ISSN: 2522-3429 (Print)
ISSN 2616-6003 (Online)

International Journal For Electronic Crime Investigation (IJECI)

Vol. 3 Issue: 1
ISSUE: Jan. - Mar. 2019

Email ID: ijeci@lgu.edu.pk

Digital Forensics Research and Services Center
Lahore Garrison University Lahore, Pakistan.

LGU International Journal for Electronic Crime Investigation
Volume 3(1) January-March (2019)

Suleman et al LGURJCSIT 2019

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 3 Issue 1, January - March 2019

An Investigation of Data Security Issues and Challenges in Cloud Computing

Muhammad Taseer Suleman
Department of Computer Science, Lahore Garrison University, Lahore, Pakistan
taseersuleman@lgu.edu.pk

Abstract:
Cloud computing has emerged to be an evolving paradigm, which is extensively used in most of the business process for data storage and keeping records. Three major problems were identified which are data confidentiality, data trust and data security which Pakistani companies are facing while using cloud computing. The Primary data was collected through questionnaire from 22 companies. The problem is solved by using survey results analysis. Survey was conducted with the help of a questionnaire, which was extracted, from three relevant studies but in different context. The result findings indicates that, in order to, keep data confidentiality the best solution is using advanced encryption methodologies to maintain data confidentiality between service providers. Moreover, to fix data trust issues, using SSO, LDAP, MS Windows authentication can ensure data is safe. In the last, findings indicate to maintain data security using strong passwords and two factor authentications is the best solution. The study is beneficial for all those companies which are offering cloud-based services, and which are using cloud-based services in Pakistan.

Keywords: Cloud computing, data security, data trust, data confidentiality, cloud computing in Lahore.

1. Introduction

Cloud computing is a service which is offered by latest information technology to its users these days. Due to its flexibility towards sharing a bulk of information without storing it on any physical storage device, it has gathered recognition in the global platform. Despite being such an innovative invention, it is still prone to numerous threats and issue. This research makes a vivid demonstration of

this technology and leading threats faced by nations due to the advent of this technology. This chapter is inclusive of various methodologies which are effective in lowering the limitation, therefore, increasing the effectiveness of this innovation. These services are provided on the rental bases over the websites and it is being used by many organizations as well. This has several benefits such as low cost, great infrastructure and IT flexibility. Generally, the cloud computing service provides the best virtual space in the system for the user to deploy their private applications to run the operations. Apart from its major benefits, there are few risks as well. These are very serious threats for the current information technology and cloud engineers as well. The basic threat and risk related to cloud computing is the security of the system and data.

In the past, to denote the cyberspace and internet, the clouds were used in the abstract shapes. On the other side as the technology changes the cloud computing has also changed itself. There is a continuous improvement can be seen in the infra structural changes of the electronic services. Moreover, the cloud computing system offers and provides its users low cost services. Besides, for software and hardware, it gives alternatives [1, 2]. Besides, cloud computing provides various ways to deal with good quality services in the organization. It further improves the performance of the applications in the system as well [3]. Amazon,

Apple's `iCloud', Microsoft, Google, and Dropox are the recognized service providers in cloud computing and they also provide best services to their users all around the world. It has introduced new dimensions in the IT field in which users are able to save their data anywhere whenever they want. Besides, by using cloud computing, users can edit and delete their personal data as well. Due to the accessibility of internet, users run their applications easily [4]. As depend on customer requirement, cloud computing can offer viable solutions which are low in cost and efficient in response. On the basis of customer requirement, cloud computing can not only provide its's customers facility to design the architecture, products and data security and confidentiality.

As soon as the customer choose to store data on cloud server it is stored in a cloud-based server which can access virtually [5]. This service can be accessed by the business keepers, and owners. It is also accessed by one whoever assign to that role that can access their own company's cloud computing provider platform. This makes clear that for a user to store or process a piece of data in cloud, he/she needs to transmit the data to a remote server over a channel [6]. This data processing and storage needs to be done with utmost care to avoid data breaches.

Even though the current trend of cloud computing (CC) allows companies to reduce business cost by not developing their own infrastructure and use cloud platforms to store the data. However, the data security and confidentiality remains a big concern for the businesses. Furthermore, businesses are reluctant to store or hand over data to other third parties due to lack of trust, and smoothness of transaction in terms of accessing the data [7].

The rest of the paper is divided as follows: The next section include a case study that support the problem of this research. Section III includes the study related to the issue in cloud computing. Section IV concludes our research work.

2. Background of the Study

This study is based on the alarming issues that are arising due to the adoption of cloud technology in the province of Pakistan. As stated by [8], in context of Pakistan, which is a growing nation, several enterprises are rising and hence is holding a vast market for implementation of information technology. With the gradual development process observed from a context of this country, it can be anticipated that the future economy of Pakistan will be entirely dependent on this evolving information technology. An inclination is observed from the enterprises dwelling in this economy towards the adoption of cloud technology. However, it is leading to issues like leakage of confidential data, security threats and issues. These issues are severely impacting the growth of a nation and it is evident from the statistical data which reveals a growth of 10.8% of unauthorized access [9]. Proper identification of reasons behind this evolving issue is required for preventing these issues and illicit activities. This study is also inclusive of identification of alternative ways in order to minimize these issues. Situational analysis over the prevailing and concurrent situation is extremely important for understanding the intensity of these data security issues over the residents, enterprises and diverse business sectors in Pakistan.

2.1. Pakistan Stock Exchange: A Case Study

In accordance with a recent issue of data security observed in the PSX, that stands for Pakistan Stock Exchange and this issue was related to leakage of trading data. Furthermore, issues regarding accessing of unauthentic and other data by senior staffs are increasing steeply. As per [10], a majority of allegations are over unauthorized access to UNIC, that stands for Individual-Unique Identification Numbers in context of share markets and stock exchanges. This number is provided to every investor and store vital information regarding both tangible and intangible assets belonging to an investor, as well as data for accessing those assets. However, these confidential numbers are getting hacked after implementation of cloud technology and that is significantly influencing the investors and brokers of this sector and leading to the downfall of an economy of an entire nation. One of the prime reason for an aggressive inclination of emerging as well as prevailing enterprises is cross-cutting of the finances required for installations of physical storage devices and increases the speed of business operations effectively [11].

The current study focuses on a majority of enterprises which are ignoring the causes security issues associated with incorporation of this technology, hence cannot identify the

measures of preventing these issues. With respect to a current statistical survey, it is observed that 72% of the entire data loss is due to leakage, 56% of entire data security threat is associated with issues over unauthorized and illicit access. Furthermore, 52% of cybercrime is due to the introduction of malware over data residing in cloud technology. Recent sources revealed that SECP that stands for Securities (and) Exchange Commission-Pakistan has made a step towards investigating the data leakage issues in diverse sectors of Pakistan [12]. Data security issues in trading sectors of Pakistan have also resulted in influencing neighboring countries like China that deals with the nation over trade and commerce [13].

3. Major issues in Cloud Computing

We discuss the cloud issue in terms of Data security, Data trust and Data confidentiality.

3.1. Cloud Computing and Data Security Issues

Although cloud computing has aberrant benefits and facilities, however, it is prone to significant issues on security. With respect to figures from Cloud-Security Alliance (CSA), over 70% of total world's business functions and operates entirely dependent on cloud systems [14]. From the reports of Cloud-security Spotlight, more than 90% of total population is moderately concerned regarding t This section represents top security issues that are prevailing in society due to advent of this innovation:

3.1.1. Breaches in D ata:

As illustrated by [15], a phenomenon is observed in this setting termed as "Man In Cloud-Attack". It has reported that approximately 50% of various IT professional are claiming cloud for data leakage. The data, which are essential to industries, are likely to get leaked due to the presence of advanced hacking methodologies.

3.1.2 Hacking of APIs and Interfaces:

A modification in cloud technology is observed which enables every cloud service to be associated with inbuilt APIs. Several IT teams manage these APIs and interaction is conducted over these cloud services [16]. The interaction mainly includes management, provisioning etc. However, these APIs don't always prove effective in providing security due to weak structures and therefore, can easily get hacked.

3.1.3 Broken Authentication and Credentials:

This promotes the breaches and hacking of data. This is mainly a consequence of inputting easy passwords, poor keys towards the management of certificates. According to [15], lack of proper management systems in extracting authentic information can lead to these problems.

3.1.4 Exploited Vulnerabilities of Systems:

Cloud computing is an association of a number of devices that are responsible for connecting every end user. This enables every user to get information regarding existing vulnerabilities of the system [17]. This information is strong to break the security system of an organization and hack essential data.

3.1.5 Ahijacking of Accounts:

The feature of cloud computing enables sharing of information among the systems which are connected in a network. This connection majority of times promote to eavesdropping of authentic information among an unwanted crowd. This mainly leads to a hijacking of accounts present in a network.
he security issues emerging due to cloud computing.

