17th International Conference on Information Technology- New Generations

ITNG 2020 Proceedings- ONLINE BOOK OF ABSTRACTS

Building the Chain: Securing the Internet of Things in Healthcare

Pebbles Eppes[1], Luay A. Wahsheh[2]

[1]Independent Researcher,

Chesapeake, Virginia, USA

[2]Department of Computer and Information Science,

Arkansas Tech University,

Russellville, Arkansas, USA

[1]*pebbles.eppes@gmail.com*, [2]*lwahsheh@atu.edu*

ABSTRACT

The Internet of Things (IoT) is a phenomenon that has swept through the world and affected every industry in an incredible way. This is especially evident in the impact it has had on healthcare. IoT has heralded an explosive use of technology in the healthcare industry, manifesting in the form of tracking personal data, diagnosing illnesses, treating patients, and more. While incorporating IoT in healthcare has shown marked benefits to the industry, these benefits are counteracted by a critical issue that is affecting the industry as a whole: cyber security. This paper will discuss the story of Michael Elliot, a hacker who discovered vulnerabilities in IoT-capable medical devices and subsequently, the value of medical data. In addition, the paper will examine cyber security issues with IoT and the impact that this has had on the healthcare industry. This paper will then discuss a solution using blockchain technology to securing IoT. Secure IoT technology would increase the amount of personal data available on individuals, allowing healthcare providers to treat patients more efficiently.

Keywords: Blockchain, Cyber Security, Hacking, Internet of Things.

1. INTRODUCTION

It was another day at the office for Michael Elliot. He sat lazily in his man cave as he watched his technological minions work. It had only taken until about early afternoon to utilize his botnet to send out thousands of malicious emails. Elliot was not without money by any means, but it never hurt to begin working on next week's paycheck. It was not long before he began to receive feedback. Elliot smiled; this was good. It was time to get to work. He began to run through the list of compromised systems before one caught his eyes. Apparently, he had successfully gained access to Chippenham Hospital in Richmond, Virginia. It was an interesting find; he had never hacked a hospital before. Cracking his knuckles, Elliot set to exploring. Interestingly enough, it was easier to hack into the network than he had thought. Continuing his exploration, he realized that it was also possible for him to hack into some of the medical devices. It was not long before Elliot realized that the combination of the wireless communication and Internet connectivity needed for the software and network-based transmission of the stored information of medical patients made medical devices more vulnerable to cyber attacks [1]. It made Elliot curious; exactly how difficult was it to hack other systems in the hospital?

The next week, Elliot devoted his time to looking for backdoors into "magnetic resonance imaging scanners, ultrasound equipment, ventilators, electroconvulsive therapy machines" and dozens of other contraptions that had obvious vulnerabilities such as "defenseless operating systems and generic passwords that could not be changed" [1]. It was incredible to Elliot. Hacking the medical devices was, for all intents and purposes, very much like stealing candy from a baby. He discovered that he could hack into an infusion pump and cause the machine to unload an entire vial of medication into a patient, all under the watchful eye of a hospital staff who would not notice a thing [1]. Further exploration of the network showed Elliot that the hospital was at least a decade behind the standard cyber security curve. Elliot could only shake his head in disbelief; how could a hospital, of all things, allow itself to be so easily hackable?

Elliot's curiosity deepened as he accessed a patient's health data. The patient's name was Jonah Pierce. It gave a great deal of information on the patient including his name, personal address and even the social security number. Elliot knew that Pierce's social security number was valuable, but wondered how he could make a profit with the rest of the medical record. Over the next few days, Elliot discovered something amazing; a stolen credit card sold for less than ten dollars on the Web's black market, but the health data he had hacked earned ten times more than that [1]. He stared at the huge amount of funds recently deposited into his bank account and smiled. It looked like he was in business.

2. THE PROBLEM

It was many months later that Elliot realized that he was not the only one who had stumbled across the future of hacking. It was in May of 2017, during some rare down time, that he read about WannaCry's infamous debut. WannaCry was a worldwide ransomware cyberattack that shut down 65 hospitals in the United Kingdom, affecting computers, storage refrigerators and MRI machines [2]. Elliot frowned as he read the news. It seemed that the importance of medical data had finally been discovered by the rest of the world. But WannaCry was not the only attack against hospitals. A few months earlier, in January, Hollywood Presbyterian Hospital in Los Angeles was forced to pay $17,000 to hackers after attackers took control of its computers [2].

Elliot could not help but shake his head as he read the words of cyber security expert, Josh Corman, on the burgeoning phenomenon to attack hospitals. Corman said, "In between the bookends of Hollywood Presbyterian Hospital and the 65 hospitals shut down in the U.K., we went from being prone and prey with no predators to now a little blood in the water. Hospitals and healthcare went to the No. 1 targeted industry last year, in less than one year … so our relative obscurity is over" [2].

As the media focused on the issue, Elliot realized that there were people taking the threat of hackers attacking healthcare organizations seriously, so much so that Dr. Jeff Tully and Dr. Christian Dameff organized an exhibition at the University of Arizona Medical School in Phoenix to allow doctors, security experts and government officials to witness the first-ever simulated hack of a hospital [2]. In their demonstration, Tully and Dameff staged a "massive cyberhack at the medical school's simulation center using three critical mock patients, without the doctors involved in the simulation knowing what was about to happen" [2]. Not only did one mock patient receive a simulated calcium channel overdose from a hacked beside infusion pump, but another's pacemaker was made to malfunction. Yet another mock patient's insulin pump delivered an incorrect dose. Elliot read that it was because of cases such as this that in 2013, Dick Cheney, the former Vice President of the United States, revealed on television that he had the wireless capability on his pacemaker disabled [2].

At first, Elliot was worried about the measures being taken. Someone had finally realized how vulnerable medical data was and was attempting to bring recognition to the lack of security and provide a solution to the problem. Then, he thought about the hospital he had so easily hacked and relaxed. Even if they managed to patch up a few vulnerabilities, it was unlikely that defenders would be able to adequately improve the security of healthcare devices quickly and efficiently enough to keep him out. For the time being, there was nothing to worry about.

3. THE INTERNET OF THINGS

Healthcare as an industry has seen incredible growth in the last few years. This is due to the explosive use of technology in tracking personal data, diagnosing illnesses, and treating patients. This use of technology has increased the amount of data available on individuals, allowing healthcare providers to more accurately and effectively treat patients. This extensive technological movement that is sweeping through the healthcare industry and beyond is called the Internet of Things (IoT). IoT is a "phenomenon that allows seamless interconnection of very small devices over Internet…" [3]. It is the ability of objects, extraordinary and mundane, to connect to the Internet and share data. In healthcare, such items include electronic pacemakers, biomedical sensors, and electronic patient tags [3].

While incorporating IoT in healthcare has shown marked benefits to the industry, these benefits are counteracted by a critical issue that is affecting the industry as a whole and has exacerbated an old and harrowing issue in healthcare: cyber security. The lack of adequate security for IoT in healthcare is particularly important and debilitating as the value of personal health information has become common knowledge among attackers. This is shown in the fact that personal health information has become the prime target of hackers, like Michael Elliot, all over the world [3].

