



## Website Assurance Monitoring Application with MD5 Hashing and SHA-26 Algorithm

**Abdullah Sani Abd Rahman**

Faculty of Sciences and Information Technology, Universiti Teknologi Petronas, Perak, Malaysia  
sani.arahman@utp.edu.my

**Samsiah Ahmad**

Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Perak Branch Tapah Campus, Perak, Malaysia  
samsi260@uitm.edu.my

---

### Article Info

#### Article history:

Received Feb 05, 2022

Revised March 15, 2022

Accepted Apr 25, 2022

---

#### Keywords:

Website assurance  
Monitoring  
MD5  
SHA26  
Graphical User Interface

---

### ABSTRACT

Websites attack by falsifying the websites contents is a serious matter of websites assurance nowadays. This problem can become more crucial if the websites authority do not take regular checking or lack of specialized experts in monitoring the changes. Time consuming and growing of websites complexity is additional reasons of the inadequate website assurance. This paper presents a new framework for websites integrity assurance through a website monitoring application. The monitoring application able to detect any modification on a website to be reverted to the actual version. The Website Assurance Monitoring application has been developed based on MD5 hashing technique and SHA26 algorithm. By using Microsoft Visual Basic 6.0, the Graphical User Interfaces (GUIs) of the application to provide an easy or user-friendly monitoring application. During the implementation testing, the functionality and usability of the website assurance application have been verified by different level of computing expert users. All the expert users agreed that the website assurance application is accurate and sufficient to detect changes occurred in websites. Regarding to processing time, majority of the inexpert computing users experienced easy and fast processing. Additionally, most of these users believed that this application can increase the integrity of a website. The proposed websites assurance monitoring application is beneficial to serve the inexpert websites authority with a user-friendly application. The application can help the administrator to preserve the integrity of a website by automatically detecting any unauthorized contents changes.

---

### Corresponding Author:

Abdullah Sani Abd Rahman

Faculty of Sciences and Information Technology, Universiti Teknologi Petronas, Perak, Malaysia

Email: sani.arahman@utp.edu.my

---

### 1. Introduction

Websites on the internet are connected by various network to be surfed by billions of various peoples, mostly because they need to get information. Unfortunately, there exists some of websites visitors that browse the contents with bad intention such as to hack to important contents due to many possible reasons include curiosity and challenge of hacking skills, sabotage and revenge. In the 2015 only, there are 11,107,846 defaced websites belong to educational institution in ASEAN have been detected, which effected to 3512 websites from Malaysia[1]. Beside educational



---

institutions, most hackers aim for government and high profit organization with the common targets including political jeopardize.

Integrity and privacy of information can be measured with many kinds of security mechanism. One way is to support encryption process to provide confidentiality, reliable authentication and integrity. Another way is to equip the websites with digital signature component to assure non-repudiation control. Checksums or hashing is also useful to ensure integrity and authentication. MD5 hashing technique are widely used to provide some assurance of protecting data and information in many kinds of computer system. MD series has been reviewed continuously to improve its performance and speed. MD hashing has been combined with SHA compression series such as SHA256 to increase the encryption performances. Research on MD5 and SHA256 in computer security is expanding and research fills the gap by presenting Graphical User Interface (GUI) for non-expert users to conduct web monitoring.

