ZULFAQAR International Journal of
Defence Science, Engineering & Technology

Journal homepage: www.zulfaqar.upnm.edu.my

Towards the Data Security and Digital Evidence based Solution in Bangladesh Perspective

Shekh Abdullah-Al-Musa Ahmed[a,*], Nik Zulkarnaen Khidzir[b], Tan Tse Guan[b]

[a] *Faculty of Creative Technology and Heritage, Universiti Malaysia Kelantan, Malaysia*
[b] *Global Entrepreneurship Research and Innovation Centre (GERIC), Universiti Malaysia Kelantan, Malaysia*

*Corresponding author: *almusa.c17e002f@siswa.umk.edu.my*

ARTICLE INFO

Article history:
Received
29-11-2018
Received in revised
20-03-2019
Accepted
29-04-2019
Available online
30-06-2019

Keywords:
Data Security,
Digital Evidence Collections,
Autopsy,
Java,
Java Security.

e-ISSN:
Type: Article

ABSTRACT

Data is anything in a form suitable for use with a computer. Data is often distinguished from programs. A program is a set of instructions that detail a task for the computer to perform. In this sense, data is thus everything that is not program code. Generally and in science, data is a gathered body of facts. Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers data. Data security also protects data from corruption. However in this article would show a method for encryption text data by java program. It will encrypt is such a way that data could not read in plain text. Whereas Forensic science is a combine science. Scientific Evidence is a part of forensic science. By using the forensic science collecting information and present it on the court. So the meaning of evidence of science representing the understanding of collection information by establishes science. For example to create a DNA profile, following the establish protocol to make a DNA profile. So by testing it thousand times it will give the same result. This is the establish rule of science. When applying this rule in the court then it will call scientific Evidence. In Bangladesh most of the time it is seen that judiciary process is depends on confession based. Justice in the lower court does not depend on Digital forensic rather depend on Confession based. The definition of document is given in Section 3 at Evidence Act, 1872 and it is amended by ICT Act 2006 by Section 87 ,it is said that creating document by electronic is also a document .So any picture or video or audio are electronic document is a document .However for digital evidence based solution in this project using autopsy forensic tools, which will run on Kali Linux Forensic mode. It will generate a report paper and calculates MD5 hash values and confirms the integrity of the data before closing the files. Not all computer offence we can called cybercrime , but if a person created forged certificate or steal computer file , may called it as a Digital Crime .In real space , there are some physical force such as robbery , theft etc. But in Digital crime, there is no physical force, but doing the crime by technology.

Introduction

Data security is usually understood to involve availability (e.g. through redundancy and management of the computing environment), integrity (e.g., through backups and verification methods), and controlling access (by authenticating users, and authorizing actions on the data). A famous quote - "It used to be expensive to make things public and cheap to make them private. Now it's expensive to make things private and cheap to make them public" — Clay Shirky, Internet scholar and professor at N.Y.U. In the archival context, including data migration within "security", since using migration to ensure the availability or the intellectual content of the data we maintain, as well as to maintain its integrity (Cremonini et al., 2009). Data security is closely related both to confidentiality (which includes de-identification and relies upon access control), and to digital rights management (which provides a frame-work for authorization). This document is one of three that together, address all these issues. This current document discusses the practices that identified to maintain data integrity and availability. The associated documents address standards data security using java program on kali Linux OS. Data is the raw form of information stored as columns and rows in databases, network servers and personal computers (Molok et al., 2018). This may be a wide range of information from personal files and intellectual property to market analytics and details intended to top secret. Data could be anything of interest that can be read or otherwise interpreted in human form. However, some of this information isn't intended to leave the system. The unauthorized access of this data could lead to numerous problems for the larger corporation or even the personal home user. Having our bank account details stolen is just as damaging as the system administrator who was just robbed for the client information in their database.