3.1.6 Cloud Security Controls

In order to combat the prevalent problems, there is an utmost requirement of discovering some modification which enhances the security systems of the cloud networks and nullifies the issues [12]. A cloud system becomes effective, if and only if, its data are secure. The very first step of securing data in cloud network is safeguarding the prevailing weaknesses in the network, here these controls play an important role. There are five categories of controls systems which are used in place of weaknesses for enhancing security:

3.2.1 Deterrent-Controls:

These controls are fabricated for reducing the

attacks which are frequent in any cloud systems [19]. It can be compared to a fence, which protects a house at primary level. It is the fire line of defence to attacks posted on cloud networks.

3.2.2 Preventive-Controls:

This system is a bit contrary to earlier control systems. It works prior to any potential attack and prevents it. It includes the building of strong authentication properties for the users of cloud that prevent access of unwanted users in the network.

3.2.3 Detective-Controls:

This system can be considered as a mix of two other system as it is comprised of both reacting and detecting element. As stated in [20], the detecting element detects the potentials, which indicate attacks, and if by chance any attack takes place, it reacts accordingly to stabilize the system.

3.2.4 Corrective-Controls:

These controls are designed for providing corrective controls over results of any incidents, such as acting or attack for restoring the neutrality of the system. Backups that are required for restoring a particular system is a relevant example of corrective control measures. Controls are shown in Fig 1.

Fig 1. Controls to make cloud secure

3.3 Data Trust Issue in Cloud

Despite the efficacy of cloud systems, there are numerous issues arising from trust management that is related to trusting of data that are available on a cloud network. As stated by [21], the term "trust" can be compared to a "fuzzy-concept", which has no existence on a global platform. However, it is responsible for the creation of alarming issues. In an environment oriented to a cloud, this trust is comprised of two specific aspects, one is a service provider and other is service requester [22]. More elaborately, Trust from service provider side is associated with factors, for instance, data availability, security, performance etc. There can be some weak links present in servers, which are targeted by people to get into the network.

3.3.1 Building a trustworthy ecosystem in cloud

As illustrated by [23], a creation of the trust is equivalently dependent upon both the service requester and provider. To achieve the equilibrium an organized and comprehensive strategy on the cloud must be designed which not only operates in a good manner but also balances this trust in future. This requires setting up of separate and confidential surveillance department in any sector, which would be entirely dedicated to trust management in a cloud-ecosystem. This entire process can be divided into a set of steps;

3.3.2 Privileged-Access

Whenever a piece of information travels to the service providers the users at end sides are required to have diverse levels of access. Specific access controllers and lack of having appropriate access controls can lead to leakage of data control the accesses. To avoid such situation, some concepts like "BYOD" were fabricated which operated on centralized access-management solution systems. These systems are quite cost-effective, manageable and accountable. These systems are abundantly available in markets, therefore, these systems should be installed in a system to get privileged and authentic access to users in a cloud network.

3.3.3 Appropriate handling of Data

This can be obtained when the provider and requester of cloud services are comprehensive

and aware the kind of data, which is accessed, processed and stored in a network. There must be proper segregation tools present in a network that would segregate information on levels of importance and relevance.

3.3.4 Implementation of Technology

Based on point of view on technological grounds, the providers of services are required to be consistent regarding compliance that can be achieved certification, controls and authentic virtual technological domains. Here, customers to evaluate the providers of cloud service can use infrastructure management.

3.4 Data-Confidentiality Issues in Cloud Computing

This section deals with data security at various levels, such as integrity, accessibility and confidentiality of data.

3.4.1 Data Security

According to [24], the structure of a particular system that is comprised of cloud computing is made of three different layers. These are platform, infrastructure and software layer. Among these, a software layer is generally associated with providing various interfaces to the users of CSP (cloud-service provider). Platform layer is oriented to nature of platform over which the application or software provided will run and infrastructure layer is related to providing resources for network, computing and storage on hardware devices. These infrastructures are provided by many virtual machines. When a data is transmitted, end-users generally use the infrastructure provided by these CSPs, therefore, CSPs know the kind of data, which are being transmitted by clients. Users using the cloud service are forced for using the interface which is exactly provided by the CSPs. Henceforth, CSPs are comprehensive towards the data used by clients. The interfaces provided by this CSPs are in a constant format while sending a particular data from one client to another, the user is forced to use that format only which is predefined by service providers. For this reason, service providers have open access to the data which is being transacted.

This feature of cloud computing is a boon and a ban at the same time. If the clients are unauthentic on the network the service provider can easily detect any discrepancy and identify the client. At the same time, if the CSP is not authentic enough, then it would lead to huge amount of information access by any authentic medium. In this technology, encapsulating data to maintain its confidentiality is difficult from the service providers. Apart from confidentiality of data, there is certain data security issue, such as controllability of access. This is associated with prioritization of access by using some selective methods. The client can select the person who will be able to access the provided data can control the access to any data. The integrity of data is related to the maintenance of data so that it is complete and not manipulated. Assured data integrity in cloud network is a big question since the data can be accessed by CSPs as well as some end-users; therefore, it is very difficult to determine whether any discrepancy took place in conveying information.

3.4.2 Appropriate Encryption

As mentioned by [25], data encapsulation can prove effective in maintaining data securely, there exist a number of advanced encryption methodologies that are termed as crypto shedding.

3.4.3 Attributes Based Encryption-Algorithm:

Here the encryption scheme is solely responsible for deciding the access strategy. In this strategy, the access becomes quite complex as the security system's difficulty increases.

Key Policy-ABE:

It is used for providing descriptions to private keys and various texts that are encrypted.

Fully Homographic-Encryption

It is a primitive cryptography methodology that offers various search functions optimum security and therefore enhances the efficiency related to search.

4. Conclusion and Future Work

This study aimed at investigating the issues faced by the Pakistani companies specifically located in Lahore which are offering cloud-based services and the companies which are using cloud computing services. First research question of the study was to find out the issues

faced by the Pakistani companies. After substantive literature review three issues identified which are data security, data confidentiality and data trust. To find the solutions of these issues second research question was formulated that how to fix these issues.

Findings of survey results indicates that for data trust problem the best solutions are using devices connected should be under control by CSP to maintain trust between cloud service providers and users and using SSO, LDAP, MS Windows authentication etc to ensure trust what on-premise authentication system compatible with cloud computing system can ne used.

Lastly, findings of survey results indicate that for data security problem the best solutions are using three phase encryptions with hardware acceleration and strong management system such as strong passwords and two factor authentications are most important to avoid data breach and loss.

5. References

[1] Feng, D. G., Zhang, M., Zhang, Y., & Xu, Z. (2011). Study on cloud computing security. Journal of software, 22(1), 71-83.

[2] Kandukuri, B. R., & Rakshit, A. (2009, September). Cloud security issues. In Services Computing, 2009. SCC'09. IEEE International Conference on (pp. 517-520). IEEE.

[3] Chen, Z. N., Chen, K., Jiang, J. L., Zhang, L. F., Wu, S., Qi, Z. W., ... & Sun, A. B. (2017). Evolution of Cloud Operating System: From Technology to Ecosystem. Journal of Computer Science and Technology, 32(2), 224-241.

[4] Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2008). A break in the clouds: towards a cloud definition. ACM SIGCOMM Computer Communication Review, 39(1), 50-55.

[5] Mollah, M. B., Islam, K. R., & Islam, S. S. (2012, April). Next generation of computing through cloud computing technology. In Electrical & Computer Engineering (CCECE), 2012 25th IEEE Canadian Conference on (pp. 1-6). IEEE.

[6] Jankoulova, I., & Daneva, M. (2012, May). Cloud computing security requirements: A systematic review. In Research Challenges in Information Science (RCIS), 2012 sixth international conference on (pp. 1-7). IEEE.

[7] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.

[8] Monteiro, A., Teixeira, C., & Pinto, J. S. (2017). Sky Computing: exploring the aggregated Cloud resources. Cluster Computing, 20(1), 621-631.

[9] Wang, L., Ranjan, R., Chen, J., & Benatallah, B. (Eds.). (2017). Cloud computing: methodology, systems, and applications. London: CRC Press.

[10] Joseph, R., & Brown, P. (2017). The Cloud Gets Personal: Perspectives on Cloud Computing for Personalized Medicine. International Journal of E-Health and Medical Communications (IJEHMC), 8(2), 1-17.

[11] Aikat, J., Akella, A., Chase, J. S., Juels, A., Reiter, M. K., Ristenpart, T., ... & Swift, M. (2017). Rethinking Security in the Era of Cloud Computing. IEEE Security & Privacy, 15(3), 60-69.

[12] Distefano, S., Merlino, G., & Puliafito, A. (2017). Device-centric sensing: an alternative to data-centric approaches. IEEE Systems Journal, 11(1), 231-241.