4. SECURING THE INTERNET OF THINGS

4.1 The Internet of Things Architecture

There are few people who would disagree that IoT poses a problem to security, safety, and privacy, even a hacker such as Michael Elliot. Though the usefulness of IoT is well-known, so are its security failures. To make the issue even more complex, IoT systems often “have unique characteristics that are not found in traditional IT systems” [4]. This makes security training for IoT a very specific process. While such training is available, it does not address the overarching lack of security in IoT devices. Security issues within the IoT-based healthcare system include security for patient confidentiality; security that enables electronic health records include authentication, data, and integrity; transmission security, and security in healthcare data access, processing, and storage [5].

Due to its inherent architectural structure, mainly the fact that IoT devices and networks have limited resources, there are major constraints to applying conventional security solutions to IoT-based systems. Some of these constraints include, but are not limited to, the fact that IoT devices are usually memory constrained, which means that conventional schemes do not work for them; IoT devices usually use low data-rate radio interfaces to communicate, which means traditional security measures cannot be applied to them because of the low bandwidth; and the fact that an “IoT milieu compromises different types of devices ranging from PCs to RFID tags and a wide range of wireless protocols such as WiFi, Zigbee and Z-Wave” [6]. It is difficult to find a solution that accommodates the sheer diversity of IoT devices with the security solutions available today.

4.2 Building the Chain

A solution has been proposed in the form of blockchain technology. Created due to a need for an efficient, cost-effective, reliable and secure system for recording and conducting transactions, blockchain “is a list of transactions, grouped into blocks and shared with members within a network” [5] and uses, “public-key cryptography to sign transactions among parties” [6]. In blockchains, data is stored on a shared, distributed ledger in which identical copies of the data is shared on multiple computers or on nodes in a network [7]. Through peer-to-peer sharing and replication, blockchain technology allows participants to share a ledger that updates with every transaction. Through a process called consensus, this peer-to-peer process ensures that changes to the data by any member in the network has the approval of every other member in the group. Every change, event or transaction is time-stamped and unchangeable after this process, making blockchain trustworthy and reliable.

From a security standpoint, “the main drawback of IoT applications and platforms is their reliance on a centralized cloud. A decentralized, blockchain-based approach would overcome many of the problems associated with the centralized cloud approach” [6]. Typically, the IoT architecture is such that IoT devices are identified, authenticated and connected through cloud servers. This centralized cloud model is susceptible to manipulation. The lack of a centralized entity will allow devices to communicate securely and exchange value with each other by executing actions automatically through smart contracts [6]. In addition, decentralized access and immutability means that malicious actions can be detected and prevented. Also, because devices are interlocked in the blockchain architecture, if a device’s updates are breached by hackers like Michael Elliot, then the system automatically rejects it.

In the healthcare industry, blockchain technology can be applied “in the context of research, clinical trials, and [population health management] PHM” [7]. If implemented properly, blockchain could fundamentally change how healthcare data is created, stored, shared and protected. Blockchain technology can further aid in data security for patient medical records by disseminating the storage of “data among patients and their healthcare providers in distributed ledgers” significantly reducing the risk of data breaches [7].

5. CONCLUSIONS

In conclusion, hackers like Michael Elliot have identified the value of medical data and now seeks after it rigorously. The benefits of securing IoT in healthcare are critical and include protecting patients, decreasing the likelihood of the theft of health information and increasing the efficiency of healthcare providers. The lack of security in IoT is a dark cloud that overshadows the incredible gains the healthcare industry has elicited by using IoT devices. Though the inherent architecture of the Internet of Things makes it insecure, blockchain technology is a solution that can help ensure that information is secure in the healthcare industry.

Securing IoT in healthcare will change the industry for the better. It will protect patients from having their personal information sold without their consent or knowledge to third parties who would use it for ill and will reduce the chances of identity threat due to the hacking of critical medical data. It will also allow healthcare providers to do their jobs without fear that they will be penalized for technological lapses and data breaches, including the legal and social consequences that follow. With the securing of IoT in healthcare, doctors can move forward with using IoT devices and can gain all the benefits that it affords such as improved outcomes of treatment.

REFERENCES

[1] L. Ayala, *Cybersecurity for Hospitals and Healthcare Facilities: A Guide to Detection and Prevention*, Apress, 2016.

[2] D. Harris, J. Kapetaneas, R. Zepeda, and L. Effron, June 2017, Fears of Hackers Targeting US Hospitals, Medical Devices for Cyber Attacks [Online]. Available: https://abcnews.go.com/Health/fears-hackers-targeting-us-hospitals-medical-devices-cyber/story?id=48348384.

[3] M. U. Ahmed, S. Begum, and W. Raad, Internet of Things Technologies for HealthCare, *Proceedings of the 3rd International Conference HealthyIoT*, October 2016.

[4] B. Russell and D. Van Duren, *Practical Internet of Things Security*, Packt Publishing Limited, 2016.

[5] S. Li and L. D. Xu, *Securing the Internet of Things*, 1st Ed., Syngress, 2017.

[6] N. Kshetri, Can Blockchain Strengthen the Internet of Things?, *IEEE IT Professional*, vol. 19, no. 4, pp. 68-72, 2017.

[7] P. Padmanabhan, *The Big Unlock: Harnessing Data and Growing Digital Health Businesses in a Value-Based Care Era*, Archway Publishing, 2017.

Internet of Things (IoT) Security threats and its Challenge on Cloud Computing: "Case Study on: Mitigating Cyber-threats Against Drones and its Susceptible Interconnected Devices."

Anteneh Girma
anteneh.girma@udc.edu
Department of Computer Science and Information Technology
Univ. of the District of Columbia

Alpha Diallo
alphaamadou.diallo@udc.edu
Department of Computer Science and Information Technology
Univ. of the District of Columbia

Abstract

The adoption of Cloud Computing has extensively changed the way organizations run their businesses. It eases the way and helped connect the world into one expansive marketplace. Moreover, Internet of Things (IoT) has practically taken many industries around the world that made connectivity options by internet, share information using cloud services that is rising significantly. The interconnected devices in cloud provides the required connectivity to share information between them. Although cloud computing has an immense benefit in terms of flexibility, economic savings, and support of new services, its enabled computational resources and services to be used and those different interconnected devises are exposed to serious cyber threats. These threats are getting more sophisticated and complex in nature. This paper will discuss the potential impacts of the existing IOT security threats and its challenges on cloud computing by reviewing and researching current survey on IoT Cloud services, and finally proposes a recommendation to mitigate cyber threats against drones and its susceptible interconnected devices.

Key words | IoT | IoT Security | Cloud Computing | Drones Security | Cloud Security

1. INTRODUCTION:

With the promise of rising efficiency and connectivity, the adoption of Internet of Things (IoT) is rapidly and inevitably spreading in our society. Although the number of "things" has strongly been increasing over the past few years, statistics predict an even further growth in the future with over 20.4 billion IoT connected devices in 2020 according to the IT research and advisory firm Gartner [1]. Indeed, this growth will bring opportunities together with challenges, and the massive introduction of this technology will need to be managed by several points of views such as legal, social, business-wise and of course technological [2].