There has been a huge emphasis on data security as of late, largely because of the internet. There are a number of options for locking down our data from software solutions to hardware mechanisms. Computer users are certainly more conscious these days, but are our data really secure? If you're not following the essential guidelines, your sensitive information just may be at risk.

Encryption has become a critical security feature for thriving networks and active home users alike. This security mechanism uses mathematical schemes and algorithms to scramble data into unreadable text. It can only by decode or decrypted by the party that possesses the associated key. Full-disk encryption (FDE) offers some of the best protection available. This technology enables you to encrypt every piece of data on a disk or hard disk drive (Posey et al., 2015). Full disk encryption is even more powerful when hardware solutions are used in conjunction with software components. This combination is often referred to as end-based or end-point full disk encryption.

Authentication is another part of data security that we encounter with everyday computer usage. Just think about when loging into email or blog account. That single sign-on process is a form authentication that allows us to log into applications, files, folders and even an entire computer system . Once logged in, we have various given privileges until logging out. Some systems will cancel a session if your machine has been idle for a certain amount of time, requiring that proved authentication once again to re-enter. The single sign-on scheme is also implemented into strong user authentication systems. However, it requires individuals to login using multiple factors of authentication. This may include a password, a one- time password, a smart card or even a fingerprint (Korchenko et al., 2010)

Data security wouldn't be complete without a solution to back-up your critical information. Though it may appear secure while confined away in a machine, there is always a chance that our data can be compromised. You could suddenly be hit with a malware infection where a virus destroys all of your files. Someone could enter your computer and thieve data by sliding through a security hole in the operating system. Perhaps it was an inside job that caused our business to lose those sensitive reports. If all else fails, a reliable backup solution will allow us to restore your data instead of starting completely from scratch (Manes et al., 2010).

Literature Review

Forensic science is a combine science. Scientific Evidence is a part of forensic science. By using the forensic science collecting information and present it Data Security and Digital Evidence based Solution on the court. So the meaning of evidence of science representing the understanding of collection information by establishes science. For example to create a DNA profile, following the establish protocol

to make a DNA profile. So by testing it thousand times it will give the same result. This is the establish rule of science, When applying this rule in the court then it will call scientific evidence. According to Hinson in the book Pragmatic - Security Metrics said about the watermarking for data security. They added that the process can be used to hide secret data to communicate between the parties so that the party will send the message to hide the message within the data and send it and the other side is the receipt of data and extract the hidden message using a specific algorithm to be agreed upon between the two parties. The watermark is one of the most important applications to hide data which is about changes in the original work (digital data) to add owner information to work (digital data as well) within this work (Fig.1). Different watermarking method camouflage stenography in camouflage hidden data while interested in the watermark interest is the protection of the work itself and not hidden data Watermark must resist any amendment to the original work (D'Arcy et al., 2014).