[13] BBC.COM (2015), Cloud Technology, Retrieved From: http://www.bbc.com/news/business-36151754 [Accessed on: 19 January, 2017]

[14] Aldossary, S., & Allen, W. (2016). Data security, privacy, availability and integrity in cloud computing: issues and current solutions. International Journal of Advanced Computer Science and Applications, 7(4), 485-498.

[15] Xia, Z., Wang, X., Sun, X., & Wang, Q. (2016). A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. IEEE Transactions on Parallel and Distributed Systems, 27(2), 340-352.

[16] Chang, V., Kuo, Y. H., & Ramachandran, M. (2016). Cloud computing adoption framework: A security framework for business clouds. Future Generation Computer Systems, 57, 24-41.

[17] Gai, K., Qiu, M., Tao, L., & Zhu, Y. (2016). Intrusion detection techniques for mobile cloud computing in heterogeneous 5G. Security and Communication Networks, 9(16), 3049-

3058.
[18] Samarati, P., di Vimercati, S. D. C., Murugesan, S., & Bojanova, I. (2016). Cloud security: Issues and concerns. Encyclopedia on Cloud Computing, 1-14
[19] Oliveira, D., Squicciarini, A., & Lin, D. (2016). Cloud Security Baselines. Cloud Computing Security: Foundations and Challenges, 56(18), 31.
[20] Zibouh, O., Dalli, A., & Drissi, H. (2016). CLOUD COMPUTING SECURITY THROUGH PARALLELIZING FULLY HOMOMORPHIC ENCRYPTION APPLIED TO MULTI-CLOUD APPROACH. Journal of Theoretical and Applied Information Technology, 87(2), 300.
[21] Chauhan, P., & Bansal, P. (2017). Emphasizing on Various Security Issues in Cloud Forensic Framework. Indian Journal of Science and Technology, 8(1).
[22] Sookhak, M., Yu, F. R., Khan, M. K., Xiang, Y., & Buyya, R. (2017). Attribute-based data access control in mobile cloud computing: Taxonomy and open issues. Future Generation Computer Systems, 72, 273-287.
[23] Mollah, M. B., Islam, K. R., & Islam, S. S. (2012, April). Next generation of computing through cloud computing technology. In Electrical & Computer Engineering (CCECE), 2012 25th IEEE Canadian Conference on (pp. 1-6). IEEE.
[24] Xia, Z., Wang, X., Sun, X., & Wang, Q. (2016). A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. IEEE Transactions on Parallel and Distributed Systems, 27(2), 340-352.
[25] Alizadeh, M., Abolfazli, S., Zamani, M., Baharun, S., & Sakurai, K. (2016). Authentication in mobile cloud computing: A survey. Journal of Network and Computer Applications, 61, 59-80.

Fatima et al LGURJCSIT 2019

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 3 Issue 1, January - March 2019

Handwriting Analysis from Individual Profiling to Forensic Questioned Document Examination

Fatima
Lahore Garrison University
Fatima.dfrsc@lgu.edu.pk

Abstract:
Handwriting Analysis is a scientific study that interprets human behaviour and personality from particularities in a given handwritten sample. Graphology is the scientific name for handwriting study and thus graphologists who study it. It is often mind or brain writing reflected by an individual with different writing features or elements placed on piece of paper. The writing elements considered for analysis are motion, hand pressure, shapes of the different characters and their spatial relationship among them. It is also practised as standard forensic process for the identification of person and authenticity of signature from written documents termed as questioned documents. These questioned documents may involve criminal or civil cases with forgery, fraudulent cheques, indentation, alteration, obliteration and erasures. Grapholgy is a manual process and to avoid cost and fatigue, automated forensic tools have been developed for handwritten documents as well as printed or scanned questioned documents. These forensic tools rely on standard protocols based on scientific methods. The results obtained from forensic Handwriting analysis and questioned document expert testimony are admissible in the court of law.

Keywords: Handwriting analysis, document examination

1. Introduction

We are living in an era where the inner peace and harmony is achieved by helping others for the personal enlightenment and self-awareness. Composed mind and body is a key unit to function smoothly towards the goals. A good mental wellbeing can be indicated by physical wellbeing but when speaking of a healthy individual, it is more than a healthy, active and diseases free body. Ones can mask his/her mental and emotional instabilities by a good and an artificial external personality to show inner balance. Doing so, they can protect their inner vulnerability by constructing a protective shield against any negative experience but lost the communication for their deeper needs and feelings. Apparently we cannot read minds but certain body movements can be observed such as body gesture and posture, tone of voice and manner of dressing can interpret the behaviour and inner psychological make-up. As the outer style often reflects the inner individual, we can reveal the true and real character behind the outer mask by thoughtful observation. Certain facial expression can interpret certain moods like a person on call can express all the conversation going on without telling verbally by facial expressions and body posture. Thus, thoughts and feelings can be demonstrated through expressive and silent body language. Similarly, handwriting too, is a silent and an expressive gesture of inner manner.

While writing, we are consciously attempting a massage for the reader. Beside the conscious information in the written words, the handwriting also gives information about how we feel when we write. During the process of writing, the arms, hands and fingers receive message/order from the mind through nervous system which together constitute the writing tool. This creative process of mind and nervous system, makes writing an expressive and representative gesture of mind behind the pen. Whereas the faces, finger prints, voices and body postures displays unique variety, so does the handwriting by characterizing the writer's

state of mind and mood changes. Despite of standard and model teaching of writing to form letters and words, no one can have writings exactly alike. As stated by an American statistician that the chance of two writing being identical is one in 68 trillion! The emotional factors and personal behaviour can also deviate the form of writing stroke and spacing. The handwriting grows and gets mature or degenerates along with the changes in personality or physical wellbeing such as age, health or tension. Such changes provides the visual history of life's emotional, mental and physical development (1, 4).

2. Graphology

The science of handwriting study did not exist for a century. With the passage of time, immense progress has been observed with a rough estimated practical success. This field was accepted by all relevant branches of the modern sciences making a combination of Art and Science. These modern sciences sets are of literature, psychology, mathematics, photography and microscopy, as well as chemistry to serve handwriting study. Various relevant procedures and tools have been introduced to this field that drawn the attention of skilled students (2, 4). The methodical interpretations of the handwriting study was first carried out by Camillo Baldi in 1622. His book entitled "Treated how, by a letter missive, one recognizes the writer's nature and qualities," was published as first known graphological paper. Abb Jean-Hippolyte Michon coined the word "graphology" by merging two Greek words graphein, to write and logos, a branch of scientific study in 1897. Thus graphology is the study of the writing based on the knowledge obtained from the growing body of an individual or the writer. Michon was the first to give the handwriting analysis a scientific bases (1, 14). Adding to his work, the handwriting study was divided into seven central basics including speed, form, pressure, continuity, order, dimension, and direction which later on will be discussed in detail (14).

Large set of people use the science of graphology as a means of discovering themselves and others, are called graphologists. They identify the overstatements/exaggerations in the writing formations which depict the similar pattern in the personality of the writer. Speaking of the traits, the graphologists practice to analyse the variation in the writing samples. An accurate and precise analysis of a handwriting sample can be performed by the interpreters with basic knowledge and good revealing skills. Different methods can be used in handwriting analysis as it is not an organised system like that of arithmetic. Practicing students should not be terrified with varying results just as of the medical and psychological fields get results.

Mind is a particular area in the study of handwriting as the psychotherapy represents the same problem. We can learn about ourselves by detailed study of our minds and bodies. To look for possible malice in body, medical sciences go for different blood tests and biopsies by analysing any useful and specific information. The mind initially motivates the writing and then it is generated in the central nervous system by the interaction of the nerve muscles. Thus study of writing has a diagnostic value in medical science to analyse the mind and body by providing the signs of physical illness, emotional changes and mental disorders caused in handwriting. Now handwriting tests are performed to distinguish between certain medical illnesses from shaking palsy and Parkinson's disease to those crippled with arthritis and grieving from high blood pressure. Other diseases that can be diagnosed by handwriting tests are tuberculosis, epilepsy, alcoholism and drug addiction that involves the loss of nerve control over fine muscular coordination resulting a tremor in the writing strokes, pressure and loss of free flow in the writer (1). Group of psychologists and psychiatrists now also widely apply writing as additional diagnostic tools under the branch of graphology called psychometrical graphology or graphometry. Graphometry uses the handwriting samples to describe the colleting techniques of psychic impressions of a person (1, 14).

3. Handwriting Analysis

Handwriting analysis is an art and old science of interpreting personality traits. Handwriting analysis is neither a cryptic study nor it is a game guessing or fortune telling. The handwriting analyst is not supposed to guess anything about the writer (5). The graphology cannot depicts the writer's age, gender, nationality and occupation from the words written on the paper and is irrelevant to the analysis (4). Gaphologist, all can do is to tell about the characters and features found in the handwriting sample (5). It is a

standard forensic practice for the identification, assessing and understanding of a person's personality by analysing basic patterns of the handwriting including strokes and pressure. Analysis of the handwritten samples exposes the real personality of an individual such as fears, honesty, emotional outlay and resistances etc. It is considered as a written trace of an individual's desired rhythm, style and typical manner of moving. Handwriting illustrates the behaviour of a person towards his/her relations with stress. In handwriting analysis, the frozen graphic structures are studied which are generated in the author's mind and placed in a written form on the paper. This piece of handwriting, portrays a window to the personality structure of writer by producing a thumbnail sketch after analysis of the all elements of writing (7, 8 and 10).