The IoT (Network of connected physical devices) applications offer new and innovative ways to organizations, to manage and monitor remote operations from industrial automation to home area networks to smart buildings, pervasive healthcare and smart transportation [2]. It allows having eyes and ears in remote places, constantly feeding applications and data stores with information. The low cost of "things" allows observing and managing activities that were previously out of reach. With the Internet of things, it is also possible to collect information about events that were once invisible, such as correlating weather patterns with industrial production. For instance, Leveraging the ongoing IoT revolution, drones have experienced accelerated transformation in their use from being hobbyist toys to complex IoT devices. Furthermore, the rollout of 5G technology is expected to enhance the ability of drones to react to commands in real time enabling instant feedback. This is expected to increase their capabilities and performance. Drones increase efficiency and productivity while reducing workload and costs. This factor makes them an invaluable addition to various sectors[4].

Intelligent drones are also expected to change how deliveries are made. Where other modes of transport are not viable, drones will come in handy. This will reduce challenges associated with delivering relief and medical supplies in disasters and emergency situations. A pilot project has already taken off in Rwanda with medical supplies supplied to remote hospitals using drones. Drones are also expected to change responses to emergencies. Apart from performing visual searches and sending feedback, drones will also be able to work together and build temporary shelters for the survivors. This will be enabled by advancements in technologies such as 3D printing using additive building manufacturing technology. In addition, drones are also going to be used to help firefighters determine exact locations of a fire as well as locating injured people. Police will use the intelligent drones to spot violent behavior and release tear gas or pepper spray to disperse crowds [3].

2. Literature review

Nowadays, Cloud computing is a well-known paradigm. However, for the sake of readability and self-containment of this research paper, we consider relevant basic notions of Cloud computing. According to NIST [6] Cloud computing is defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". It provides a high-level overview of the Cloud and identifies the main actors and their role in Cloud computing. Each actor is an entity, i.e., a person or an organization, that either takes part in a transaction/process or performs some tasks in Cloud computing. In terms of interactions, there are several possible scenarios [7]. Generally, a Cloud consumer may request a Cloud service from a Cloud provider, either directly or via a Cloud broker. A Cloud auditor conducts independent audits and may contact other actors to collect the necessary information.

The recent paradigm shift in the IT sector leading to cloud computing however innovative had brought along numerous data security concerns. These threats mainly originate from its own main characteristics issues such as multi-tenancy, loss of control over data and trust [12]. However, with the continuous growth of cloud computing and related services, security and privacy has become a critical issue [10]. One major such security laps is that referred to as the Man in the Middle (MITM) attack where external data are injected to either hijack a data in transit or to manipulate the files and object by posing as a floating cloud base. [8]. Moreover, the paradigm of multimedia distribution has been shifted from the models in traditional ways to the one in cloud computing. Security and privacy are two most important issues in multimedia distribution [9]. cloud security is multipath. Through transient applications and services, lively up around multiple data centers, with dozens or hundreds of free micro services, each with their own access mechanisms, with the widespread acceptance of virtualization and the recent extensive rage over containerization, care on top of cloud specific security vulnerabilities are a huge effort in itself [11]. Distributed protocols for cloud storage correctness assurance will be of most importance in achieving a robust and secure cloud data storage system in the real world [13].

3. Drone Security Issues:

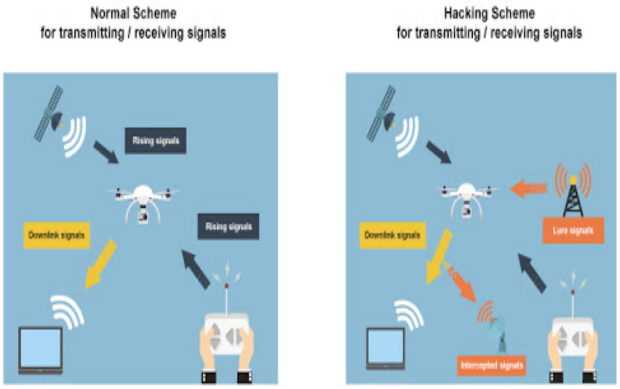
Smart devices collect information about us, our homes and our lifestyles. To mitigate the threat, organizations need to consider training physical security staff to spot drones, installing jamming signals and treating their airspace as an extension of the corporate attack surface. Constant change of their passwords is necessary, as one of the primary security breaches is password theft. Updating and upgrading software, firewalls, applications within the organization running their businesses using drones and data. For small office/home office wireless networks, operators may consider mitigations commonly used to address war-driving attacks, such as turning off the wireless network when not in use, updating administrator passwords on routers regularly, and using security measures such as wireless traffic encryption and firewalls.

Drones facilitate a range of possibilities, from delivery and fulfillment to logistics, security, law enforcement and action by first responders. However, among the security concerns that need to be addressed include: How can citizens ensure their information is secure from possible cyber-attacks? With all our technological advancements, have we exposed ourselves to increased cyber-attacks? How do we balance innovations with cybersecurity and privacy risk exposures? How these devices can be properly protected? How are they susceptible to hacks? What can we do to combat the security risks and challenges drones create? Will these measures enable fool proof prevention of hacking drones? What should be the role of government in drone regulation when it comes to protecting the privacy and safety of citizens? How can we improve the security of connected devices and instill high confidence in their security?

4. Primary Drone’s Cyber Threats

There are two primary cyber threats to drones: hijacking and supply chains (fig 1).

Figure 1



4.1 Hijacking

Commercial drones can be hijacked relatively easily. In 2016 Samy Kankar develop a program called Skyjack in order to reprogram the software on a drone using standard radio frequencies to gain access and take control of the drone [14]. Using this device, he could scan for nearby drones with vulnerable MAC addresses, it could hijack them and gather up a swarm of drones controlled by a single hacker with an inexpensive Raspberry Pi controller. In 2017, Jonathan Andersson a security expert made a device (called it Icarus) in which he could tune into the drone's communication frequency. Even though the communication channel hopped every 11 milliseconds, Icarus waited on one channel, and in the available 11 milliseconds hacked the drone's encryption and hijacked the device [14].

4.2 Supply chain

Because most commercial drones are largely manufactured abroad, the supply chain is another threat that could affect its assembled components manufactured abroad. With contemporary geo-political tensions, there is always a concern that such devices might contain a hidden backdoor for overseas governments. Another concern is that today's commercial drones almost come with a video camera. Hackers could obtain recorded data by hijacking the device and stealing the data. But many drones automatically upload recorded data in real-time for storage in the cloud. This raises concerns for even innocently obtained images, if a drone pilot accidentally records something sensitive, that data is immediately online and vulnerable to theft if the storage service is improperly secured. The U.S. government is so concerned over the storage of drone data that earlier this year and the US Department of Homeland Security issued an alert that Chinese-made drones may be a “potential risk to an organization’s information,” and could be sending flight data back to their manufacturers [5].