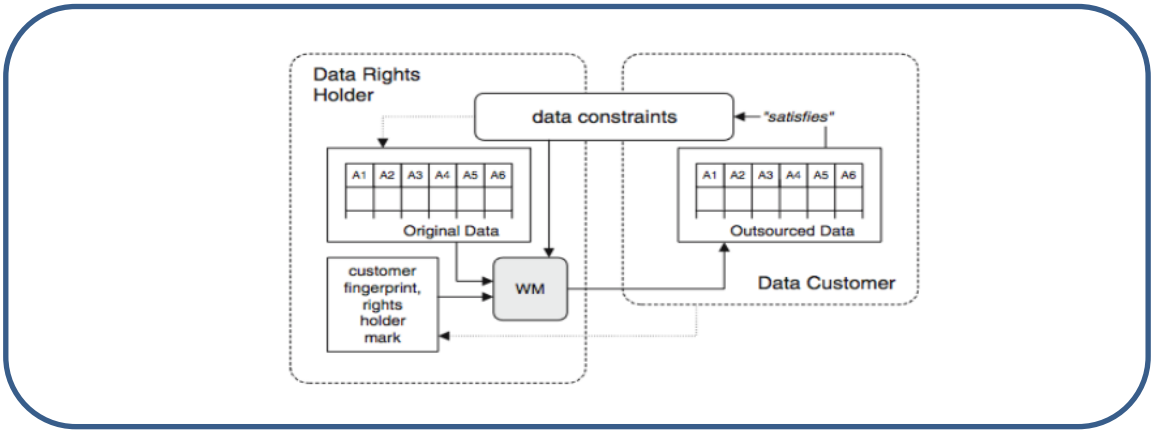

Fig.1: Showing the watermarking methods, a set of data constraints are continuously evaluated in the encoding process to ensure quality of the result.

May be exposed watermark for many different threats that attempt to remove or modify the watermark. Including image compression, start jamming, conversion to another domain, different filters, sports transfers, tag, pseudo revoke parts of the image randomly had lost a large part of the watermark can increase the effectiveness of the watermark by repetition, temporal or spatial fingerprints, and use more than one algorithm at the same time.

Cryptographic software often plays a critical role in computational systems. Any failure or deficiency in a cryptographic module can be exploited to compromise the system's safety, which can lead to catastrophic events from the security point of view. Every system that runs cryptographic software does it because it needs to protect information. From the email sent between friends, to industrial projects or government secrets, the need to hide data from an adversary is real and necessary. In the modern society, where the access and use of computer networks is something that grows every day, the use of Cryptography is imperative (Cremonini et al., 2009). When correctly implemented and used, cryptography is able to effectively protect data. Not because it is absolutely unbreakable, but because it makes un-authorized acquisition of the information computationally infeasible or cost-prohibitive. A programmer willing to protect some sensitive data should choose the most appropriate cryptographic technique, find a detailed description to permit its encoding in the target programming language, adopt formats for the data and be aware of die rent sorts of vulnerabilities and associated counter-measures. It is definitely a difficult task that demands deep knowledge in a wide range of areas. Some guidelines are needed and here's where the cryptography standards appear. The elements are confidentiality, possession, integrity, authenticity, availability, and utility. The merits of the Parkerian Hexad are a subject of debate amongst security professionals (Molok et al., 2018). In 2011, The Open Group published the information security management standard O-ISM3. Digital forensic in Autopsy is a user interface that makes it simpler to deploy many of the open source programs and plug-in used in the Sleuth Kit collection. The graphical user interface displays the results from the forensic search of the underlying volume making it easier for investigators to flag pertinent sections of the data (Buskirk et al., 2006). The tool is largely maintained by Basis Technology Corporation with the assistance of programmers throughout the community. The company sells support services and training for using the product. Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the

recovery and investigation of material found in digital devices, often in relation to computer crime (Buskirk et al., 2006). In computer science, data is anything in a form suitable for use with a computer. Data is often distinguished from programs. A program is a set of instructions that detail a task for the computer to perform. In this sense, data is thus everything that is not program code. Generally and in science, data is a gathered body of facts. Some authorities and publishers, cognizant of the word's Latin origin and as the plural form of "datum," use plural verb forms with "data". Others take the view that since "datum" is rarely used, it is more natural to treat "data" as a singular form. Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption. Data security is the main priority for organizations of every size and genre. Examples of data security technologies include software/hardware disk encryption, backups, data masking and data erasure. A key data security technology measure is scrambling, where digital data, soft-ware/hardware, and hard drives are scrambled and rendered unread-able to unauthorized users and hackers.