## **2. Literature Review**

Web pages have evolved into a very complex and dynamic websites applications. At the same time, despite its complexity, the contents of websites confronted with some important security risks. Therefore, research on web security has been rapidly progressed to discover strategies and techniques for more reliable web applications. Some of the proposed techniques employed machine learning detection model. For example the research in [2] that use Convolutional Neural Network (CNN) to detect the anomaly web attack. Similarly, CNN has also been used in [3] but the researchers extended the single CNN used in website features extraction with Bayesian classifier for detecting the attack. Memory CNN is another work introduced by [4] to incorporate the conventional CNN with long short-term memory (LSTM) used to detect the sequence of requests sent by a web attacker. Acknowledging that websites security is complex with multi-attributes components that need to be observed with different perspectives, deployment of decision support tool for the web security has been proposed by many researchers. Fuzzy Analytic Hierarchy Process (Fuzzy AHP) [5] and Unified Fuzzy symmetrical multi-criteria decision-making [6] are the research works that cater the multi-attributes components of websites monitoring. In [7], Fuzzy multi-objective technique was used for mitigating risk of website focusing on medical image processing system. Different in [8] and [9], two different CAPTCHA techniques have been adapted by the two different studies to enhance website security against bots, spam and web attacks. Understanding human behavior on website security is another interesting research. Understanding passwords of Chinese web users from their birthday, name and bifacial-security is the work proposed by [9]. Meanwhile, the pattern of click-related behaviors on the web and its impact to the web security has been introduced by the researchers in [10]. Getting insight on users perception, awareness and behavior on web privacy tools has been reported in [11]. To educate and raising awareness on web security, cyber security social engineering research has been conducted by researchers in [12]. To deal with human attitudes towards web security, researchers in [1], [13] established security policies to enforce success implementation of web security among the users. Using encrypted algorithm as introduced in [14] has given me an attractive idea to use MD5[15] hash function and SHA-256[16] algorithm for the Website Assurance Monitoring system.

## **3. Research Method**

### **3.1 Development Tools**

The main tools for this application development is Microsoft Visual Basic 6.0 to develop the GUI. Microsoft Access is the database platform in the application and IIS server used to store all the websites to be monitored by the application. The communication between client and server was supported by File Transfer Protocol (FTP), which is the simplest way to exchange files between computers on the Internet. For the security mechanism, hashing and compression with MD5 (RFC1321) and SHA-256 have been used. Research has revealed that MD5 is the fastest while SHA-256 is the strongest security measure. Combining MD5 and SHA-256 can compliment each other to resolve the slower processing in SHA-256 and least strong ability in MD5 (Refer Table 1).

Table 1. Comparison of Algorithm

Algorithm	Security level	Speed
MD5	Least strong	Fastest
SHA-1	Medium strong	Medium
SHA-256	Strongest	Slowest

Table 1 show that the characteristics of three hashing and compression algorithms, which the strongest security support is provided by SHA-256 but it is the slowest algorithm to complete[17].

### 3.2 Application Architecture

The architecture to describe the Website Assurance Monitoring application is divided into three sections which are the primary architecture, application flow and algorithm architecture. The primary architecture is presented in the following Figure 1.

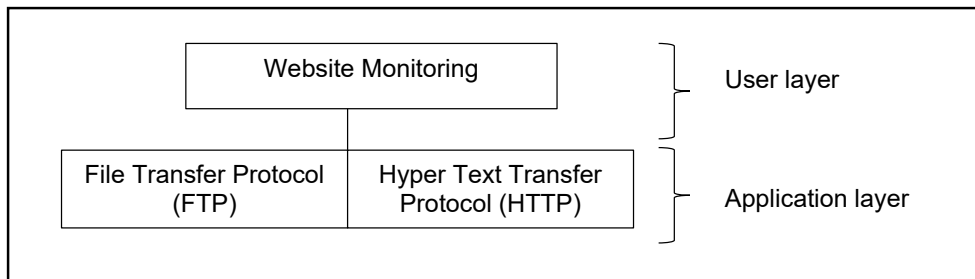


Figure 1. Primary architecture

The primary architecture presents the logical structure of the application, which is divided into user layer and application layer. The developed application with GUI support is the main component in the user layer. In the application layers, FTP and HTTP are the two network application with TCP/IP protocol. Furthermore, the flowchart of the application is depicted in Figure 2.