5. Existing Proposed Approach and their Vulnerability

The Internet of Things (IoT) and the Smart City generate and collect unprecedented datasets on people [15]. As a wireless IoT devices, drones are susceptible to all the cyber threats that face the Internet of Things and can be hijacked for unintended purposes [4]. Cyber-criminals may also look to take advantage by performing man-in-the-middle attacks against employees, carry out network reconnaissance and IoT devices such as smart light bulbs, or even wireless mice. Hacked drones are breaching physical and cyberdefenses to cause disruption and steal data. Those bad purposes include threats to our privacy, to cybersecurity, and even to our physical safety.

Other proposal recommends applying methods that include radar, infrared (IR) sensors, and acoustic sensors:

- One way is by spoofing or simulating the GPS signal the drone uses to navigate using a GPS jammer to cause vulnerable drones to land, fly off course, return home, or crash by preventing the drone from receiving GPS signals (Fig 2 below).

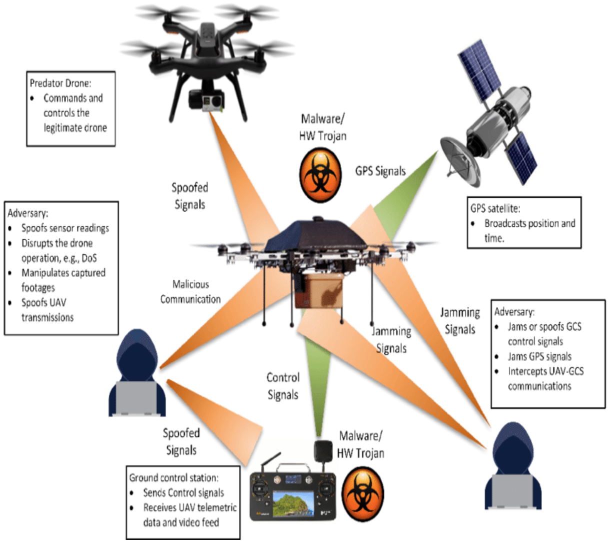
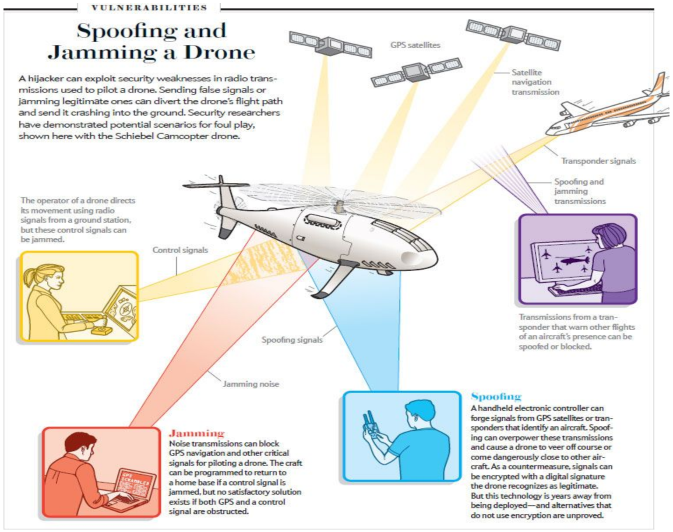


Figure 2

- Downlink threats are another category (Figure 3) that includes intercepting video, images, or data broadcast from the drone to the base station. Video footage taken by drones (especially consumer models) is often transmitted via an unencrypted radio format that could theoretically be intercepted, stored, and transferred by anyone within range.

Figure 3



Spoofing and Jamming a Drone

A hijacker can exploit security weaknesses in radio transmissions used to pilot a drone. Sending false signals or jamming legitimate ones can divert the drone's flight path and send it crashing into the ground. Security researchers have demonstrated potential scenarios for foul play, shown here with the Schiebel Camcopter drone.

The operator of a drone directs its movement using radio signals from a ground station, but these control signals can be jammed.

Transmissions from a transponder that warn other flights of an aircraft's presence can be spoofed or blocked.

Jamming

Noise transmissions can block GPS navigation and other critical signals for piloting a drone. The craft can be programmed to return to a home base if a control signal is jammed, but no satisfactory solution exists if both GPS and a control signal are obstructed.

Spoofing

A handheld electronic controller can forge signals from GPS satellites or transponders that identify an aircraft. Spoofing can overpower these transmissions and cause a drone to veer off course or come dangerously close to other aircraft. As a countermeasure, signals can be encrypted with a digital signature the drone recognizes as legitimate. But this technology is years away from being deployed—and alternatives that do not use encryption are unproved.

6. Conclusion:

In conclusion we can say that even though the utilization of IoT devices is growing at a fast rate as well as drones use, we are still in the early days of drone development. Over the next few years coming their capabilities will expand even more. As a society and law enforcement we need to be aware of the threats this could deliver. Devices developed for good reasons can be misappropriated for bad purposes. We are planning to extend our research to take our proposal to the next step where we limit our scope, set our requirements, test our approach and discuss the results.

7. References

1. Drones as the New "Flying IoT": They'll Track People and Deliver Goods Using a New Low-Power Architecture to Juice the Apps While Staying Aloft: IEEE Computer Society. (n.d.). Retrieved from https://www.computer.org/publications/tech-news/research/flying-iot-toward-low-power-vision-sky.

2. Innovative ways to use IoT-enabled drones in the near future. (2019, August 2). Retrieved from https://www.iot-now.com/2019/08/02/97962-innovative-ways-use-iot-enabled-drones-near-future/

3. Martin, A. (2019, July 27). IoT in action. Retrieved from https://towardsdatascience.com/iot-in-action-a8b7fac83619.

4. Statista Research Department. (2019, November 14). IoT: number of connected devices worldwide 2012-2025. Retrieved from https://www.statista.com/statistics/471264/iot-number-of-connected-devicesworldwide/.

5. What Security Threats Are Posed By Drones? (n.d.). Retrieved from: https://blog.avast.com/what-security-threats-are-posed-by-drones.

6. Mell, P.; Grance, T. The NIST Definition of Cloud Computing; Technical Report, 2011. Available online: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (accessed on 4 June 2019)

7. Liu, F.; Tong, J.; Mao, J.; Bohn, R.; Messina, J.; Badger, L.; Leaf, D. NIST Cloud Computing Reference Architecture; Technical Report 2011; NIST: Gaithersburg, MD, USA, 2011.

8. Olanrewaju, R.F., Islam, T., Khalifa, O.O., & Fajingbesi, F.E. (2018). Data in Transit Validation for Cloud Computing Using Cloud-Based Algorithm Detection of Injected Objects.

9. Xiong, L., Xia, Z., Chen, X. et al. Multimed Tools Appl (2019) 78: 30297. https://doi.org/10.1007/s11042-018-6981-6

10. Chen, L. (2019). Security, privacy, and digital forensics in the cloud. Singapore: Wiley Blackwell.

11. G, E., & S, D. V. (2015). A Review on Security Threats and Vulnerabilities in Cloud Computing. International Journal of Engineering Research And, V4(07). doi: 10.17577/ijertv4is070073

12. Yao, M., Zhou, D., Deng, R., & Liu, M. (2018, June 8). A Security Protocol for Access to Sensitive Data in Trusted Cloud Server. Retrieved from https://link.springer.com/chapter/10.1007/978-3-030-00009-7_48.