No one can have the flawless writing style. Graphology reveals the strength and limitations found in our personality, can help us to grow and develop as an individual. The handwriting analysis can interpret both positive and negative aspects of the writer's personality based on the writing flow and other features in combination. The first impression of a writing piece can direct the reader towards dominant and most important handwriting movements. Such as of those writing samples with more contradictory elements interpret that the writer has some inner conflicts which may be unconscious and not recognisable by the writer. Some writing piece has a tidy looks which interprets a tidy mind and well organised living standards. If a writing is dominating the space, then the writer will have the capacity to rule the people around them. Speedy and energetic writing reflects a person with quick mental skills. A general and an original writing style does not depicts the traits of the writer as the writer does not take into account the other writing features and is difficult to read the writing suggestions.

Every feature of handwriting including size, slant, spacing and pressure etc. conveys a meaning in a general way with the associated symbols. Such as the strokes of pen on a piece of paper symbolise the writer's emotions, their facial expression and quality of voice or body language. It is not only the handwriting movement to interpret the traits but the combination of all features of writing style that builds up the picture of the writer. For a correct interpretation, graphology uses 3 different handwriting movements with same meaning and at least 300 different handwriting features during writing analysis, and are measured by following precise rules. Some of these movements are natural and some are superficial which can be changed with the mood (4). A detailed description of these handwriting movements are as follows,

3.1. Zones

- There are three zones in handwriting namely upper zone (UP), middle zone (MZ) and lower zone (LZ). Each zone is with average size of 3mm. The writer is well balanced if all zones are of equal size and this can be obtained if three zones go together. Only letter f spans all three zones as shown in figure 1a.
- Vowels (a, e, I, o, and u) and all other small letters that don't have extensions such as c, m, n, r, s, v, w, x, are included in the MZ letters as given in figure 1b). Some parts of other letter including b, d, h, and y are also written in MZ. MZ interprets that how the writer fit and relates to others in everyday life. Ego of ones can be depict by this zone.
- The UZ interprets the values, goals and ambitions with the letter b, d, f, h, k, I, and t as mentioned in figure 1c. If these letters are extended then it indicates unrealistic expectations and achievements.
- The letters that drop below the baseline such as f, g, j, q, y, and z are LZ letters as Y letter shown in figure 1d. The LZ interprets the physical drive, feelings and security needs of a person.
- One zone larger than other zone depicts extra energy invested. As if the UZ is larger the writer puts interest more on ideal and aspiration hopes. Larger LZ shows interest on material needs and consideration or sometimes a person down to earth (1, 2, 4 and 5).

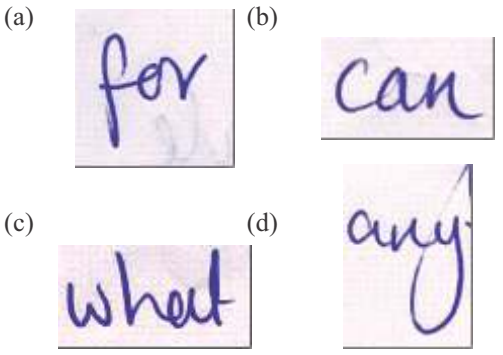


Figure 1: UZ, MZ and LZ illustrations with respect to letters positions on paper (4).

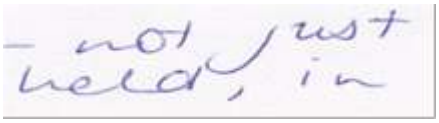
3.2. Baselines

• The baseline is known as the writing line where the middle zone letters assemble as given in following figure 2. The straight direction of the line indicates the sentiments, state of mind and as well as the basic image of writer's personality.

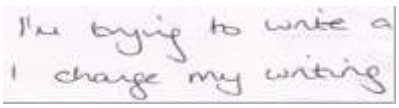
Figure 2: Baseline along with all three zones(1).

- Straight Rising lines as written in figure (3a) show willpower, goal, confidence, positivity and a jolly mood.
- Straight lines interpret reliability of determination, command and discipline.
- Falling lines can be resulted due to any physical illness or fatigue that can be momentary by making them doubtful.
- Wavy lines as shown in figure (3b) predict someone who avoids trouble by being tactful.
- Concave lines as in figure (3c) show a regaining of power and energy which gives the writer courage, strengths and willpower.
- Convex lines as shown in figure (3d) interprets a declining of early interest and energy by being a good starter who gets easily fed up, or becomes a bad finisher with lack of fortitude.

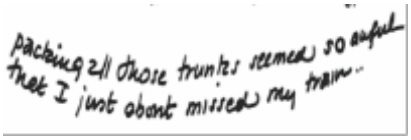
(a)



(b)



(c)



(d)

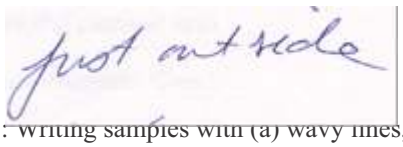


Figure 3: Writing samples with (a) wavy lines, (b) straight rising lines, (c) concave line, and (d) convex line (1, 4).Figure 3:

3.3. Slant

The slant specifies openness towards or away from other people therefore disclosing the social approach and emotional resistance. Also characterises whether the writer pay attention to future or past. A slant in writing can be of inclined or rightward slant, leftward or declined slant and upright or vertical slant as shown in following figure;

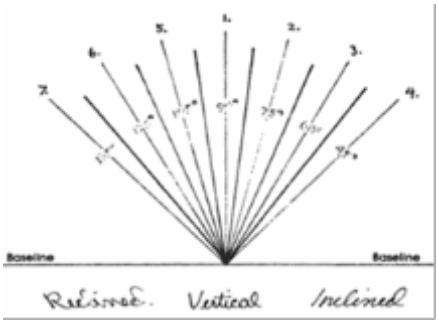


Figure 4: Graphical figure showing Slant types along baseline (1).

• Rightward or Inclined slant indicates that the writer is kind, talkative, courageous, friendly, passionate, bold and spontaneous, led by heart overhead.

• Leftward or Declined slant interprets the writer to be thoughtful, reserved, careful, faithful, deep, and makes conclusions based on past experiences. It is difficult to know them well as feelings are concealed. They need to be fair and balance to themselves and get annoyed easily if pushed for more commitment.

• Upright or Vertical slant movements show stability, independency and truthfulness. The writer is intelligent, judgmental, composed in crisis and pay attention to present time by ruling head over heart.

• Mixed slant shows someone who may be volatile in their reactions with internal clash and lack of coordination by being irritable and flexible with artistic skill.

•

3.4. Pressure

Heavy pressure point out good vitality altitudes, strength and obligation. Very heavy pressure means that the writer responds fast to criticism. This can be felt on the reverse of the paper with an outward impression. Light Pressure is illustrations of sensitivity to atmosphere and understanding to people. Sometime can be with

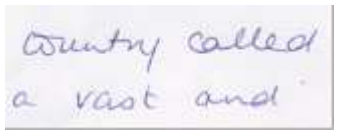
less liveliness. Light pressure is observed without impression on the reverse of the paper.

3.5. Width

Width is the measure of space between the letters in the middle zone. Wide and narrow space defines the broad and narrow width.

- **Broad writing** infers plane extension - social or physical responses. People with broader writing as shown in figure (5a) tend to be sincere, practical, and open minded, talkative, travel loving, and luxurious.
- **Narrow writing** denotes control and prevention of social development with self-discipline. They are budget oriented, creative, reserve, and narrow-minded as in following figure (5b).

(a)



(b)

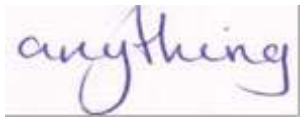
Figure 5: Writing width showing (a) broad and (b) narrow writing types (4).

3.6. Size

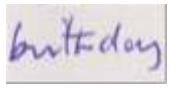
The average size of the handwriting that spans all three zones is 9mm or 10mm that is known as medium size. Writing size that is less than 9mm is considered small size and writing that is larger than 10mm is considered as large size indicating the level of activity, confidence and significance of the writer.

- Large size indicates enlargement and filling of the writing space that shows a person who is friendly, social and open towards people. They are determined, optimist, ruling, voyager, courageous, kind, arrogant, and lonely. Very large writing indicates a show-off who wants to be noticed as shown in figure (6a).
- Medium size will show a person with a frank and faithful outlook.
- Small size as in figure (6b) shows the opposite side of person with inconsistent and varying personality- movement that is inhibited. They are modest, ruling, thoughtful and active in their academic field, and sometimes being less social unless contacted by others.
- A variable size writing mainly in the MZ will show someone who is delicate responsive to the environment as shown in figure (6c). They may be irritating and undetermined in their track of life.