Methodology

Information security must protect information throughout the life span of the information, from the initial creation of the information on through to the final disposal of the information. The information must be protected while in motion and while at rest. During its life-time, information may pass through many different information processing systems and through many different parts of information processing systems. There are many different ways the information and information systems can be threatened. To fully protect the information during its lifetime, each component of the information processing system must have its own protection mechanisms. The building up, layering on and overlapping of security measures is called defense in depth. In contrast to a metal chain, which is famously only as strong as its weakest link, the defense-in-depth aims at a structure where, should one defensive measure fail, other measures will continue to provide protection. However in this article emphasize on to write java program in serialization and deserialization method. Serialization in java is a mechanism of writing the state of an object into a byte stream. Java provides a mechanism, called object serialization where an object can be represented as a sequence of bytes that includes the object's data as well as information about the object's type and the types of data stored in the object (Cremonini et al., 2009). After a serialized object has been written into a file, it can be read from the file and de-serialized that is, the type information and bytes that represent the object and its data can be used to recreate the object in memory.

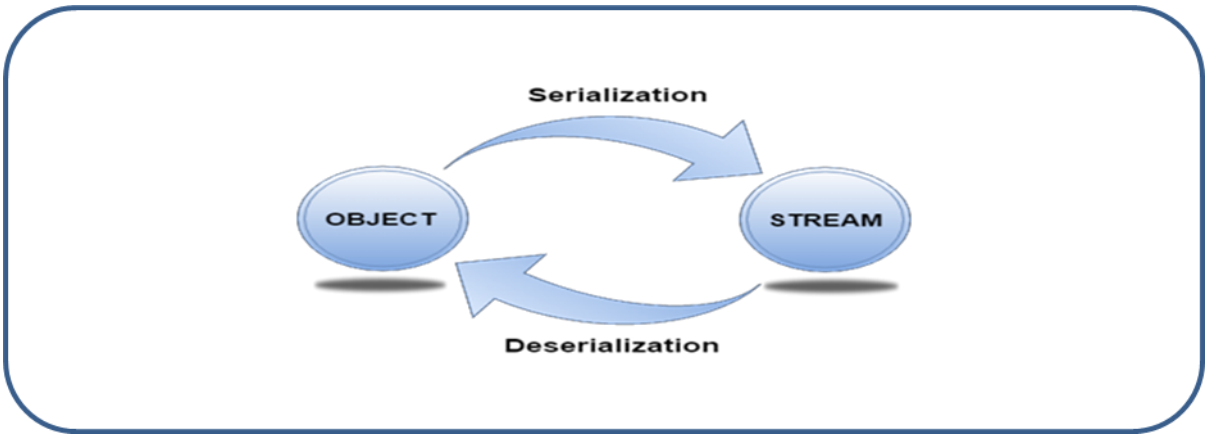

Fig. 2: Showing the Java method for converting data into an-other format

Classes Object Input Stream and Object Output Stream are high-level streams that contain the methods for serializing and desterilizing an object. The Object Output Stream class contains many write methods for writing various data types, but one method in particular stands out – public final void write Object (Object x) throws I/O Exception. The above method serializes an Object and sends it to the output stream. Similarly, the Object Input Stream class contains the following method for desterilizing an object –public final Object read Object (Object x) throws I/O Exception, Class Not Found Exception. This method retrieves the next Object out of the stream and desterilizes it. The return value is Object, so you will need to cast it to its appropriate data type. Suppose that having the following Employee class, which

implements the Serializable interface. Neither so encrypted text in such a manner that intruder neither can nor read the message. Another thing is how to collect digital information and submit it to court. Not all computer offence can called cybercrime, but if a person created forged certificate or steal computer file, may called it as a Digital Crime .In real space, there are some physical force such as robbery, theft etc. But in Digital crime, there is no physical force, but doing the crime by technology (Taylor et al., 2015). However in real space, if any crime happens, then can determine where and what time this crime is happened. But in the case of digital crime, it is difficult to find out the time and place, that is why it is difficult to find out the criminal in digital space. So, someone has done a crime by computer, police may be seize the computer. And how to take the evidence from this computer, and how this evidence should be present in the court, that we don't know. Suppose any cybercrime happened in Bangladesh. Then where shall we go for this? If any digital crime is happened in our country, then we have to go to Police. But there is a problem; here police cannot investigate for himself. The ICT Act, 2006 said about a Controller. So, should take permission from the controller. It is a problem. Because if any physical crime is happened in a place, then there would be some evidence. But in the case of digital crime, the evidence can be deleted so easily with software. So if someone goes to the police and when police is wait for controller permission, in this time the evidence could be deleted. It means digital crime evidence is very short time evidence. The problem of ICT Act, 2006 there is no framework to take digital evidence to court (Kim et al., 2013).