13. A Trusted Framework for Data Security in Cloud Environment. (2015). International Journal of Science and Research (IJSR), 4(11), 1728–1730. Doi: 10.21275/v4i11.sub159028

14. Abazari, F., Takabi, H., & Analoui, M. (2019). Hacking and Countermeasures in the Cloud. Security, Privacy, and Digital Forensics in the Cloud, 129–141. doi: 10.1002/9781119053385.ch6

15. Losavio, M. M., Chow, K. P., Koltay, A., & James, J. (2018). The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security. Security and Privacy, 1(3). doi: 10.1002/spy2.23

Quantum Cryptography in the Future of Cybersecurity

Ping Wang, Robert Morris University
Hubert D’Cruze, University of Maryland

ABSTRACT

Cryptography has been an essential safeguard component in protecting and securing data and networks, including Internet of Things (IoT) devices and networks. Quantum computing brings substantial benefits and challenges to the developments of system architectures and cryptosystems. This proposed research explores the security benefits and challenges of quantum computing and quantum cryptography. This research explores the role of quantum computing and quantum cryptography in the field of cybersecurity with a particular focus on IoT security and privacy. The goal of the proposed study is to evaluate quantum and post-quantum cryptographic solutions and propose a post-quantum security model for future IoT devices and networks.

KEYWORDS: Encryption, cryptography, quantum computing, quantum cryptography, post-quantum cryptography, post-quantum security, quantum key distribution (QKD), cybersecurity, Internet of Things (IoT)

RESEARCH DESCRIPTION

Cryptography is the art of encoding and encrypting information to hide it or keep it secret from unauthorized recipients. Information concealment has been present in many cultures and can be dated back to ancient times. Cryptography has been an essential control in protecting data confidentiality and integrity, and encryption solutions and algorithms have undergone generations of evolution and improvement to address vulnerabilities exposed by cryptanalysis. There has been productive research on quantum-resistant public-key cryptography or postquantum cryptography (PQC) with promising application opportunities (Chen, 2017). Quantum cryptography, which is based on quantum computing derived from the laws of quantum physics, presents a robust security alternative to data encryption as Quantum Key Distribution (QKD) is capable of detecting intrusions and eavesdropping attempts and aborting and restarting data transmission for secure and unbreakable data communication (Buenano et al., 2019; Takeoka, Fujiwara, & Sasaki, 2019). The world’s largest Quantum Key Distribution (QKD) network so far with 32 trusted nodes has been operational in China since 2017 (Takeoka, Fujiwara, & Sasaki, 2019).

With fast growth and adoption of the Internet of Things (IoT) in services, infrastructure and consumer industries, IoT devices and networks and the IoT-dependent society are facing increased security challenges and vulnerabilities including communication attacks that demand comprehensive technical controls and security policies (Rizvi et al., 2018). With mobility and complexity in IoT deployment, existing security and encryption technologies for traditional networks may not be suitable for all scenarios and need to be carefully reviewed (Wei, Liao, Li,

& Gong, 2017). Effective encryption technology and techniques with fine-grained access controls may be used to implement and reinforce IoT security policies (Oualha, 2018). Recent research has also found that quantum cryptography can be integrated with modern security technologies on data storage network based on QKD and secret sharing and allowing secure authentication, transmission, storage and backup for disaster recoveries (Takeoka, Fujiwara, & Sasaki, 2019). This is very valuable development in quantum cryptography that will potentially benefit the security and privacy of IoT networks and devices. Therefore, the proposed research is of significant value to the IoT security research community and the benefit of the society in general. The goal of this proposed research is to propose a security model for IoT networks with integration of quantum cryptography.

RESEARCH PLAN

The proposed research is to develop and propose a theoretical model for securing future IoT networks with integration of postquantum cryptography. To begin with, the research study needs to review and evaluate the existing research on the topic of quantum cryptography and cybersecurity in order to identify the strengths and limitations of quantum cryptography. The research literature review will cover the three categories identified by Wallden and Kashefi (2019): the post-quantum category, the quantumly enhanced category, and the quantumly enabled category. The post-quantum category deals with required changes such as hard problems used, security definitions and proof techniques; the quantumly enhanced category focuses on various enhancements in protocols including information theoretic security, increased efficiency, and functionalities such as quantum key distribution; the quantumly enabled category focuses on different communication infrastructures available such as protocols for quantum encryption and quantum authentication (Wallden & Kashefi, 2019).

The proposed model from this study will address the various security threats and risks at different levels of IoT security domains and sub-domains identified by Rizvi et al. (2018). The proposed model will incorporate the strengths of quantum cryptography as a key part of the solutions, which include its unconditional security, unique sniffing detection, and the security of QKD (Zhou et al., 2018). In addition, research has found that IoT devices and networks are vulnerable to the threats of quantum-computer-assisted cryptanalysis (Suolmalainen, Kotelba, Kreku, & Lehtonen, 2018). The proposed model from this study will address quantum immunity for IoT, illustrate the relationships among various components and explain how the quantum cryptography constructs help to resolve the IoT security challenges.

REFERENCES

Buenano, H., Guachimbosa, V.H., Ruiz, J., Mera, J.S., & Guerrero, J.S. (2019). A reliable security alternative: Quantum cryptography. *2019 Sixth International Conference on eDemocracy & eGovernment (ICEDEG)*. 357-361.

Chen, L. (2017). Cryptography standards in quantum time: New wine in an old wineskin? *IEEE Security & Privacy,* July/August 2017. 51-57.

Oualha, N. (2018). Reinforcing IoT-enabled security policies. *17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering.* IEEE Computer Society. 831-836.

Rizvi, S., Pfeffer III, J., Kurtz, A., & Rizvi, M. (2018). Securing the Internet of Things (IoT): A security taxonomy for IoT. *17th IEEE International Conference on Trust, Security and Privacy in Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering*. IEEE Computer Society. 163-168.

Suolmalainen, J., Kotelba, A., Kreku, J., & Lehtonen, S. (2018). Evaluating the efficiency of physical and cryptographic security solutions for quantum immune IoT. *Cryptography,* 2018-2 (5), 1-20.

Takeoka, M., Fujiwara, M., & Sasaki, M. (2019). R&D trends and future prospects of quantum cryptography. *New Breeze,* Winter 2019. 4-8.

Wallden, P., & Kashefi, E. (2019). Cyber security in the quantum era. *Communications of the ACM, 62*(4), 120-129.

Wei, B., Liao, G., Li, W., & Gong, Z. (2017). A practical one-time file encryption protocol for IoT devices. (2017). *2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC).* IEEE Computer Society. 114-119.

Zhou, T., Shen, J., Li, X., Wang, C., & Shen, J. (2018). Quantum cryptography for the future Internet and the security analysis. *Security and Communication Networks.* 1-7.

The analysis of how the cost of a Cyber-security Data breach could be Quantified.

Richmond Ikechukwu Ibe Ph.D.

