International Journal of Psychosocial Rehabilitation, Vol. 23, Issue 04, 2019
ISSN: 1475-7192

A Conceptual Diagram for Secure Virtual Office Services

Nor Azlina Abd Rahman, Daniel Mago Vistro, Tee Jia Le and
Cheok Jia Fuei

Abstract--- *A virtual office is a business platform exists in cyberspace. A virtual office setup allows business owners and employees to work from any location by using technology such as laptop computers and cell phones with internet access. A virtual office can provide significant savings and flexibility compared to renting a traditional office space. This system enables the employer to monitor the employees remotely. Meetings can be conducted via teleconferencing and video conferencing, and documents can be transmitted electronically. Any file transferred will be encrypted to ensure the confidentiality of the data. Integrity check will be done by the system during downloading or receiving the files. The USB ports will be protected to ensure no files can be transferred to the external drive. Digital invoice will be generated instead of manual invoice that need to use digital signature to ensure non-repudiation. This digital invoice will be more efficient to track any transaction history and at the same time will make stock monitoring will be more efficient as any invoice issued the product, stock will automatically deducted from central database. The user can set the system to notify the user when the available stock less than the amount set by the users. This research paper analyzing the user requirements towards the need of virtual office and conceptual diagram proposed as per overall virtual office services that required by the target users which are small and medium enterprise companies.*

Keywords--- *Virtual Office System, SME, Integrity Check, Secure Deletion, USB Block, Remote Monitoring.*

I. INTRODUCTION

Virtual office, a common business platform acquires by organizations to enhance performance of employees in achieve business objectives. In addition, virtual office provides convenient to employees and employers to complete their tasks at anywhere and anytime with the usage of computing platform such as mobile, computers, web applications and operating systems.

Moreover, virtual office assist organizations to save expenses on expanding working environments with the increase numbers of employees as all the tasks able to present virtually such as video conferencing and real-time online sharing documents. As all the tasks transmission pass through internet access, it is crucial to ensure security on the transmission method of the confidential documents and data. File Transmission Protocol (FTP) shall

Nor Azlina Abd Rahman, Asia Pacific University of Technology & Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia. E-mail: nor_azlina@apu.edu.my
Daniel Mago Vistro, Asia Pacific University of Technology & Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia. E-mail: daniel.mago@apu.edu.my
Tee Jia Le, Asia Pacific University of Technology & Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia.
Cheok Jia Fuei, Asia Pacific University of Technology & Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia.

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019

encrypted with proposed algorithm to prevent accessible from unauthorized personnel. Meanwhile, transmission of data through external hard drive or Universal Serial Bus (USB) shall prohibited to ensure internal security of organization. In addition, virtual office application shall generate digital invoice instead of physical invoice for employees to issue towards clients. All the transmission of digital invoice will be recorded to ease tracking process for person in charge whenever there is need to doing so. The aforementioned digital invoice also assists stock monitoring to keep inventory amounts up-to-date with database.

As organizations continue to expand, probability for workplace issue escalate proportionally which eventually causes numerous potential levels of impact related with employee, sensitive business data confidentiality and inefficiency of stock processing function. The aforementioned impact often resulting in performance distortion issue of employee which eventually disrupt business benefits of organization.

First of all, there are circumstances employer facing difficulties in constantly monitoring performance of staffs with current working environment as employer might need to attend meeting and business trip and not able to constantly stay in office. In addition, it is difficult for small-medium enterprise employer to keep with employees' progress individually as this will take enormous amount of times which violated definition of efficiency [1]. Besides, meeting schedule might occur delay due to unavoidable reasons which affect employee apprise progress towards employer.

Meanwhile, organizations facing numerous of challenges in protecting data confidentiality due to rapid development of information technology such as cybercrime and low IT security awareness of employee. The aforementioned challenges put organization into enormous hazard by compromising the entire business operation workflow in case attacker manage to breach into security of business infrastructure and facilities which eventually causes data leakage and exposed business assets. In addition, low security awareness of employee often utilizes by attackers with numerous type of cybercrime attack method such as malicious software and spoofed application [2].

There are several methods for malware attack to invade computing machine of victims. Malicious software often spread via file transmission among the employees' computing machine with the usage of email or file sharing in workgroup. Attacker often using phishing attack by imitate as authorized email sender towards victim with email that consist infected email attachments [3]. In addition, malicious software often spread to devices and computing machine within same internal network.