(a)



(b)



(c)

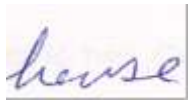
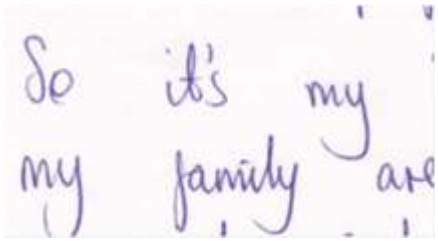


Figure 6: An illustration of writing sizes including (a) large size, (b) small size and (c) variable size (4).

3.7. Spacing between words

- Wide spacing shows that the writer needs social space as barrier between him and others. Too wide spacing as given in figure (7a) shows that he desire to make social interaction but find difficulty. It also indicates a person being independent and judgemental who needs personal space.
- Narrow spacing shows that the writer needs to contact people due to his insecurity. He tries to be friendly, kind, open, and is unable to live alone as shown in figure (7b).
- Variations in spacing shows instable approach to others, and behaviour that cannot be relied upon.

(a)



(b)

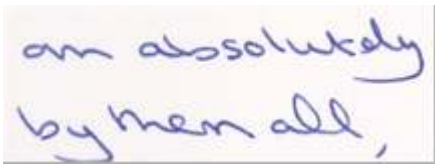


Figure 7: Writing samples showing (a) wide spacing and (b) narrow spacing between words (4).

3.8. Spacing between lines

Clear spacing indicates good neutral decision, a sense of balancing and a vibrant mind.

- **Very wide spacing**

Between the lines interprets a loss social contact with people around or poor hold of the certainties of normal life as shown in figure (8a).

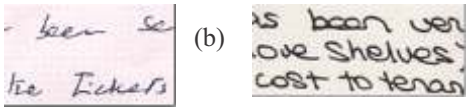
- **Narrow spacing**

As shown in figure (8b) indicates poor conclusion over incapability to view things – lack of perception.

- **Mingled lines**

Are formed when loops from the LZ get crossed over with loops from the UZ and indicates signs of mental disorders or confused thoughts as in following figure (8c).

(a) (b)



(c)

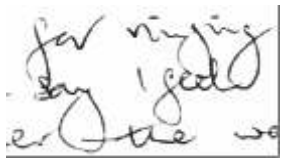
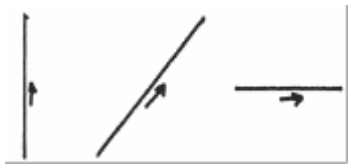


Figure 8: Writing samples showing (a) wide spacing, (b) narrow spacing and (c) mingled between lines (4).

3.9. Strokes

Strokes are the movements of letters while writing any word that could be straight, square, vertical, horizontal or diagonal as shown in following figure;

(a)



(b)

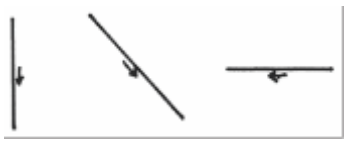


Figure 9: Graphs showing (a) upward and rightward strokes and (b) downward and leftward strokes movements (1).

- **Starting strokes**

Shows that the writer desires to plan the future as they are thoughtful, straight and sometimes can postpone. The presence of straight strokes in LZ may show annoyance or willpower. If there is no stroke in the writing then it shows that the writer has finalised their plans and ready to react to conditions.

- **End strokes**

Indicate that the writer has completed their social tasks or any public matter. If the end strokes don't come back down to the baseline then it means that to commit or accept things is difficult for the writer. The absence of end strokes shows independency, maturity and unpredictable.

Presence of long curved stroke interprets kindness and sympathy whereas a long straight stroke on baseline means that the writer is doubtful and inquisitive. The final stroke that moves from MZ to LZ indicates stubbornness and hooks in the strokes shows greediness or persistence.

3.10. Loops

Presence of loops in the zones specifies thoughts, visions and sentiments. Shapes and locations of loops give different meanings like straight strokes which are up and down indicates that the writer is sensitive with emotions and is down to earth to do any task as shown in figure 10.

- Loops in UZ shows that the writer is concerned about things through their fancy world in a practical manner. This imaginary thoughts and ideas come through the presence of wide loops.
- Full loop in the LZ with heavy pressure shows liveliness, curiosity in money and physical materials whereas full loop with light pressure shows desire for safety. An unfinished or incomplete loop in LZ shows prevention of violence and conflict. Variant loops in LZ shows that the writer may be impatient or fuzzy emotionally.

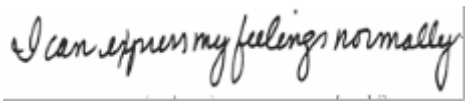


Figure 10. Loops formation and variation with respect to UZ and LZ in writing (1).

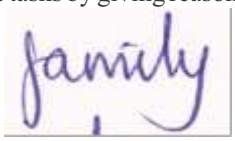
3.11. Connection

• Connection is formed by the joining of letters in a word showing that the writer can be ruled only by motivation and reasoning. More connectedness as given in figure (11a) shows the person enjoys more when in company of other people. These type of people is decent at focusing and finalising tasks but finds it tough when interrupted.

• **Disconnected**

Writing as shown in figure (11b) indicates person who follows natures and perception. He is able to cope with numerous tasks at once and has an artistic mind.

• Writing with Combination of connected and disconnected shows that the person is natural and complete tasks by giving reasons.

(a) 

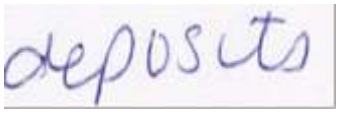
(b) 

Figure11:Connection (a) and disconnectedness (b) between letters in a word(4).

3.12. Forms of Connection

Forms of connection interprets the boldness and mental aptitude of the writer towards the people and world.

• **Arcade** writing as shown in following figure is formed when m and n letters make arches with curved tops depicts loyalty, care, liberty, reliability and systematic task leaning people. They are materialistic learners and do their work with routine.

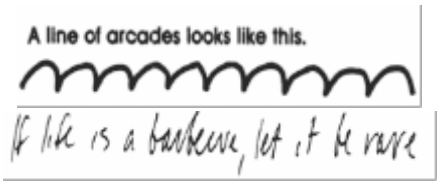


Figure 12: Graphical representation of Arcade writing (1).

• Garland form comes when arcade is inverted and shows a person who writes in cursive way. M and n form cup shapes which shows that the writer enjoys by helping other as in following figure;

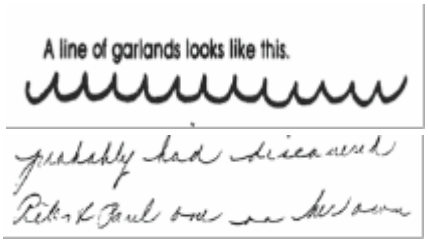


Figure 13: Garland formation in writing (1).

• Angle formation gives impression of curiosity and efficiency. Angular writing indicates a person who does not care about clash. Angular writing looks like as in following figure;

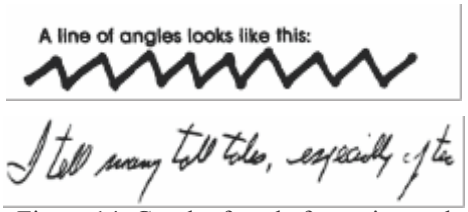


Figure 14: Graph of angle formation and angular writing (1).

• **Thread** writing form is like untied wool as illustrated in following figure. Writers with this type of writing are attentive and flexible but can be mysterious. They are patient and respond quickly rather waiting by good observation. Thread writing shows that the person is concerned about and does not other people to know them.

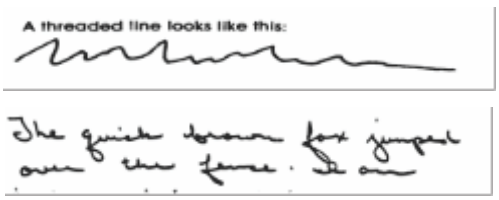


Figure 15: Thread formation and threaded writing (1).

· Wavy line is a mixture of all above forms that indicates maturity and expertise of someone. They are flexible, imaginative and have good handling mechanisms. People with rounded forms are friendly.

3.13. Style

Style deals with the look of the writing that how basic or complicated it is. A basic and simple style is readable only with important strokes. A simplified writing style interprets that a person has a concrete approach to life. They are objective, sensible and fluent, and focused on

truths by quick or clear respond.

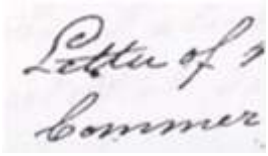
- **Enriched**

Style as shown in figure (16a) is with extra strokes specifies that person is possibly unusual, artistic and desires to be familiar. Enriched writing shows slow and controlled movements by creating imaginary look. They can have desire for luxury, amazement and lack neutrality.