[1]Department of Computer Science, The University of Cumberlands

Williamsburg, KY, U.S.A,

richmond.ibe@ucumberlands.edu, richyryke2010@gmail.com

ABSTRACT

Organizations depend on Information Technology for efficiency and productivity increase. Besides, technology has changed the way most organizations conduct their businesses. However, cybercrimes have called for security consciousness to protect organizational data. The trend of cybercrime has become an ongoing event, cyber breaches are on the news every day, and organizations have lost millions of Dollars and often failed to quantify the cost of data breaches. The problem researched is that many organizations lacked the skills to quantify the cost of a data breach after cybersecurity attacks. The dispiriting factor appears to be that, quantifying the cost of a data breach after cyber-attack appears to be difficult. This event does not only affect corporates, but millions of customer records, payment card data, and loss of trade secrets are also affected. The cyber threats are exacerbating in sophistication and reprehensible way. The purpose of this research is to see if there could be a harmonious method of quantifying the cost of a data breach. The significance of this research is that the study could possibly help to discover new ways an organization can use to quantify the cost of a data breach. As we know that many organizations appear not to have an approach to calculate or quantify the cost of a data breach after a cyber-security attack. Even if they do, it appears to be guesswork. Besides, this research study could go a long way to help in determining the cost of a data breach. Having an in-depth understanding of the cost will help an organization to classify their asset based on the asset value, as well as protecting the critical asset. The theoretical framework for this research is grounded on the cost-based approach. The research method that will be used will be a mixed method. The data collection technique will be based on primary and secondary data collection. The primary data collection will be elicited by using a questionnaire, and the secondary data collection will be done through the internet sources or through a facilitator in organizations that accept to share their information based on the status quo.

INTRODUCTION

Organizations depend on Information Technology for efficiency and productivity increase. Besides, technology has changed the way most organizations conduct their businesses. However, cybercrimes have called for security consciousness to protect organizational data. The trend of cybercrime has become an ongoing event, cyber breaches are on the news every day, and organizations have lost millions of Dollars and often failed to quantify the cost of data breaches. Varilis, Petkovic & Zannone (2012), asserted that "In the recent years the number of data breaches reported by public and private organizations have increased sharply. For instance, a study from Ponemon Institute in 2012 showed that 94% of US hospitals for example suffered serious data breaches."

(para2). According to the data, “The primary cause is that IT systems often implement inadequate measures that allow users to have access to sensitive data, which they are not authorized to access.” (para 2).

This event does not only affect corporates, but millions of customer’s records, payment card data, and loss of trade secrets are also affected. The cyber threats are exacerbating in sophistication and reprehensible way. The need to provide training on cyber security management is not only to focus on thwarting hackers that intend to disrupt your business or deface your website; but investigate into quantifying the status-quo. Conceivably, we must be prepared to address the threats from professional cyber-espionage or foreign government intrusion into an organizational IT infrastructure. In this regard, we must use a bottom-top approach to develop a method that could help to quantify the cost of a data breach.

Problem Statement

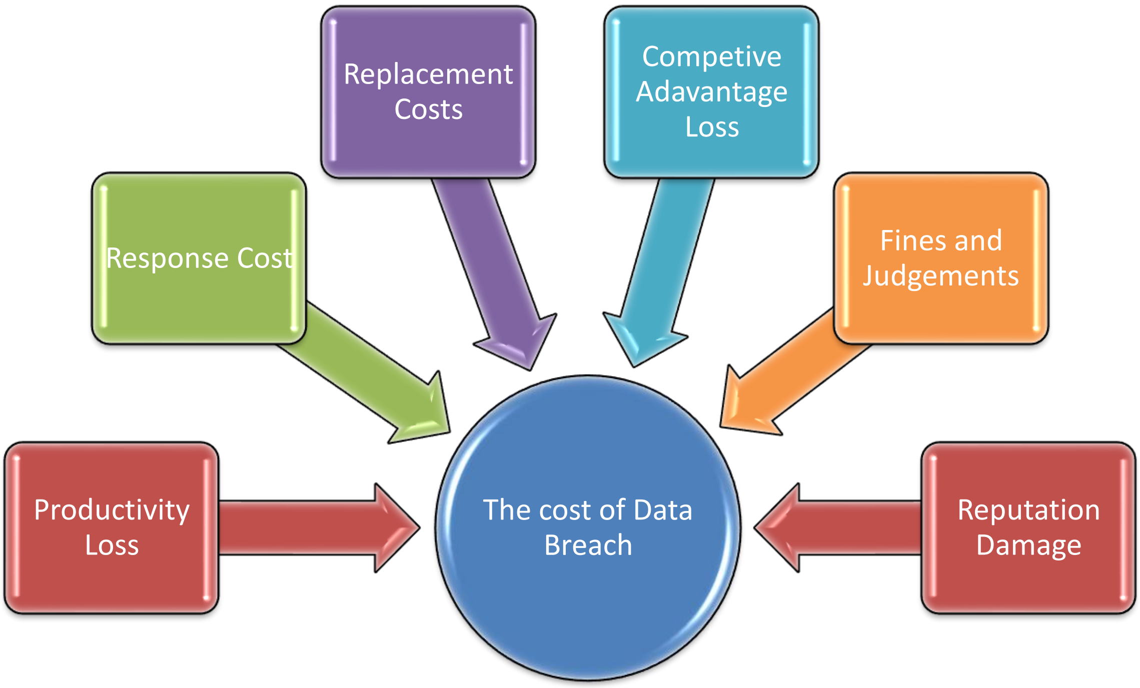
Organizations face serious challenges as businesses are conducted via the web. Many kinds of attacks occur and defending these attacks are becoming more challenging in our organizations today. The dispiriting factor appears to be that, quantifying the cost of a data breach after cyber-attack appears to be difficult. Some of the research article that tend to quantify the cost of a data breach appears to be guessing. According to Acohido (2017). “For some time, “Ponemon” a consulting firm has used a cost-per-record measure to help companies and insurers get an idea of how much a breach could cost them. Its estimates are widely used.” However, there seem to be a dispute amongst organizations for applying this model.

After an attack, organizations tend to perform the risk analysis such as: Valuations of the critical assets in hard costs, A detailed listing of significant threats, Each threat's likelihood and possible occurrence rate. In addition, Loss potential by a threat, and the dollar impact that the threat will have on an asset. All of these were in an effort to determine the cause of loss and the amount that was lost from an attack.

Theoretical Framework

This research will be grounded on the cost-based theoretical model. The reason of using this approach is that data breach cost money, therefore, it will help to gain an accurate understanding of the problem. Besides, this approach will help in determining the value of the asset both tangible and intangibles, which could possibly be difficult to quantify using other approaches. More also, the cost analysis will break down the cost summary into constituents and determine the driving factors. Then, the researcher can explore the report based on each factor for easy quantification. However, the cost-based approach will only explore the economic impact Analysis of the cyber-security data breach.

Conceptual Framework



The above diagram Fig1 is a conceptual framework based on the cost model theory. The framework is looking into Six different areas that is associated with the cost of a data breach. These areas include both the tangible and intangible cost.

