research Report, Government Business Council, Brocade Networking Solutions, 2013.

[19] Ponemon Institute, "Big data analytics in cyber defense," Research Report, EB-7499 02.13, 2013.

[20] A. A. Cárdenas, P. K. Manadhata, and S. P. Rajan, "Big data analytics for security," *IEEE Security & Privacy*, vol. 11, pp. 74-76, 2013.

[21] T. A. Baklanoff and A. A. Padath, "Usability, security and healthcare systems: Design, challenges and perspectives," *Journal of Information Assurance and Security*, vol. 7, pp. 366-376, 2012.

[22] U.S. Department of Defense, *Strategy for operating in cyberspace*. Washington, DC, USA: Department of Defense, 2011.

[23] A. Flowers and S. Zeadally, "US policy on active cyber defense," *Homeland Security & Emergency Management*, vol. 11, pp. 289–308, 2014.

[24] D. E. O'Leary, "Artificial intelligence and big data," *IEEE Intelligent Systems*, vol. 28, pp. 96-99, 2013.

[25] C. Q. Ji, Y. Li, W. M. Qiu, U. Awada, and K. Q. Li, "Big data processing in cloud computing environments," presented at the 2012 International Symposium on Pervasive Systems, Algorithms and Networks, San Marcos, Texas, USA, December 13-15, 2012.

[26] V. Gadepally, B. Hancock, B. Kaiser, J. Kepner, P. Michaleas, M. Varia, and A. Yerukhimovich, "Computing on masked data to improve the security of big data," presented at the The 2015 IEEE Symposium on Technologies for Homeland Security (HST'15), Greater Boston, Massachusetts, 2015.

[27] Y. A. Younis, M. Merabti, and K. Kifayat, "Secure cloud computing for critical infrastructure: A survey," presented at the The 14th Annual PostGraduate Symposium on The Convergence of

Telecommunications, Networking and Broadcasting (PGNet 2013), Liverpool, UK, July 24-25, 2013.

AUTHORS

Dr. Lidong Wang is an Associate Professor in the Department of Engineering Technology at Mississippi Valley State University, USA. His current research interests include: Big Data, information security, data mining, and biometrics, etc. He was the President of the Electricity, Electronics & Computer Technology (EECT) Division of the Association of Technology, Management, and Applied Engineering in USA. He has published over 60 papers in various journals. He has been the Editor-in-Chief of the International Journal of Automated Identification Technology (IJAIT) for seven years.

Ms. Cheryl Ann Alexander is a graduate of the University of Phoenix where she earned a dual Master's degree in Healthcare Administration and Nursing, and she is currently a doctoral candidate and will graduate soon. She is Chairman of the Board of Technology & Healthcare Solutions, Inc., a nonprofit research and consultant firm located in Mississippi, USA. She is a member of both engineering and healthcare organizations, and is a managing editor of a journal in engineering technology. She has published over 24 papers in professional journals.