- **Neglected**

Writing lacks necessary features which makes it unreadable as given in figure (16b). This happens due to short time, trying to cover all ideas on paper or the writer is not concerned with the reader by losing connection. This type of writing style shows laziness, lateness and irregularity.

(a)



(b)

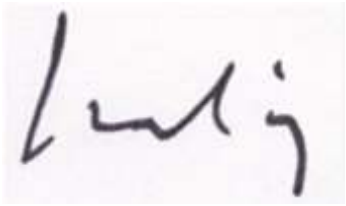


Figure 16: Writing styles showing (a) enriched and (b) neglected ones (4).

- **Copybook**

Style is exactly as it was trained at school that indicates someone who follows the rules is reliable and enjoys team work.

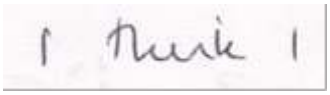
3.14. Personal Pronoun I

- The I letter in a sentence indicates the writer's opinion of their personality that how they perceive themselves. A tall I letter regular in size indicates strong self-possession and straight I without stroke indicates someone who sticks to fundamentals as shown if figure (17a).

- **Curved I towards left**

Shows some affection to past and self-consciousness. Letter I with small stroke when compared to the rest of the text shows lack of self-confidence. Letter I with stroke at top and bottom shows a business approach.

(a)



(b)

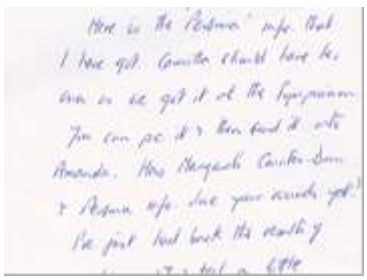
Figure 17: Different presentation of letter "I" in writing (4)

- I letter when written like number 2 specifies feeling of being second level by avoiding getting too close to people.

3.15. Margins

- Left margin as shown in figure (18a) depicts past and beginnings of new roots. A wide left margin means that the writer is likes to move on away from the past. Narrow margin means that the writer is careful to move on with connection to the past. A straight and aligned margin shows decent self-discipline.
- Right margin as given in figure (18b) demonstrates future and people around. A wide margin means there is an unknown fear and when it is narrow shows annoyance and keenness to get out there with things.

(a)



(b)

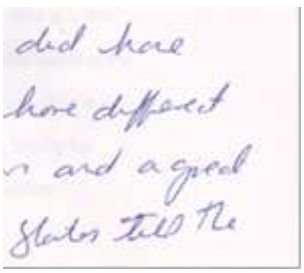


Figure 18: Writing samples showing (a) left margin and (b) right margin with respect to page alignment (4).

4. Signature analysis

In handwriting signature and personal pronoun I are possibly the two most familiar graphic movements that a person writes on the paper.

They are symbols of one's image shortened into a small informative layout. Where the handwriting could be an unconscious attempt, the signature is a conscious form of handwriting that symbolizes the actual person with desires of be recognized by the people. As the person matures, so does the signature. We can produce signature of desire by practice but destroyed due to more usage as in case of doctors or directors who signs numbers of routine certificates. We create the signature to represent our self to world by writing it on checks, credit cards, documents, and driver licences. Differences and similarities are important to be noted in the body of hand writing for a correct depiction of personality. When both body writing and signature are regular, it shows an upfront and truthful person as follows;

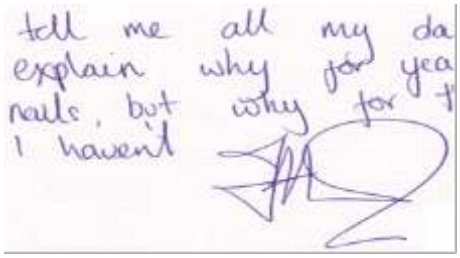


Figure 19: Writing sample showing that text and signature both are regular (4).

- **Larger signature**

Represents people who wants attention and good impression. Desires to look more confident than he really feels as can be noticed in following sample;

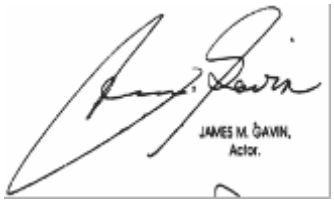


Figure 20: Sample of Larger Signature (1).

- **Smaller signature** indicates person who does not pursue a high profile and deals with people in a formal way as in following figure;

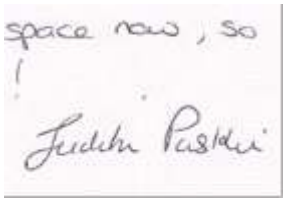


Figure 21: Sample of Small signature (4).

- **Signature slanted**

More towards right than the script displays welcoming and communicative nature of the writer that easily become artificial. Socially friendly but work individually.

- **Upright signature**

Than text shows independency but desire to work socially as they are comfortable with crowd as follows;

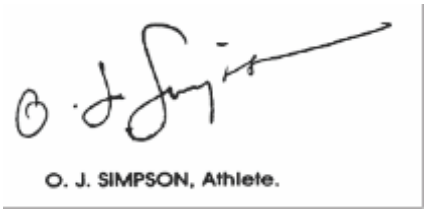


Figure 22: Sample of Upright or inclined slanted signature (1).

- **Signature with full stop**

Shows reserve attitude of the writer who does not want interruptions in private concerns.

- **Signature with underline**

Shows emphasis to the signature that the write wants attention. A dramatic line represents an actor and a wavy line says that the write wants to be liked by the readers. Both full stop and underline can also be noticed in one signature as follows;

Figure 23: Signature sample showing Full stop and Underline (4).

- Graphic effects with loops, thread and angle formation especially when differ from the body of writing shows interests in others by being friendly and attentive but for his own mean (1, 2, 3, and 4).

5. Question Document Examination

Respectively each age has its crimes along with the relevant defensive conditions and measurements. Similarly the crimes get advance with the same manner of development in

measuring conditions. In respond to this, the society becomes alert to overtake crime by discovering new measures (2, 3 and 11). People get the knowledge of handwriting for many motives such as the science of criminology offer courses which entitle one to be a qualified and licenced handwriting expert. The results obtained for the purpose of finding identification and validity of a particular document is admissible in the court of law. Professionally qualified person in this field is known as questioned document examiner. A questioned document expert works in collaboration with law enforcement agencies, attorneys, and one who is determining the actual writer (1). Expert witness which is definitely scientific, and not only empiric has got important place in the court of law (2). With the service of handwriting expert, many trial cases have been proceeded to determine the guilt or innocence of the offender like those of psychologists and psychiatrists cases (1).

Forensic document examiner deals with the authenticity of the questioned document. They can identify the documents if they are genuine by determining the time frame when it was created, who create it, what materials used in preparing or any modification in the original script. The look for alterations, obliterations, erasures, and substitution in any document evidence. To narrow the identification, they study methods, techniques and materials. Crucial clues can be obtained from the ink, paper, writing tools, ribbons, stamps and seals used in the production of the document. Other valuable evidence can also be obtained from visible marks on or invisible impressions in document for further assistance. Documents related to criminal or civil cases can provide an abundance number of information for the case proceedings. Such as suicide note found next to the death body can tell either it was written by the killer to cover up his crime or really by the suicide himself. Other cases involve the note written by bank robbers with invisible impressions that can give clue about the address or the will of a healthy person altered by the relative for the windfall (3).

Forensic questioned document is often linked to white collar crime such as fraud cheque. However, forensic questioned document examination is also practiced in a wide range of cases like medical misuse, art forgeries and homicides. Digital age is making way for the criminals by the availability of useful software programs such as Adobe Photoshop, Acrobat and others that help to create and manipulate documents form fraudulent contracts to currency. Other investigated questioned documents that are parts of our daily life include questioned signatures, documents with alleged fraudulent alterations, disputed documents with concern of age or date alterations, typewriting questioned documents, and documents that identify a person by handwriting from anonymous and disputed letters or registers. By comparing these documents, the forensic document examiner can include a suspect or exclude an innocence from the investigation (2, 3).