Methodology

The proposed research method will used Mix-method approach. This is because the qualitative arm of the method will help to elicit the data collection process while the quantitative arm will be used for data-validation. Besides, using mixed method will ensure cross-validate of data and which will increase the precision of the result.

Data collection Technique

The data will be collected using Questionnaire on the qualitative arm of the research. Then, on the quantitative arm, I will use the secondary data collection technique such as the internet sources and asking organizations for help.

Literature Review

According to HIPAA (2019), "Over the past five years, the average cost of a data breach has increased by 12%. Further, the global average cost of a data breach has increased to $3.92 million. The average breach size is 25,575 records and the cost per breached record is now $150; up from $148 from 2018." (para 2). The article asserted that the healthcare industry data breach impact was felt globally. This means that the healthcare industry has the highest breach costs with an average mitigation cost of $6.45 million. (para3).

The literature also reviewed that Healthcare data breaches typically cost 65% more than data breaches experienced in other industry sectors. This article asserted that Data breach costs are the highest in the United States, where the average cost of a data breach is $8.19 million – or $242 per record. The average cost of a healthcare data breach in the United States is $15 million. (HIPAA, 2019).

Critical Analysis

According to Acohido, (2015), the cost of a data breach rose from $3.5 million in 2014 to $3.8 million in 2015 with an average cost per loss recorded as from $145 to $154 per record. However, IBM sponsored research showed that cost of a data breach jumped from $105 to $165 in 2019. The report also, showed that the cost was high in the health care industry at $363 per compromised record than in the retail sector.

However, Verizon organization perceived that quantifying the cost of a data breach by pure cost per record should be avoided. In fact, I concur with Verizon's objections because pure cost may not have accounted for the intangibles. Such as, notification for the breach, legal investigations, administrative cost, customer satisfaction, opportunity loss, organization's reputation, information hotlines and credit monitoring and so on. These were the thing that should be quantified for the ongoing research.

References

Acohido, **B. (2015).** How to Measure Data Breach Costs? A dispute between Ponemon Institute and Verizon over how to estimate the value of a breach may complicate the calculation. [Blog]. Retrieved from https://www.insurancethoughtleadership.com/how-to-measure- data-breach-costs/

HIPAA Journal, (2019). 2019 Cost of A Data Breach Study Reveals Increase in U.S. Healthcare Data Breach Costs. Retrieved from https://www.hipaajournal.com/2019-cost-of-a-data-breach-study-healthcare-data-breach-costs/

Ponemon Institute, (2016). 20161 Cost of Data Breach Study: Global Analysis. Retrieved from http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094

Varilis, S. Petkovic, M., & Zannone, N. (2012). Data Leakage Quantification. Retrieved from http://security1.win.tue.nl/THeCS/pubs/data_leakage_quantification.pdf

The artificial neural network approach for process faults identification of an MSPC-MEPC process

Yuehjen E. Shao

Department of Statistics and Information Science, Fu Jen Catholic University
New Taipei City, Taiwan, R.O.C.

stat1003@mail.fju.edu.tw

ABSTRACT

A product or a process with high quality is one of the most important core values for business companies. The integration of automated and monitoring technologies is an effective way to achieve the core value. Process faults (PFs), such as shift or trend faults, would commonly have been occurred in manufacturing processes, and those faults upset the process and result in poor quality for the processes and products. If those PFs can be identified and removed in a real-time manner, the process improvement could be greatly attained. In recent years, because advanced technology has changed the way of traditional process control, the integrated use of multivariate statistical process control (MSPC) and multivariate engineering process control (MEPC) has been applied to multivariate processes. In addition, the benefits of MSPC-MEPC has been reported. Because the multivariate process contains two or more quality characteristics, it is difficult to identify which one or which set of quality characteristics are at faults when an out-of-control signal is triggered by MSPC. Although the issue of identification of PFs has been broadly investigated, there has been little research focused on the identification of the PFs for an MSPC-MEPC process. In this study, because the artificial neural network (ANN) classifier performs well in the classification tasks, we propose an ANN approach to identify the source of the PFs for an MSPC-MEPC process. Furthermore, a series of computer experiments are performed to evaluate the effectiveness of the proposed ANN approach.

Key words: artificial neural networks; process faults; multivariate statistical process control; multivariate engineering process control

1. INTRODUCTION

The multivariate statistical process control (MSPC) charts have been widely reported that their effectiveness for monitoring a multivariate process. However, because a multivariate process possesses two or more quality variables, it is complicated to identify which one or which set of quality variables are at faults. Accordingly, even when an out-of-control signal is triggered by MSPC chart, it is difficult to identify which quality variables are responsible for the signal. Therefore, the identification of the source of process faults (PFs) has become an important research issue for business companies.

Due to its importance, the identification of PFs has been greatly investigated in recent years [1–8]. In addition to certain decomposition approaches which have been proposed [1–3], some soft computing techniques have been designed to identify PFs for an out-of-control process. In [4], they made a comparison for the identification performance among artificial neural network (ANN), support vector machine (SVM), and the decomposition methods when the PFs existed in a multivariate process. In [5], they made a comparison between artificial neural network (ANN) classifier with the methods proposed by [1]. For the identification of PFs for a multivariate process, they all concluded that the performance of soft computing methods are better than the decomposition methods. Additionally, although many studies have shown the effective integration of SPC-EPC mechanism to improve the manufacturing processes, there has been very little research addressed on the effectiveness of identification of PFs for the MSPC-MEPC system. Consequently, while most of the research has been devoted to identifying the sources of the PFs for multivariate statistical process control (MSPC) applications, the present study is unique in determining the faults for the combination of MSPC and multivariate engineering process control (MEPC) applications.

The purpose of the present study is to present a useful classifier to identify the PFs for an MSPC-MEPC system. Because of its excellent performance on the classification tasks [9–11], the present study applies the artificial neural network (ANN) technique to serve as the classifier in order to identify the PFs for an MSPC-

MEPC system. The performance of the proposed ANN classifier is evaluated through a series of computer simulations. The rest of this study is organized as follows. Section 2 presents the models of an MSPC-MEPC system. The PFs models are also addressed. The simulation results of the ANN classifier are discussed in Section 3. The final section concludes the present study.

2. THE MSPC-MEPC SYSTEM

Based on their suggestions [12–13], the present study uses the following model (with m inputs and p outputs) to represent an MSPC-MEPC system.

$$y_i \ = \ \alpha + \beta x_{i-1} + a_i, \tag{1}$$

where $y_i(p \times 1)$ is the multivariate process outputs at time i, $\alpha(p \times 1)$ is the offset parameters, $\beta(p \times m)$ is known as the gain parameters, $x_i(m \times 1)$ is the controllable variables, and $a_i(p \times 1)$ is assumed to be the white noise (i.e., normally distributed with mean of zero).