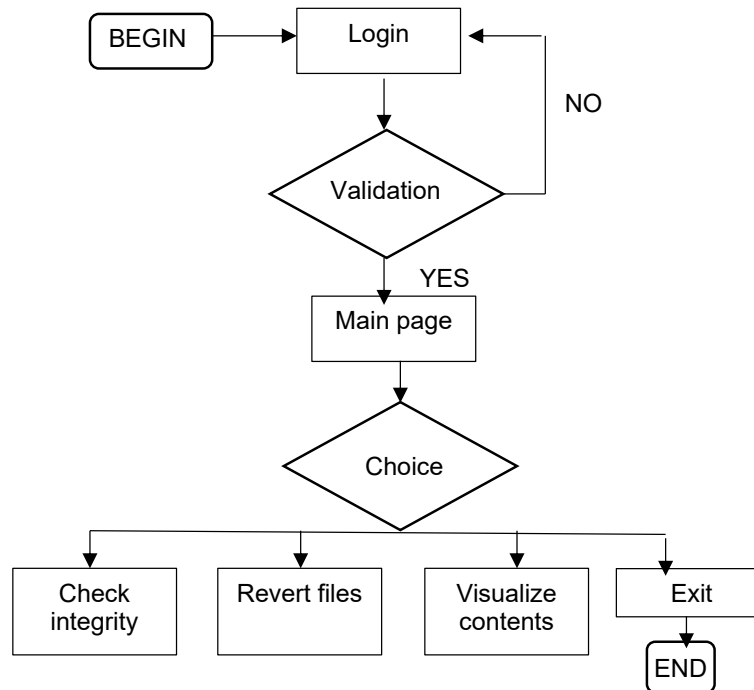


Figure 2. Application flow

From the login page (refer to Figure 3), user needs to key in the admin username and password for authentication process that only allow three time of attempts.

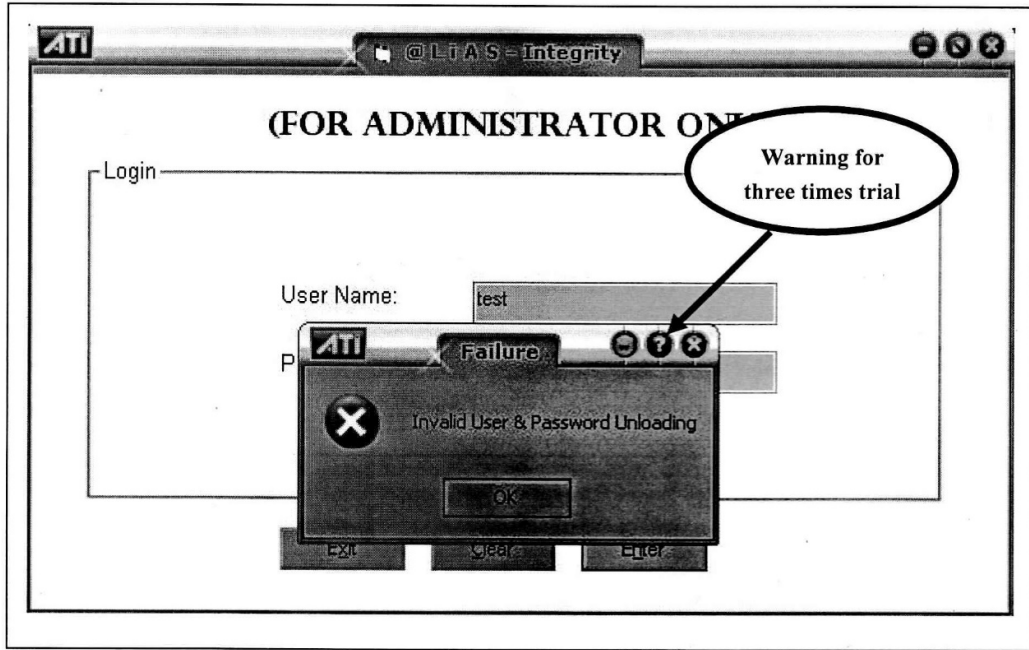


Figure 3. Login menu

In the main page, users are provided with four choices namely check integrity, revert files, visualize contents and exits. To check the integrity, user can enter the source file (htm or html file), click the Hash and Compare buttons as seen in Figure 4.