One of the famous social engineering attacks is spoofed application function by tricking victim's access into fake application purpose to fraud victim in providing attackers with confidential business data and financial information of organization [14]. The aforementioned issue also known as website defacement attack which purpose to compromise and vandalize application by replacing original information and content into counterfeit information [4]. The aforementioned attack able to achieve with the utilization of SQL injections by exploiting vulnerabilities of the application database currently in use by organization with SQL queries to dump and modify information stored.

Inventory inefficiency also one of the existing problems of organization which will increase time consumption for employee in managing amount of inventory [5]. This is due to the acquisition of outdated inventory management system where components not working in sync by the time client purchase certain amount of products. In addition,

poor categorization management of products also one of the crucial factors which causing inventory inefficiency. An efficient inventory system shall update amount of products automatically once every transaction made and able to customize product sorting according to preference and requirement of users.

II. REQUIREMENTS ANALYSIS

Questionnaires used to gather the requirements of the users for secure virtual office system. The questionnaire will be distributed online so that participants can participate in the questionnaire with their own devices at any time.

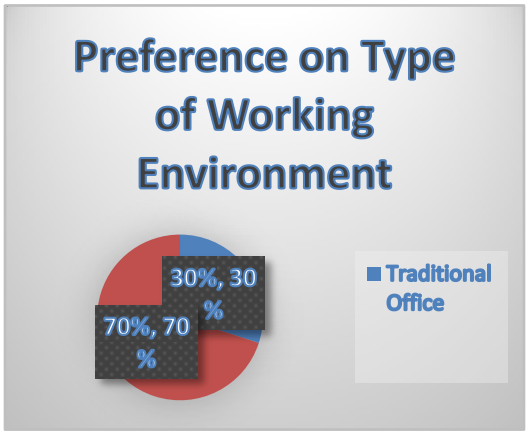

Figure 1: Acceptance to Work Remotely

According to data gained from pie chart in figure 1, 70% of respondents prefer virtual remote website application as working environment and meanwhile, there are 30% of respondents prefer traditional office as working environment. This shows an overwhelming majority of participants agree that employers should allow employees to work remotely. Thus, further validating the need for an online Virtual Office.

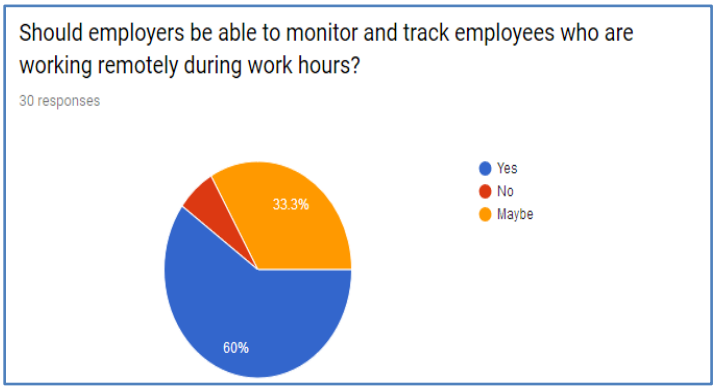

Figure 2: Employee Monitoring Remotely

Based on the pie chart in figure 2, 60% of participants agree that employers should be able to track employees working remotely, with less than 10% participants disagreeing. This is a subjective topic due to personal privacy and accountability reasons, hence 1/3 of participants were unsure whether to agree or disagree Working remotely will make the employee feel more convenient while the employer still can monitor the employee remotely. Hence this could increase the productivity of the employee and also the employer.

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019

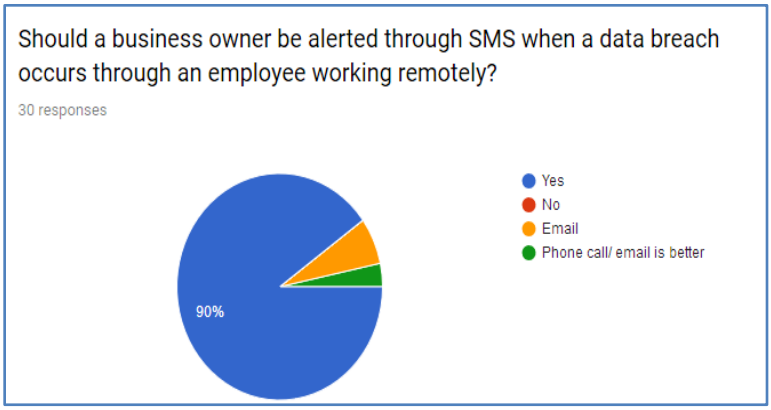

Figure 3: Notification of Data Breach

Figure 3 shows that 90% of the participants agree that business owners should be able to receive SMS alerts or notification if there is anything detected by the system such as malware, data breach or any other suspicious activities that could give impact to the business.