Data Security Types

Data security means protecting data, such as a database, from destructive forces and from the unwanted actions of unauthorized users. So another way can explain Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption. Data security is the main priority for organizations of every size and genre (Molok et al., 2018).

Examples of data security technologies include software/hardware disk encryption, backups, data masking and data erasure. A key data security technology measure is scrambling, where digital data, software/hardware, and hard drives are scrambled and rendered unreadable to unauthorized users and hackers.

Data security is also very important for health care records, so health advocates and medical practitioners in the U.S. and other countries are working toward implementing electronic medical records (EMR) privacy by creating awareness about patient rights related to the release of data to laboratories, physicians, hospitals and other medical facilities.

Software-based security solutions encrypt the data to protect it from theft. However, a malicious program or a hacker could corrupt the data in order to make it unrecoverable, making the system unusable. Hardware-based security solutions can prevent read and write ac-cess to data and hence offer very strong protection against tampering and unauthorized access.

Hardware based security or assisted computer security offers an alternative to software-only computer security. Security tokens such as those using PKCS#11 may be more secure due to the physical access required in order to be compromised. Access is enabled only when the token is connected and correct PIN is entered (see two-factor authentication). However, dongles can be used by any-one who can gain physical access to it. Newer technologies in hardware-based security solve this problem offering full proof security for data (Posey et al., 2015).

A hardware device allows a user to log in, log out and set different privilege levels by doing manual actions. The device uses biometric technology to prevent malicious users from logging in, logging out, and changing privilege levels. The current state of a user of the device is read by controllers in peripheral devices such as hard disks. Illegal access by a malicious user or a malicious program is interrupted based on the current state of a user by hard disk and DVD controllers making illegal access to data impossible. Hardware-based access control is more secure than protection provided by the operating systems as operating systems are vulnerable to malicious attacks by viruses and hackers. The data on hard disks can be corrupted after a malicious access is obtained. With hardware-based protection, software can-not manipulate the user privilege levels. It is impossible for a hacker or a malicious program to gain access to secure data protected by hardware or perform unauthorized privileged operations. This assumption is

broken only if the hardware itself is malicious or contains a backdoor. The hardware protects the operating system image and file system privileges from being tampered. Therefore, a completely secure system can be created using a combination of hardware-based security and secure system administration policies.

Constitution of Digital evidence

Electronic evidence is valuable information stored or transmitted in digital form. Anyone can use the digital evidence into the court, make them as real evidence and submit as digital evidence to trial. It is not only the information that is stored, but also the way the evidence is gathered. Its latent, alterable, perpetual and vulnerable nature distinguishes it from documentary and oral evidences. The court needs to judge about the evidence is real and relevant. Although there are so many differences between real-life and the virtual life but still digital evidence would be counted as important evidence document. The evidences should be authentic. According to the author Hinson (2007), the word authentic means "having a claimed and verifiable origin or author-ship". The use of digital evidence has increased in the past few decades as courts have allowed the use of e-mails, digital photographs, ATM transaction logs, word processing documents, instant message histories, files saved .From accounting programs, spreadsheets, internet browser histories, databases, the contents of computer memory, computer backups, computer printouts, Global Positioning System tracks, logs from a hotel's electronic door locks, and digital video or audio files. As we pointed out earlier that ICT Act failed to provide robust guideline for the acquisition & retention of computer generated evidence. Here I would like to refer to Section 9 of the ICT Act, 2006 (Peltier et al., 2006), in favor of my arguments. Section 9 of the ICT Act, 2006 provides that: The Act gives a statutory definition of the criminal offence of fraud, defining it in three classes - fraud by false a fine and a new offence of participating in fraudulent business carried on by a sole trader was established by Section 9. Further, in the ICT Act, the exact qualification of a forensic expert is not notified yet. In Bangladesh, we do not have a national accreditation program for expert witnesses in computer forensics which would definitely assist the courts in testing the qualifications of expert witnesses.