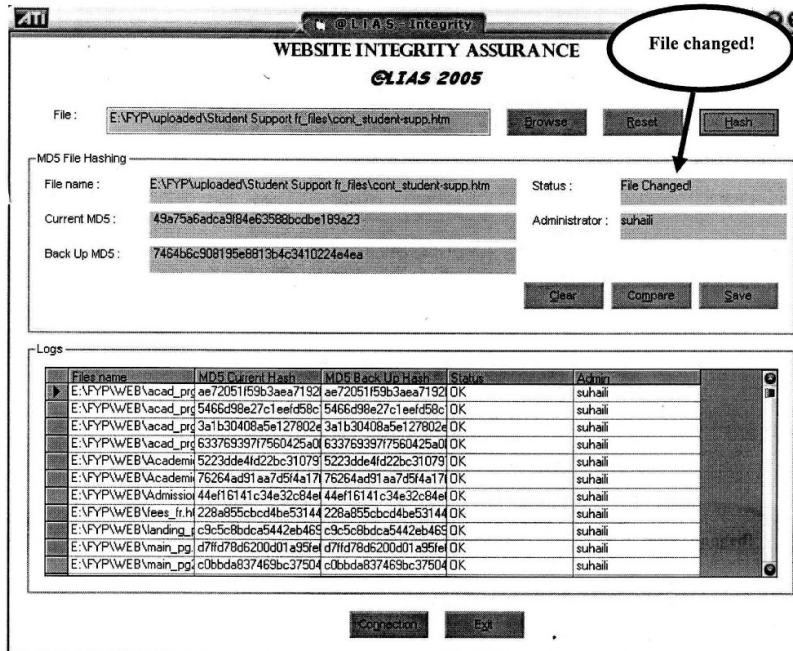


Figure 4. Main menu and status File Changed

As for an example, Figure 4 shows that the file hashed was already changed because the checksum files (Current MD5 and Back Up MD5) were totally different. At the logs part, the application shows the list of history files that have been compared previously. The following Figure 5 shows the page if no modification has been made on the compared files.

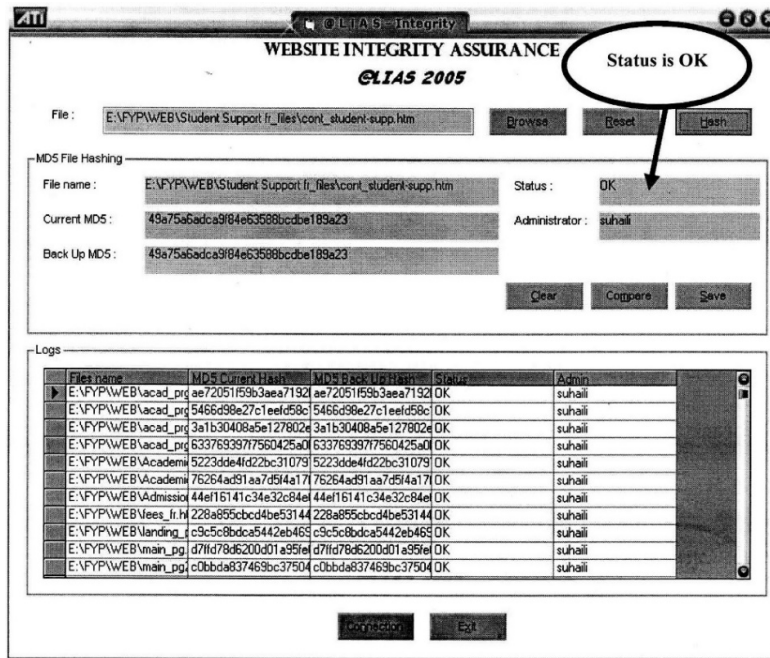


Figure 5. Main menu and status OK

If the user click Compare button, detail comparison of the two files will be displayed. Pop up message box will appear to notify the user and the changes codes are highlighted so that the users can easily detect and modify the codes. Figure 6 presents the compare page.