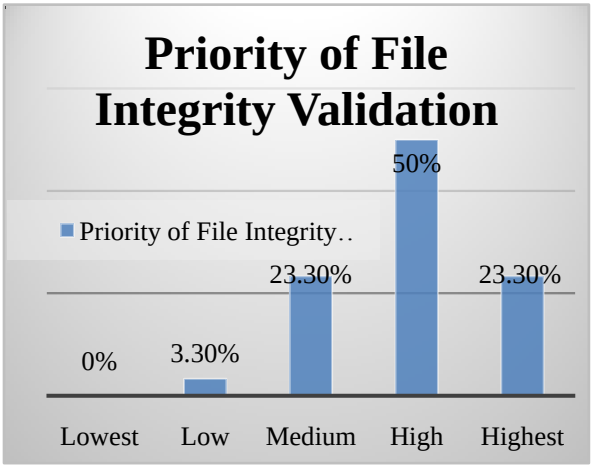

Figure 4: File integrity Validation

According to bar chart in figure 4, 50% of respondents rate the priority of file integrity validation with high while there is only 3% of respondents rate the priority of file integrity validation with low. This means that most people nowadays are aware on file security where only authorized party that allow to do any modification to the files. Integrity check for the file is important to ensure the originality of the file.

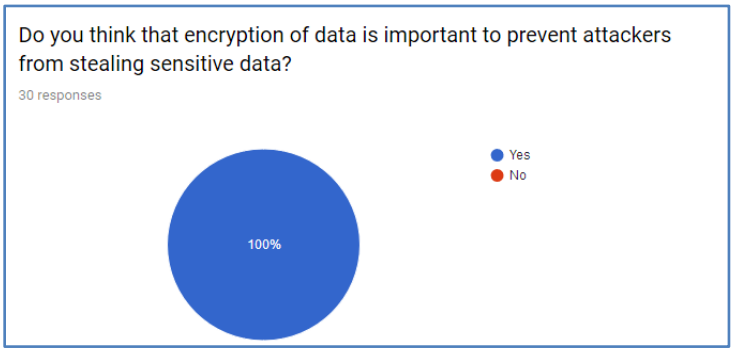

Figure 5: The Importance of Data Encryption

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019

Pie chart in figure 5 shows that 100% of the participants agree that encryption of data is a priority in order to prevent data theft. This shows that participants prefer their data to be encrypted and stored securely.

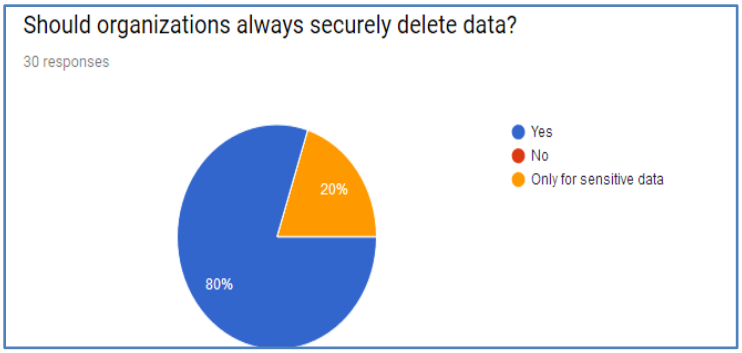

Figure 6: Acceptance of Secure Deletion of the Data

According to the analysis from the data shown in the figure 6 pie chart, 80% of participants agree that businesses should always securely delete data while 20% only think that secure deletion of data should only happen for sensitive data. This may be due to the complexity and speed of securely deleting data. Nevertheless, all of the participants agree that sensitive data should be deleted.