For Equation (1), there is initially no PFs in the system. However, once the PFs have occurred in the system, the system in Equation (1) would become:

$$y_i \ = \ \alpha + \beta x_{i-1} + U_i \tag{2}$$

where U_i is the PFs at time *i*. The present study uses the following PFs models for an MSPC-MEPC system, and they include [21-22].

$$\text{Shift:}\, U_i^{SHI} = R_i + a_i, \tag{3}$$

$$\text{Stratification:}\, U_i^{STA} = ba_i \tag{4}$$

where U_i^{SHI} represents the value of shift (SHI) disturbance at time *i*, R_i stands for the level of shift disturbance, which is assumed to follow a uniform distribution within the range of (1, 2), U_i^{STA} represents the value of stratification (STA) disturbance at time *i*, and *b* represents random noise, which is assumed to follow a uniform distribution within the range of (0.2, 0.4). In addition, Figures 1 and 2 show the patterns for the shift and stratification PFs for a process.

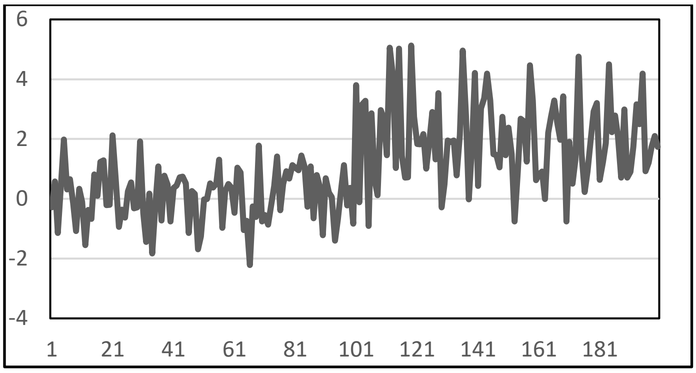


Figure 1. The pattern of the shift PF

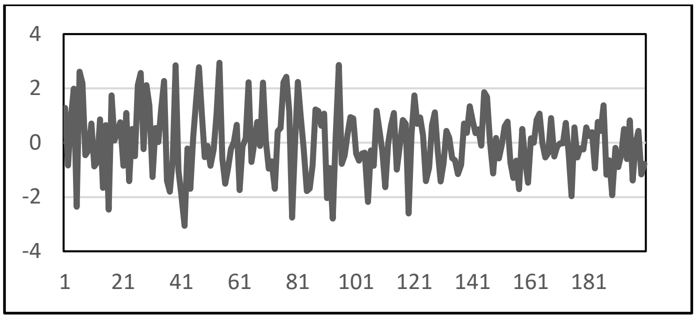


Figure 2. The pattern of the stratification PF

3. RESULTS

The present study uses the ANN classifiers to identify the PFs of an MSPC-MEPC system. The ANN are one of the most common techniques for the classification tasks. For further details and modeling of ANN, please refer to the following research [9–11].

The present study used two designs for ANN classifier. The first design uses the process outputs y to be the input variable. The second design for ANN considers both MEPC adjustments and y as the ANN's inputs. The present study uses 2800 and 1200 data vectors for the training and testing phases, respectively. The present study uses the correct identification rate (CIR) as a performance measure for the ANN classifier. The CIR is defined as:

$$\text{CIR} = {}^{n_c}/_{T}, \tag{5}$$

where T is the total number of observations used for the identification process and n_c is the number of observations in T where the actual PFs are correctly identified.

After performing ANN classification, Table 1 shows the identification results for two PFs in an MSPC-MEPC system. Furthermore, by observing Table 1, we can notice that CIR percentage improvement of the second design over the first scheme are 6.52% and 105.38% for STR and SHI PFs, respectively.

Table 1. *ANN Classification Results of two PFs*

PFs	CIR (first design)	CIR (second design)
STR	53.35%	56.83%
SHI	41.67%	85.58%

4. CONCLUSIONS

The present paper is concerned with the identification of PFs for an MSPC-MEPC systems. We utilize the ANN classifier with two different designs to identify two PFs in a multivariate process. Additionally, the performance of the ANN classifier is conducted through the computer simulations. The second design of the ANN has satisfactory results in identifying PFs for a process.

In this study, we only consider two types of PFs to be identified. Accordingly, an attempt to include more PFs should be a good contribution of future study. Also, some other soft computing techniques, such as support vector machine, extreme learning machine, and/or random forests, are worthy of accomplishment to enhance the CIR for the future research direction.

Acknowledgements: This research is partially supported by the Ministry of Science and Technology of the Republic of China (Taiwan), Grant No. 108-2221-E-030-005.

REFERENCES

[1] Mason, R.L.; Tracy, N.D.; Young, J.C. (1995), Decomposition of T^2 for multivariate control chart interpretation. *J. Qual. Technol.* ***27***, pp. 99–105.

[2] Mason, R.L.; Tracy, N.D.; Young, J.C. (1997), A practical approach for interpreting multivariate T^2 control chart signals. *J. Qual. Technol.* ***29***, pp. 396–406.

[3] Runger, G. C., Alt, F. B., & Montgomery, D. C. (1996). Contributors to a multivariate statistical process control chart signal. *Communications in Statistics: Theory and Methods*, ***25***, pp. 2203-2213.

[4] Shao, Y.E.; Hsu, B.S. (2009), Determining the contributors for a multivariate SPC chart signal using artificial neural networks and support vector machine. *Int. J. Innov. Comput. Inf. Control*, ***5***, pp. 4899–4906.

[5] Aparisi, F.; Avendaño, G.; Sanz, J. (2006), Techniques to interpret T^2 control chart signals. *IIE Trans.* ***38***, pp. 647–657.

[6] Shao, Y.E.; Lu, C.J.; Wang, Y.C. (2012), A hybrid ICA-SVM approach for determining the fault quality variables in a multivariate process. *Math. Probl. Eng.* ***2012***, 284910.

[7] Bersimis, S.; Sgora, A.; Psarakis, S. (2017), Methods for interpreting the out-of-control signal of

multivariate control charts: A comparison study. *Qual. Reliab. Eng. Int.* ***33***, pp. 2295–2326.

[8] Pina-Monarrez, M. (2018), Generalization of the Hotelling's T^2 decomposition method to the R-chart. *Int. J. Ind. Eng. Theory Appl. Pract.* ***25***, pp. 200–214.

[9] Gauri, S.; Chakraborty, S. (2008) Improved recognition of control chart patterns using artificial neural networks. *Int. J. Adv. Manuf. Technol.* ***36***, pp. 1191–1201.

[10] Ebrahimzadeh, A.; Addeh, J.; Rahmani, Z. (2012), Control chart pattern recognition using K-MICA clustering and neural networks. *ISA Trans.* ***51***, pp. 111–119.

[11] Addeh, A.; Khormali, A.; Golilarz, N.A. (2018), Control chart pattern recognition using RBF neural network with new training algorithm and practical features. *ISA Trans.* ***79***, pp. 202–216.

[12 Tseng, S.T.; Mi, H.C.; Lee, I.C. (2016), A multivariate EWMA controller for linear dynamic processes. *Technometrics* ***58***, pp. 104–115.

[13] Yang, L.; Sheu, S.H. (2007), Economic design of the integrated multivariate EPC and multivariate SPC charts. *Qual. Reliab. Eng. Int.* ***23***, pp. 218–2007.