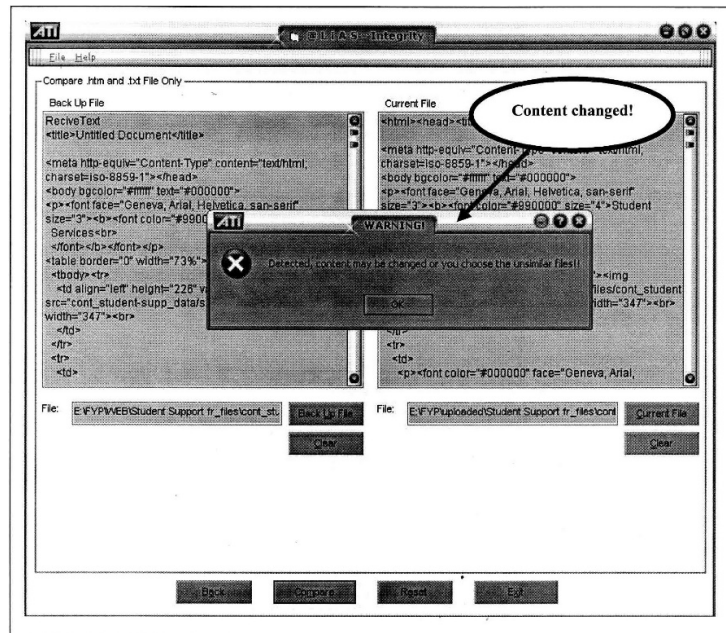


Figure 6. Compare page

---

### 3.3 Application evaluation

Functional and usability evaluation have been conducted to test the Website Assurance Monitoring application. Functional evaluation will verify the ability of the application to detect changes on a modified website while usability subjects involved two types of users either expert or unexpert computer security literate. All the users worked in the University Teknologi Petronas, Seri Iskandar, Perak. The expert users were the IT department staffs and lecturers who teach Computer Science subjects while the inexpert were randomly selected from students who were not from the Computer Science and Information Technology courses.

## 4. Results and Discussion

### 4.1 Functionality Test Result

Figure 6 was a webpage from the original creation while Figure 7 was the webpage after changes have been made. Modification on the webpage was done for the purpose of testing the Website Assurance Monitoring application. All the users who embarked on the usability survey used to given webpages without any prior explanation on the webpage's contents. They only been asked to compare the contents of the two webpages. The results of usability testing is depicted in Table 2.

Table 2. Results of usability testing

	Expert users (n=30)		Inexpert users (n=100)	
	Accuracy (%)	Trustworthy (%)	Easy to Use (%)	Trustworthy (%)
<b>Agreed</b>	100	85	82	60
<b>Undecided</b>	0	12	13	35
<b>Not agreed</b>	0	3	5	5

Based on 30 numbers of expert users, all of them agreed that the Website Assurance Monitoring able to detect the changes accurately and most of them (85%) believe that the application can be relied to ensure the integrity of a website (85% of trustworthy). There exists 12% the expert users were undecided on the trustworthy as they believed that the security of websites not only relied on the websites contents but requires others aspects to be concerned. The rest of 3% that not agreed with the trustworthy is the lecturer who never teach Computer Security subject.

Easy is use is the most positive feedback given by the 100 of inexpert users. Although they did not have strong knowledges on computing and computer security, the perceived that the website assurance is good to be used by end users. However, not many of the inexpert users believed that the application is good enough for trustworthy. Only 60% of the inexpert users agreed on trustworthy compared to 85% of the expert users.

## 5. Conclusion

The main task of the Website Assurance Monitoring application is to detect changes of website and notify the administrator on the web attack scenario. In essence, we have the same opinion with the expert comments that mentioned this application is not exactly applicable to avoid threat but it is good enough to reduce the web attack that may occur from the contents modification. Thus, this application received instructive recommendations from the expert users to improve the functionality including to consider computer forensic ability to investigate the details of hackers. Additionally, to provide varieties on the hacking algorithm will make the application more robust such as to allow users to choose any algorithm from the SHA series such as SHA-1, SHA-224 and SHA-512 to be combined with the MD5. As the application only detecting text file from the web page codes, it is suggested for future enhancement to include image or video contents screening.

---

## Acknowledgements

The authors gratefully acknowledge the student (Nur Suhaili Ramli) from the Universiti Teknologi Petronas who developed the Website Assurance Monitoring system. We also like to thanks both Universities from the Universiti Teknologi Petronas and Univesiti Teknologi MARA (Perak Branch) for the support.

## Conflict of Interest



The authors declare no conflict of interest in the subject matter or materials discussed in this manuscript.