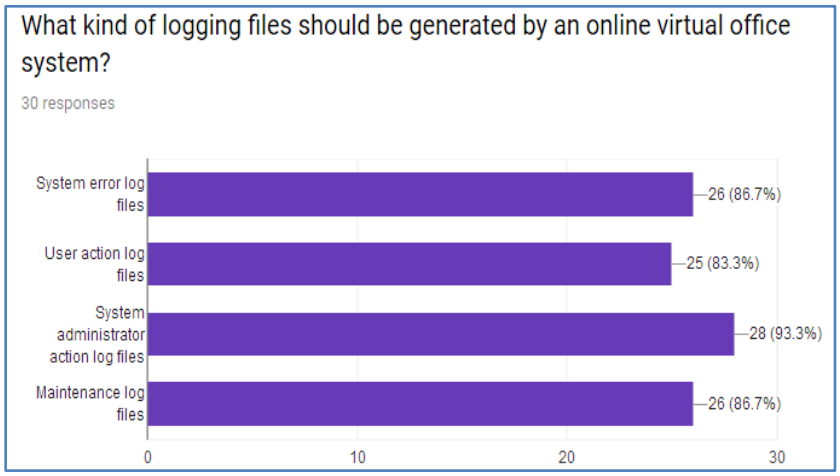

Figure 7: Types of Log File to Generate

According to the graph in figure 7, almost every participant believe that an online virtual office system should have logging for the above tasks. This is to ensure that all the users' activities are being keep track so that any circumstances can be traced back for recovery or any other security action purposes.

As per overall analysis based on the data collected, a vast majority of participants do not mind to work remotely, thus having a need for a virtual office system. According to the data collected, location tracking while working remotely is just slightly acceptable, with many participants opting to share only their location to their employers. From the data gathered, the researchers also can see that there is a demand for video conferencing and automated secure deletion of the files. Since participants value their privacy and prefer to encrypt their network traffic, the Secure Smart Virtual Online Office will also use network traffic encryption to prevent data theft. In conclusion, the original features that were planned by the researchers will be retained after analyzing the data.

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019

III. RESULTS AND DISCUSSION

This section discussing on the conceptual diagram of Secure Virtual office system based on analysis on users' requirements towards the system.

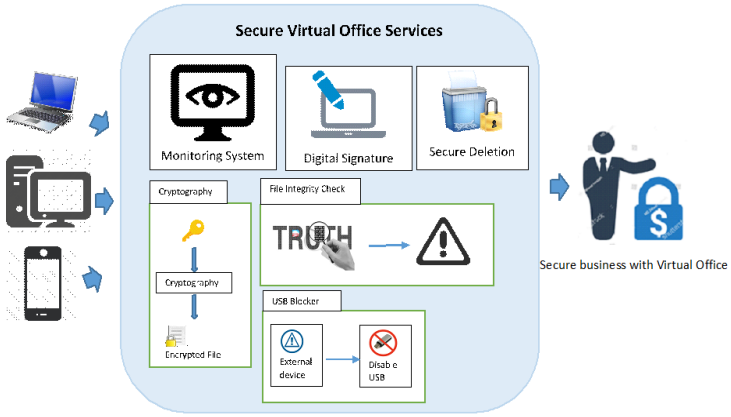

Figure 8: Conceptual Diagram of Secure Virtual Office Services

The components of the conceptual diagram of the system are:

- ***Accessing Devices***

The system can be accessed through laptop, desktop and also mobile phone. The system is web application that can access from any devices as the system developed to make it responsive to any type of devices.

- ***Secure Virtual Office Services***

To ensure the security of the system, several services provided which are:

- Remotely monitor the staffs and identify their exact location.
- One of the ways to track location is by using the Global Positioning System (GPS). GPS is currently one of the most widely used geo-location technology to identify location, pinpoint an object or a person's location on Earth [6]. As GPS technology become increasingly common, almost every smartphone nowadays has a GPS receiver installed within it. As quoted by Djuknic & Richton in 2001, "Assisted-GPS technology offers superior accuracy, availability, and coverage at a reasonable cost". Services which are given the permission to record location histories are able to gather the data and places where someone has been to [15].
- Other technologies such as WiFi positioning system also exists as a way for determining location. While the GPS is a good way to obtain location data outdoors, it works poorly for indoor environments due to its reliance of satellites visibility [7]. A research done by Woo, et al. in 2010 has found that using WiFi-based indoor positioning systems were accurate within a 5m variance, proving the utility of WiFi-based positioning systems.
- Companies which collects and aggregates data using technologies mentioned above such as Google are able to create products such as Google Maps which has massively improved quality of life for people all over the world. As pointed out by Tahir, 2015, with the help of Google's databases, a user is able to track his location in real time.