A computer forensic expert plays a vital role in criminal/civil justice system, and selection of experts must not be done in haste. Some-time, a qualified expert may shed light to a dark arena and trace new evidence which in long run change the verdict. For example, in the case of Peach v Bird (2006), the defendant had been acquitted of charges of possessing child pornographic images. An appeal was lodged. Although no images of child pornography were able to be recovered from the hard drive, the forensic examiner, using "En-Case software" found various incriminating file names as well as evidence that the hard drive had been erased and overwritten in an attempt to remove evidence.

Discussion and Conclusion

This article focus on how to make secure the data in digital evidence based solution. However there is a perception that computer generated evidence or digital evidence somehow changes the true nature of the original evidence and is therefore untrustworthy. If presented properly with due authentication, digital evidence can be capable of offering tremendous help to the courts. In many cases, digital evidence has allowed the courts to gain valuable information which to some extant ensure correct verdict. Further, it has allowed the court to receive evidence that it would not have been able to receive without the assistance of digital technology. But unfortunately, in our country, courts are not fortunate enough to be aided by digital technology as the existing legal framework is not equipped to handle digital evidence. The laws relating to the admissibility of documentary evidence in Bangladesh are convoluted and not designed to deal with electronic data in mind. In the absence of any amendment, Evidence Act (I of 1872) is not modern enough to facilitate the concept of digital evidence. It is surprising to know that we don't have any statutory provision to deal with any digital evidence except the ICT Act (Maruf et al, 2010). India and Bangladesh both inherited the old British colonial regulation from their inception, but India managed to amend its statutes and became very much familiar with the impact of modern high-tech gadgets. The Indian Evidence Act (I of 1872) as amended by the Information Technology Act 2000 elaborately deals with the issues of admissibility of electronic records (Section 65-B). But as a colonial cousin we failed to do the same. We are to some extent living in the realm of law, having the characteristics of a pre-modern society. We have successfully enacted ICT Act in 2006 which attempts to render the admissibility of digital evidence, including electronic evidence, but we were unable to eliminate foreseeable lacunas in it.

As a result the ICT Act 2006 failed to acknowledge a range of forensic procedures and practices which are very much needed in ensuring authenticity of a data. Further, poor acquisition guideline made the process of retention of digital evidence so vulnerable that ensuring Integration of Forensic Techniques into the Threshold of Admissibility as Evidence 63 authenticity of a data became an impracticable task (Sakil, 2018). Therefore, an amendment of both the Act is a dire need. As the chances of success in litigation depend heavily on the availability of strong evidence, new or amended Evidence Act is essential for handling digital evidence. New or amended Evidence Act should suggest different procedures for authentication of electronic evidence, as with the establishment of a complete chain of custody, from the person who first copied the data to the person who produced the printout for the trial, or the use of electronic signatures.

References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology, 33*(3), 237-248.

Algarni, A., Xue, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook. *European Journal of Information Systems 26*(6), 661-687.

Applegate, S. D. (2009). Social Engineering: Hacking the Wetware! *Information Security Journal: A Global Perspective, 18*(1), 40-46.

Brill, A., Pollit, M., & Whitcomb, C. M. (2006). The Evolution of Computer Forensic Best Practices: An Update on Programs and Publications. *Journal of Digital Forensic Practice, 1*(1), 3-11.

Brotby, W. K. & Hinson, G. (2013). *PRAGMATIC Security Metrics: ApplyingMetametrics to Information Security* . CRC Press.