6. Equipment used in Forensic Questioned Document Examination

The handwriting analysis is not only restricted to understanding of personality, health issues or mental problems but it is also applied by the forensic document examiners to check the authenticity or forgery. These examiners study different structures associated to the motion and pressure of the written document, shape and three-dimensional relationship among them. Depending on standard protocols, the examiners process the documents manually which requires a substantial amount of time that leads to a subjective analysis which is problematic to repeat. Many automated forensics tools are used to execute handwriting analysis from scanned documents such as Graphj and Biomatric signature. These tools help the examiners to perform analysis in a more neutral and replicable ways. These tools and techniques are controlled under well-established principles of physics and chemistry. A typical questioned document unit in any crime laboratory is basically equipped with microscopes, digital imaging instrumentation, infrared and ultraviolet light sources, video analysis tools and some specialized equipment such as electrostatic detection device (EDD), and materials to perform analytical chemistry (2, 3 and 12). A brief details of these devices and equipment illustrated as follows;

6.1. Graphj

GRAPHJ is a forensics tool use for handwriting analysis. The tool has been designed with forensics protocol applied for Report Investigation Science (RIS). Graphj guide the

examiner (1) To detect text lines and different words in the document automatically, (2) To detect significant features in the handwritten text, (3) To measures the height and width of the detected elements, and (4) To generate a report that contains all parameters utilized during analysis. Report generation improves the repeatability of the entire process (12, 14, 15 and 16). Process of handwriting analysis via Graphj is graphically given as follows;

Figure 24: The typical workflow of handwriting analysis in GRAPHJ (15).

6.2. Biometric Signature

Signature is subjected to the handwriting analysis where researchers used the idea of graphology to build an automated signature verification system. In this system the signature features are analysed computationally. The same features studied in graphology are considered for the automated signature verification (12, 14). Biometric signature is used for the recognition purposes of digital signature based on the features when signing his/her name. Biometric system detects the direction, stoke, distance, size, pressure and shape of a person's signature enabling handwriting to be a reliable sign of identity. GrafoCerta which means sure signature was first developed by Italian company named "Namirial". It has research capability particularly in forensic sector. A research laboratory on handwriting analysis was created by a team of handwriting experts and computer engineers (13).

6.3. Electrostatic Detection Device (EDD)

Electrostatic detection device such as Electrostatic Detection Apparatus (ESDA) is used for the visualization of documents with indented impressions not visible to naked eye. Toner and applied charges are used to the indented area making them visible. ESDA uses the principle that indented area carries less negative charges than surroundings which causes the toner to be attracted to this area, revealing the presence of indentation. Documents with indented impressions can be recovered up to seven layers beneath the original writing by using this technique. The documents with indented impressions as old as 60 years can be successfully visualized if not mishandled or properly stored (3) as in following case;

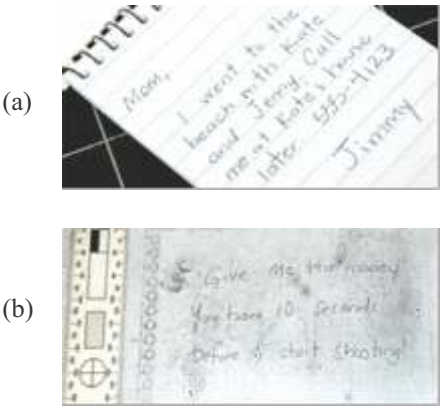


Figure 25: (a) A note book found with suspect's personal effects, (b) The same note book when analyzed with an EDD reveals invisible impressions of the robbery demand note (3).

6.4. Video Spectral Comparator (VSC)

Ultraviolet and infrared wavelengths of light are used in many photography and other imaging devices for detection of invisible alterations, obliterations and erasures from the documents. Video spectral comparator is of such devices that uses radiation of different wavelengths to analyze if any different source of ink is added, altered or removed. These variations in ink source produce different wavelengths of lights which is detected by VSC as in following altered cheque case (figure 26) and obliterated note (figure 27);

Figure 26: (a) Altered Cheque written in black ballpoint pens when viewed with visible light, (b) same Cheque viewed with infrared radiation (VSC) (3).

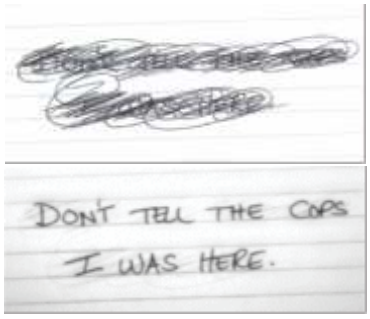


Figure 27: (a) Obliterated note viewed with visible light, (b) same note viewed with Infrared radiation (3).

6.5. Detection of Document by Source

6.5.1. Detection of Individual Dye Components

Chemical composition of inks on a document can be identified by a process call Liquid Chromatography. Small cuts from the questioned document are dissolved in a solvent and then analyze the source of ink by comparing it to the respective or relevant state ink standards set.

6.5.2. Detection of Printed Documents

The source or model or particular make of documents typed by specific machine or printed by any with inkjet printer, fax machines or photocopier machines can be detected by comparing the questioned document to the referred source or standards. Even the process of making can be analyzed known to any specific maker or provider or machine.

6.5.3. Seals and Stamps

Questioned documents bearing rubber seals impressions, watermark or embossed seals can be examined the suspected devices that may have been used in its preparation such as writing instruments, papers, rubber stamps, sealing and printing devices, and manufacture's marks (2, 3 and 9).

7. Conclusion

Handwriting analysis is performing a special role in predicting ones individuality with certain writing features. Handwriting analysis becoming a vast growing forensic field which is not only applied by the graphologist, psychiatrists or psychologists, medical examiners but also by forensic questioned document examiners. Handwriting analysis or forensic questioned document examination is making it easy to control the growing crime rate in our society. Along with the advancement in crime patterns, forensic handwriting analysis is playing its role too in a successive way by developing different scientific methods and tools. These methods are based on standards set by the scientific community or respective area laboratory and are admissible in court of law following expert testimony.

8. References

[1] M. Karen and S.R. Mary, "Handwriting Analysis".

[2] S.O. Albert, "Questioned Documents", The lawyer's Cooperative Publishing Co, 1910.

[3] "A simplified guide to forensic document examination", NFSTC Science Serving Justice, pp. 395-2511.

[4] B. Gill and M. Big, "Graphology Information for Radio Oxford', March 2008.

[5] S. Dorothy, "Handwriting Analysis', Folkways Records and Service Corp, 1962.

[6] A.B. Bart, "Handwriting Analysis Quick Reference Guide for Beginners", Empressé Publishing, 1994.

[7] K.G. Parmeet and P. Deepak, "Behavior Prediction through Handwriting Analysis", International Journal of Computer Science and Technology,. Vol. 3, 2012.

[8] D.A. John and O.F.M. Cap,"Personality Profile through Handwriting Analysis", Anugraha Publication, 2008.

[9] H.H. Heidi, W. Elizabeth and J.W. Emily, "Survey of Forensic Handwriting Examination", 2015.

[10] N.S. Sargur, H.C. Sung, A. Hina and L. Sangjik, "Individuality of Handwriting", National Criminal Justice Reference Service, 2001.

[11] Questioned Document, Virginia Department of Forensic Science, 2015.

[12] Automated Forensic Handwriting Analysis, Proceedings of the 2nd International Workshop, 2013.

[13] P. Milena and F. Roberto, "Forensic Handwriting Analysis: A Research by means of Digital Biometrical Signature", 2013.

[14] S.O. Luiz, J. Edson, F. Cinthia and S. Robert, "The Graphology Applied to Signature Verification".
[15] G. Luca, M.F. Giovanni, F. Antonino and S. Angelo, "Forensic analysis of handwritten documents with GRAPHJ", Journal of Electronic Imaging, July 2018.
[16] G. Luca, M.F. Giovanni, F. Antonino and S. Angelo, "GRAPHJ: A Forensics Tool for Handwriting Analysis", 2017.

Malik et al LGURJCSIT 2019

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 3 Issue 1, January - March 2019

Internet of Things & Cyber Security

Muhammad Shairoze Malik,
Lahore Garrison University, Lahore
shairozemalik@lgu.edu.pk

Abstract:
In today's world, the internet has become the necessity of life. The rapid advancement in technology and inexpensive access to the internet has increased the use of IoT devices in our everyday life. On the positive side, these devices have made our life luxurious by removing the human intervention, but they have also significantly increased the attack vectors in the cyber world. The purpose of this research paper is to look into the effects of the Internet of Things (IoT) devices in our cyberspace and to see how vulnerable we are, in internet society.

Keywords: Internet of Things, IoT, Cyberspace Threats, Security Threats, Cybersecurity, Attack Vectors

1. Introduction

The Internet of Things is a system of interconnected devices that exchange data among themselves via the internet. IoT has diffused in all activities of our daily life, such as healthcare, travelling, businesses, financial transactions, and marketing.

The immense dissemination of inter-connected devices in the IoT has made colossal demand for strong security in light of the developing interest of millions or maybe billions of connected devices and services around the world [1-3].

The number of attacks is rising day by day and has been on the increase in both number and sophistication. Not only the size of the network is growing along with potential attackers, but the tools and techniques used by attackers are becoming more and more sophisticated as well [4-5].

Security is a process of protecting an asset against unauthorized access, physical damage, loss or theft, by maintaining integrity and confidentiality of information [5-6]. As Kizza said [5], there is no such thing as total security of any object, physical or electronic, because no object can have perfectly secure state and still be operational. Ensuring IoT security means maintaining the highest intrinsic value for both physical devices and non-physical ones (data, services, and information).