## References

- [1] M. A. Soetomo and R. Aseptia, "Risks Mitigation of Defacement Attack Vectors on Educational Institution Websites by Using OWASP and Risk IT Frameworks," *ACMIT Proc.*, vol. 3, no. 1, pp. 14–23, 2016.
- [2] A. Tekerek, "A novel architecture for web-based attack detection using convolutional neural network," *Comput. I& Secur.*, vol. 100, p. 102096, 2021.
- [3] X. Gong *et al.*, "Estimating web attack detection via model uncertainty from inaccurate annotation," in *2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, 2019, pp. 53–58.
- [4] I. Jemal, M. A. Haddar, O. Cheikhrouhou, and A. Mahfoudhi, "M-CNN: a new hybrid deep learning model for web security," in *2020 IEEE/ACS 17th International Conference on Computer Systems and Applications (AICCSA)*, 2020, pp. 1–7.
- [5] A. Agrawal, M. Alenezi, R. Kumar, and R. A. Khan, "Measuring the sustainable-security of Web applications through a fuzzy-based integrated approach of AHP and TOPSIS," *IEEE Access*, vol. 7, pp. 153936–153951, 2019.
- [6] P. H. Phung, H.-D. Pham, J. Armentrout, P. N. Hiremath, and Q. Tran-Minh, "A user-oriented approach and tool for security and privacy protection on the web," *SN Comput. Sci.*, vol. 1, no. 4, pp. 1–16, 2020.
- [7] R. Ranchal, B. Bhargava, P. Angin, and L. ben Othmane, "Epics: A framework for enforcing security policies in composite web services," *IEEE Trans. Serv. Comput.*, vol. 12, no. 3, pp. 415–428, 2018.
- [8] K. M. Alalayah, "reCAPTCHA: Human Based Embedded Image Generation and Recognition for Web Security," *Int. J.*, vol. 9, no. 7, 2021.
- [9] D. Wang, P. Wang, D. He, and Y. Tian, "Birthday, name and bifacial-security: understanding passwords of Chinese web users," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 1537–1555.
- [10] I. Sanchez-Rola, D. Balzarotti, C. Kruegel, G. Vigna, and I. Santos, "Dirty clicks: A study of the usability and security implications of click-related behaviors on the web," in *Proceedings of The Web Conference 2020*, 2020, pp. 395–406.
- [11] P. Story *et al.*, "Awareness, adoption, and misconceptions of web privacy tools," *Proc. Priv. Enhancing Technol.*, vol. 2021, no. 3, pp. 308–333, 2021.
- [12] H. Aldawood and G. Skinner, "Educating and raising awareness on cyber security social engineering: A literature review," in *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, 2018, pp. 62–68.
- [13] D. L. Bishop, "Improvements of User's Security and Privacy in a Web Browser," University of Dayton, 2021.
- [14] J. Simarmata *et al.*, "Implementation of AES Algorithm for information security of web-based application," *Int. J. Eng. Technol.*, vol. 7, no. 3.4, 2018.
- [15] A. M. Ali and A. K. Farhan, "A novel improvement with an effective expansion to enhance the MD5 hash function for verification of a secure E-document," *IEEE Access*, vol. 8, pp. 80290–80304, 2020.
- [16] M. R. L. Perez, B. Gerardo, and R. Medina, "Modified sha256 for securing online transactions based on blockchain mechanism," in *2018 IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and*

- Management (HNICEM)*, 2018, pp. 1–5.
- [17] H.-J. Kang and Y.-Z. Li, "Design and implementation of hash function scheme targeted at short message processing," *Computer (Long. Beach. Calif.)*, vol. 121672, p. 7, 2022.
- [18] A. G. Bluman, *Elementary statistics: A step by step approach*. McGraw-Hill Higher Education New York, NY, 2009.

### Biography of all authors

Picture	Biography	Authorship contribution
	<b>Ts. Abdullah Sani Abd Rahman</b> obtained his first degree in Informatique majoring in Industrial Systems from the University of La Rochelle, France in 1995. He received a master's degree from Universiti Putra Malaysia in Computer Science, with specialization in Distributed Computing. Currently, he is a lecturer at the Universiti Teknologi PETRONAS, Malaysia and a member of the Institute of Autonomous System at the same university. His research interests are cybersecurity, data analytics and machine learning. He is also a registered Professional Technologist. He can be contacted at email: sani.arahman@utp.edu.my.	Drafting and final checking the article
	<b>Ms Samsiah Ahmad</b> obtained her first degree in Data Communication and Networking from the University Teknologi MARA, Malaysia in 2005. She is received a master's degree from Universiti Teknologi Malaysia in Computer Science, with specialization in Information Security. Currently, she is a lecturer at the Universiti Teknologi MARA, Malaysia. Her research interests are cybersecurity, big data analytics and machine learning. She is also Certified Computer Forensic Investigator. She can be contacted at email: samsi260@uitm.edu.my	Literature review and analysis