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019

- ***Digital Signature***

As Virtual office system is going to use all e-documents hence the use of digital signature will enhance the security of the system. Digital signature is implemented to the invoice that issued to the customer to guarantees that the contents of the invoices have not been altered in transit. Besides that the use of digital signature is also to guarantee that the individual that sending the invoice really is who he or she claims to be.

- ***Secure Deletion***

Being able to delete data is a very common function in every operating system, however the delete function in most operating system does not really delete data from the hard disk, it merely removes the visible link to the data, and marks the storage block as free on the hard disk. Expensive forensic techniques such as magnetic force microcopy etc. are even able to reconstruct overwritten data from hard disks [8].

Many methods have been invented to address this issue at the lowest layer possible – the physical layer which depending on the medium may be flash memory or a magnetic drive [9]. Proposed a method for secure deletion for magnetic hard disks using Run-Length Limited (RLL), Modified Frequency Modulation (MFM) or Partial-Response Maximum-Likelihood (PRML) encoding methods. The basic concept of his method is by overwriting each region of the disk up to 35 times with multiple patterns to securely delete data.

However, data encoding techniques have advanced a lot since Gutmann's paper was published, Gutmann himself has stated that his method is no longer needed as a few passes of writing random data to modern drives is more than sufficient [9]. For flash memory such as the consumer NAND flash memory, data can only be accessed by blocks or pages, added on by the fact that microcontrollers which use technologies such as wear leveling can make secure deletion hard [10]. Thus, proposed a method that is by encrypting the data with a key then overwriting the key with random data multiple times which should result in the effect of a secure deletion [11].

- ***Cryptography***

According to research and analysis on AES, DES and RSA encryption algorithms conducted, the researchers conduct comparison among three aforementioned encryption algorithms based on the performance and security level [12]. Conclude that RSA is the most secure encryption algorithm in terms of decryption and encryption time comparing with AES and DES. According to experimental results, encryption and decryption using RSA require more time consumption which ensure the performance of RSA in securing data [16].

Based on the findings proposed, RSA encryption which is the most popular asymmetric encryption systems using to date function by using public key and private key as authentication method. RSA consist three levels which are RC4, RC5 and RC6. RC4 is a variable key size stream cipher based on the use of random arrangement while RC5 emphasize on parameterized algorithm with a variable block. RC6 is an evolution of RC5which including feature of multiplication of integer for 4 bit working registers which make it so secure in terms of data encryption. Thus, researcher shall acquire RSA as encryption algorithm for the data transferred in proposed system to ensure data integrity and confidentiality [12] [16].

- ***File Integrity Check***

The researchers propose system, Tripwire as file system integrity checker which facilitate process in monitoring a set of files and directories for UNIX system administrator in case unauthorized modifications occur. The mechanism for the proposed system work by comparing unique identifier of file system with duplicated version of file system. In case there is any unmatched identifier, Tripwire will detect the changes and thus able to ensure file integrity. Meanwhile, signature model acquired by Tripwire including MD5, MD4 and MD2 [13].

Tripwire system consist vulnerability and weakness which might interfere user experience. Tripwire using an unencrypted database which is readable in case anyone manage to access to the internal system. In order to secure the database, the system shall acquire tamper-proof database on a write-protect disk which can only access in reading mode. Besides, the acquisition of MD5 as hashing function for signature model in Tripwire consist vulnerability in collision and able to decrypt easily with current existing decryption technology such as Cain & Abel. Thus, Tripwire shall acquire SHA-256 as replacement hash function value instead of MD5 as SHA-256 consist larger bit size which make it less susceptible to brute force attacks [13].

- ***USB Blocker***

Virtual office system able to detect any external drive that plug in to the system and block the port. Blocking any external drive that detected at the workstation is to prevent the leakage of private and confidential data.

IV. CONCLUSIONS

In conclusion, a secure platform for employees to perform their task is very much needed. This system will solve the needs by combining security, ease of use, and custom business requirements together into one.

Tasks such as secure deletion of data will be performed automatically when users perform a delete operation on data that is stored within the database. This way, the user experience is not impacted and data is securely deleted from the system and hard disks. This will also ensure that attackers are unable to recover deleted information from the hard disks.