Buskirk, E. V. & Liu, V. T. (2006). Digital Evidence: Challenging the Presumption of Reliability. *Journal of Digital Forensic Practice, 1*(1), 19-26.

Cheung, S. K. S. (2005). Information Security Management for Higher Education Institutions. Intelligent Data analysis and its Applications, 1(2-3), 55-68.

Cremonini, M. & Nizovtsev, D., (2009). Risks and Benefits of Signaling Information System Characteristics to Strategic Attackers. *Journal of Management Information Systems, 26*(3), 241-274.

D'Arcy, J., Herath, T. & Shoss, M.K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems, 31*(2), 285-318.

Duff, A. S. (2005) Social Engineering in the Information Age*. An International Journal, 21*(1), 67-71.

Gonzales, R., Llopis, J. & Gasco, J. (2013). Information technology outsourcing in financial services. *The Service Industries Journal, 33*(9-10), 902-924.

Hinson, G. (2007). The State of IT Auditing in 2007. *The EDP Audit, Control, and Security Newsletter, 36*(1), 13-31.

Kebande, V. R. & Venter, H. S. (2018). Novel digital forensic readiness technique in the cloud environment. *Australian Journal of Forensic Sciences, 50*(5), 552-591.

Kim, E. B. (2013). Information Security Awareness Status of Business College: Undergraduate Students. *Information Security Journal: A Global Perspective, 22*(4), 171-179.

Korchenko, O., Vasiliu, Y. & Gnatyuk, S. (2010). Modern quantum technologies of information security against cyber-terrorist attacks. *Aviation, 14*(2), 58-69.

Manes, G. W. & Downing, E. (2010). What Security Professionals Need to Know About Digital Evidence. *Information Security Journal: A Global Perspective, 19*(3), 124-131.

Manske, K. (2006). An Introduction to Social Engineering. *Information Systems Security, 9*(5), 1-7.

Maruf, A., Islam, M. R. & Ahamed, B. (2010). Emerging Cyber Threats in Bangladesh: In Quest of Effective Legal Remedies. *Northern University Journal of Law, 1*(4), 112-124.

Mohamed, N., Nawawi, A., Ismail, I. S., Ahmad., S. A., Azmi, N. A. & Zakaria, N. B. (2013). Cyber fraud challenges and the analysts competency: Evidence from digital forensic department of Cyber Security Malaysia. Recent Trends in Social and Behaviour Sciences - Proceedings of the 2nd International Congress on Interdisciplinary Behavior and Social Sciences, 581-583.

Molok, N. N. A., Ahmad, A. & Chang, S. (2018). A case analysis of securing organisations against information leakage through online social networking. *International Journal of Information Management, 43*(4), 351-356.

Myyry, L., Siponen, M.,Pahnila, S. & Vartiainen, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, 18(2), 126-139.

Peltier, T. R. (2006). Social Engineering: Concepts and Solutions. *Information Systems Security, 15*(5), 13-21.

Pieters, W. (2011). The (Social) Construction of Information Security. *The Information Society, Volume 27*(5), 326-335.

Posey, C., Roberts, T. L. & Lowry, P. B. (2015). The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. *Journal of Management Information Systems, 32*(4), 179-214.

Sakil, A. H. (2018). ICT, youth and urban governance in developing countries: Bangladesh perspective, *International Journal of Adolescence and Youth, 23*(4), 219-234.

Singleton, T. W. & Singleton, A. J. (2008). The Potential for a Synergistic Relationship Between Information Security and a Financial Audit. *Information Security Journal: A Global Perspective, 17*(2), 80-86.

Sumner, M. (2009). Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness. *Information Systems Management, 26*(1), 2-12.

Taylor, R. G. (2015). Potential Problems with Information Security Risk Assessments. *Information Security Journal: A Global Perspective, 24*(4-6), 177-184.

Wiebke, A. (2009). Agents, Trojans and tags: The next generation of investigators. *International Review of Law, Computers & Technology, 23*(1-2), 99-108.