Furthermore, by implementing network traffic encryption on the server, users of the system can just connect to the system without worrying data interception from potential attackers on the network. Security will be kept in mind while developing the system to make it hard for potential attackers to deface the system and steal data.

Through the research and data gathering, the researcher will have adequate data and information that will aid them in developing the system. While developing the system, security will be the one of the highest priority as it is extremely important for a business platform to be secure to prevent financial damages and loss.

ACKNOWLEDGMENTS

The authors wish to express gratitude to the management of Asia Pacific University for their support in this conference.

REFERENCES

[1] Pirraglia, W., 2019. Organizational Problems in the Workplace. Retrieved Mar 25, 2019, from http://smallbusiness.chron.com/organizational-problems-workplace-12570.html
[2] Hughes, C., 2017. 3 challenges to securing business data. Retrieved Mar 26, 2019, from https://www.csoonline.com/article/3187305/data-breach/article.html
[3] Symantec, 2019. How to safely and securely use USB memory sticks. Retrieved Mar 26, 2018 fromhttps://us.norton.com/internetsecurity-emerging-threats-how-to-safely-and-securely-use-usb-memory-sticks.html
[4] Trend Micro Forward-Looking Threat Research Team, 2018. Understanding Motivations and Methods of Web Defacement. Retrieved Mar 25, 2019.
[5] FullQuota Editor, 2014. 3 Keys To Eliminating Common Warehouse Inventory Management Inefficiencies. Retrieved Mar 27, 2019 from https://www.bspny.com/blog/3-keys-to-eliminating-common-warehouse-inventory-management-inefficiencies
[6] Koshima, H. & Hoshen, J., 2000. Personal Locator Service Emerge. *IEEE Spectrum*, Issue Feb. 2000, pp. 41-48.
[7] Lee, Y. W., Suh, Y. & Shibasaki, R., 2008. A GIS-based simulation to predict GPS availability. *KSCE Journal of Civil Engineering*, 12(6), pp. 401-408.
[8] Peterson, Z. N. J. et al., 2005. Secure Deletion for a Versioning File System. *s.l., USENIX Association.*
[9] Gutmann, P., n.d, 1996. Secure Deletion of Data from Magnetic and Solid-State Memory. Retrieved Mar 27, 2019 fromhttps://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html.
[10] Lee, B., Son, K., Won, D. & Kim, S., 2011 . Secure Data Deletion for USB Flash Memory. *Journal of Information Science and Engineering*, pp. 933-952.
[11] Heo, J. et al., 2008. *Secure Deletion for NAND Flash File System.* Fortaleza, Ceara, Brazil, ACM.
[12] Mahajan, D. P. & Sachdeva, A., 2013. A Study of Encryption Algorithms AES, DES and RSA for Security. *Global Journal of Computer Science and Technology Network, Web & Security* , 13(15), p. 15.
[13] Kim, G. H. & Spafford, E. H., 1994. *The Design and Implementation of Tripwire: A File System Integrity Checker*. West Lafayette, COAST Laboratory Department of Computer Sciences .
[14] Akamai Technologies, Inc, 2015. *Strategies for Cyber-Attack Protection: Managed Web Security Services.* Retrieved Mar 4, 2019.
[15] Tahir, M. F., 2015. Global Positioning System (GPS) Based Location Finder on Android, s.l.: Blekinge Institute of Technology.
[16] Singh, S. P. & Maini, R., 2011. Comparison of Data Encryption Algorithms. *International Journal of Computer Science and Communication* , 2(1), pp. 125-127.
[17] P. Mary Jeyanthi, Santosh Shrivastava Kumar "The Determinant Parameters of Knowledge Transfer among Academicians in Colleges of Chennai Region", *Theoretical Economics Letters,* 2019, 9, 752-760.
[18] P. Mary Jeyanthi, "An Empirical Study of Fraudulent and Bankruptcy in Indian Banking Sectors", *The Empirical Economics Letters,* Vol.18; No. 3, March 2019, ISSN: 1681-8997, which is in C category of ABDC List. http://www.eel.my100megs.com/volume-18-number-3.htm
[19] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Hybrid Metaheuristic techniques", *International Journal of Business Intelligence Research,* - Volume 5, Issue 1, April-2014.
[20] P. Mary Jeyanthi, "INDUSTRY 4.O: The combination of the Internet of Things (IoT)and the Internet of People (IoP)", *Journal of Contemporary Research in Management,* Vol.13; No. 4 Oct-Dec, 2018, ISSN: 0973-9785.
[21] P. Mary Jeyanthi, "The transformation of Social media information systems leads to Global business: An Empirical Survey", *International Journal of Technology and Science (IJTS),* issue 3, volume 5, ISSN Online: 2350-1111 (Online). URL: http://www.i3cpublications.org/M-IJTS-061801.pdf
[22] P. Mary Jeyanthi," An Empirical Study of Fraud Control Techniques using Business Intelligence in Financial Institutions", *Vivekananda Journal of Research* Vol. 7, Special Issue 1, May 2018, ISSN 2319-8702(Print), ISSN 2456-7574(Online). URL: http://vips.edu/wp-content/uploads/2016/09/Special-Issue-VJR-conference-2018.pdf Page no: 159-164.
[23] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Artificial bear Optimization Approach", *International Journal of Scientific & Engineering Research,* Volume 4, Issue 8, August-2013. URL: https://www.ijser.org/onlineResearchPaperViewer.aspx?Business-Intelligence-Artificial-Bear-Optimization-Ap-proach.pdf
[24] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Optimization techniques for Decision Making", *International Journal of Engineering Research and Technology,* Volume 2, Issue 8, August-2013.

[25] Mary Jeyanthi, S and Karnan, M.: "A New Implementation of Mathematical Models with metaheuristic Algorithms for Business Intelligence", *International Journal of Advanced Research in Computer and Communication Engineering*, Volume 3, Issue 3, March-2014.
[26] Dr. Mary Jeyanthi: "Partial Image Retrieval Systems in Luminance and Color Invariants: An Empirical Study", International Journal of Web Technology (ISSN: 2278-2389) – Volume-4, Issue-2. URL: http://www.hindex.org/2015/p1258.pdf
[27] Dr. Mary Jeyanthi: "CipherText Policy attribute-based Encryption for Patients Health Information in Cloud Platform", *Journal of Information Science and Engineering* (ISSN: 1016-2364)
[28] Mary Jeyanthi, P, Adarsh Sharma, Purva Verma: "Sustainability of the business and employment generation in the field of UPVC widows" (ICSMS2019).
[29] Mary Jeyanthi, P: "An Empirical Survey of Sustainability in Social Media and Information Systems across emerging countries", *International Conference on Sustainability Management and Strategy"* (ICSMS2018).
[30] Mary Jeyanthi, P: "Agile Analytics in Business Decision Making: An Empirical Study", *International Conference on Business Management and Information Systems"* (ICBMIS2015).
[31] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence – soft computing Techniques", *International Conference on Mathematics in Engineering & Business Management* (ICMEB 2012).
[32] Mary Jeyanthi, S and Karnan, M.: "A Comparative Study of Genetic algorithm and Artificial Bear Optimization algorithm in Business Intelligence", *International Conference on Mathematics in Engineering & Business Management* (ICMEB 2012).
[33] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Data Mining and Optimization for Decision Making ", 2011 *IEEE International Conference on Computational Intelligence and Computing Research* (2011 IEEE ICCIC).
[34] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Data Mining and Decision making to overcome the Financial Risk", 2011 *IEEE International Conference on Computational Intelligence and Computing Research* (2011 IEEE ICCIC).
[35] Dr. Mary Jeyanthi, S: "Pervasive Computing in Business Intelligence", *State level seminar on Computing and Communication Technologies.* (SCCT-2015)
[36] Dr.P.Mary Jeyanthi, "Artificial Bear Optimization (ABO) – A new approach of Metaheuristic algorithm for Business Intelligence", ISBN no: 978-93-87862-65-4, *Bonfring Publication.* Issue Date: 01-Apr-2019
[37] Dr.P.Mary Jeyanthi , "Customer Value Management (CVM) – Thinking Inside the box" – ISBN : 978-93-87862-94-4, *Bonfring Publication*, Issue Date: 16-Oct-2019.
[38] Jeyanthi, P. M., & Shrivastava, S. K. (2019). The Determinant Parameters of Knowledge Transfer among Academicians in Colleges of Chennai Region. *Theoretical Economics Letters*, 9(4), 752-760.