This paper looks forward to contribute to a deeply understanding of IoT devices and to deeply study some of the attack vectors which can be performed by script kiddies to damage the integrity of IoT based operations.

2. Background:

IoT devices enable the internet to interact with the physical environment. There are three key concepts in IoT domain;

I. Sensors: Sensors are the hardware equipment which convert physical environment into electronic data so it can be processed digitally.

II. Devices: Devices are the physical things to which sensors are attached. They can be human, cars, electronic appliances, etc.

III. Services: According to Thomas [7], a transaction between service consumer and provider is regarded as an IoT service. It performs a predefined function based on the data collected by sensors or initiate actions which cause a change in physical world.

IoT is a hardware component which connects physical and digital world. Also known as a smart thing, which can be healthcare devices,

home appliances, cars, automated factories and almost about anything connected in a network and installed with sensors providing information about physical environment (e.g., humidity, motion detection, fire alarms, pollutions), actuators (e.g., displays, motor-controlled devices, light switches) and embedded computers [11, 12].

An IoT devices is able to communicate with ICT systems and other IoT devices, the communication medium can be cellular, WLAN, wireless, Bluetooth or any other technology. IoT devices are classified as small or normal sized; fixed or mobile; internal or external powered; logical or physical object; automated or non-automated; IP enabled object or Non-IP based object.

Most IoT devices are vulnerable to attacks both internal and external because of their characteristics. Due to resources constraints in terms of power, memory and computational capabilities, it is difficult to implement strong security measures.

In the world of IoT, due to interconnectivity, if one device gets compromised and fall into the wrong hands, the whole network may get compromised. Some reasons, why the connected machines are so valuable for cyber-attacks, are as follows:

I. Physical access to such devices is easy as they operate unattended by humans.
II. Mostly IoT networks work in wirelessly connected network, which make the travelling data vulnerable to eavesdropping.
III. Due to minimum hardware and low power usage, the IoT devices cannot support complex security applications.

Cyber-attacks could be initiated against any IoT infrastructure, causing damage to system operations and endangering the general public and could cause serious economic damage to the owner [8, 9]. Some examples are as follows:

_ A cybercriminal could potentially get access and take control of home automation system of a smart home, enabling the attacker to change the states of heating/cooling systems, lighting, air-conditioning and disabling security systems.

_ Public access to resources such as water and power can by stopped by launching cyber-attacks against public infrastructure like power or water treatment plants systems [10].

_ A cyber-attack on Iran's nuclear facility by the worm known as Stuxnet, caused the enrichment centrifuges to break down [11].

It is obvious now that using IoT technology within physical environment opens doors to new security problems. So consumers of IoT technology should be vigilant about such privacy and security problems.

3. Threats, Vulnerabilities and Security:

In security; physical resources, services and information, both in transmission or storage needs to be protected against any unauthorized access.

In an IoT enriched environment, IoT devices are accessed by multiple objects which includes ICT systems, other IoT devices, authorized users, because of which it is important to control the access to devices and also verify the authenticity of a connection, weather the connection is from an authorized object or not, and if authenticity cannot be verified than no connection to the IoT device should be allowed, because in such scenario an attacker can impersonate as a legitimate object to get access to a device from which the attacker can compromise the security of the whole network.

In addition to the access to devices, another key point is to ensure the privacy of transmitted data. As in an IoT environment, devices, services and users connect to each other over the internet and exchange data between themselves, it is of utmost importance that the data is secured and protected with strong encryption so an attacker should not be able to extract valuable data even if the attacker somehow gets access to the travelling data. To ensure the privacy, a trusted point to point connection needs to be established between devices for data exchange.

Weaknesses in the software and hardware of IoT systems are regarded as the vulnerabilities as they can be exploited by an intruder to get unauthorized access to data and conduct harmful activities.

When the weakness in the IoT systems can be exploited, they are regarded as threats to the systems. Threats can come from two main sources: natural and humans [13,14]. Natural threats like disasters (earthquake, fire, flood, etc.) can cause damage to systems, but there can be no safeguards against such atrocities. The best approach to protect systems against natural threats is to implement damage control plans

like backup and redundant systems. On contrary, human threats are those threats in which people are involved, such as internal [15] (attacks performed by authorized people) or external [16] (organizations or individual working from outside the network) threats, to cause harm and disrupt the environment. Human threats are classified as:

3.1 Unstructured-threats:

Threats comprising of inexperienced individuals also called script kiddies, who perform attacks using easily available hacking tools without any deeper understanding or any major goals in mind.

3.2 Structured-threats:

Threats consisting of experienced professional working individually or collectively, such people know system vulnerabilities and have deeper understanding of the key concepts, they can develop and exploit malicious scripts and codes. An example of such an attack is a network attack aimed at high value targets in private and government sector to steal valuable data and cause disruption in system, this type of attack is known as Advance Persistent Threats (APT) [17, 18].

Criminals launch cyber-attacks to gain personal satisfaction or to indemnify for some lose. These criminals could be anyone, an individual, organized group, hacktivists, or even governments working against other governments. Cyber-attacks have many forms, ranging from passive reconnaissance to active attacks, some common attack forms are:

i. **Physical:** This attack results in damage or destruction of hardware component. As IoT devices mostly work unattended by humans and are spread over a large area, they are highly susceptible to physical attacks.

ii. **Reconnaissance:** This type of attacks, either passive or active, are used to perform information gathering and mapping the services and systems used in a network or to what type of vulnerabilities can be exploited. Some Example are, port scanners [19], sniffers [20], traffic analysis and gathering IP address information.

iii. **DoS (Denial of Service):** This type of attack results in non-availability of network or system resources to users. Due to limited computational and memory capabilities, IoT devices are highly vulnerable to such attacks. An example would be the deauthentication attacks performed over wireless network due to a vulnerability in 802.11 wireless transmission protocol to restrict authorized user to access their own network [21].

iv. **Access attacks:** This type of attack results in unauthorized access to network by an intruder. It comes in two forms: Physical access to hardware and remote access to IP-enabled devices.

v. **Privacy attacks:** Due to easy availability to large amount of information through remote access, privacy of data has become increasingly difficult. Some common attack types are; data mining (to discover information not generally available in certain databases), cyber espionage (to obtain confidential information about others by using malicious tools and techniques), eavesdropping (listening between conversations [22]), tracking (to track individual using UID of devices they own), password based attacks (attempts made to guess user's passwords either by dictionary attacks or brute-force attacks).

vi. **Cyber-crimes:** The smart IoT devices are used to exploit users for materialistic gains such as identity theft, intellectual property or brand theft and fraud [4,5,23].

vii. **SCADA attacks:** Supervisory Control and Data Acquisition Systems are just like any other TCP/IP systems and are vulnerable to cyber-attacks [24, 25] like Denial of Service or Trojan attacks to gain control like the attack of Iran nuclear facility [11] as discussed before.

4. Discussion:

The exponential development in IoT industry has led to more challenging privacy and security risks. Many of those risks are due to IoT hardware vulnerabilities caused by hackers and improper utilization of system resources. The IoT should be developed so as to guarantee safe and simple use by users. Consumers need confidence in IoT devices to completely adapt it so they can enjoy its benefits without privacy and security risks.

The IoT devices are exposed to multiple threats as discussed in this paper but there are no simple

steps that can be taken to ensure the security of these devices. There is a strong need to develop resources who have deep understanding to system capabilities and are equipped in identifying and patching security vulnerabilities in these devices before any kind of harmful exploitation.

5. Conclusion:

To ensure protection and availability of IoT devices and services, privacy and security challenges need to be addressed. It is concluded that much works stays to be done in the development and enforcement of IoT security by both end users and vendors. Upcoming standards need to address the flaws in current security mechanisms. Future work in IoT industry need to aim at deeper understanding of security risks and their implications in IoT environment and these things are to be considered early in product development cycle.

6. References

[1] J. S. Kumar and D. R. Patel, "A survey on internet of things: Security and privacy issues," International Journal of Computer Applications, vol. 90, no. 11, pp. 20–26, March 2014, published by Foundation of Computer Science, New York, USA.

[2] A. Stango, N. R. Prasad, and D. M. Kyriazanos, "A threat analysis methodology for security evaluation and enhancement planning," in Emerging Security Information, Systems and Technologies, 2009. SECURWARE'09. Third International Conference on. IEEE, 2009, pp. 262–267.

[3] D. Jiang and C. ShiWei, "A study of information security for m2m of iot," in Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on, vol. 3. IEEE, 2010, pp. V3–576.

[4] B. Schneier, Secrets and lies: digital security in a networked world. John Wiley & Sons, 2011.

[5] J. M. Kizza, "Guide to Computer Network Security". Springer, 2013.

[6] G. M. Koien and V. A. Oleshchuk, "Aspects of Personal Privacy in Communications-Problems, Technology and Solutions". River Publishers, 2013.

[7] M. Thoma, S. Meyer, K. Sperner, S. Meissner, and T. Braun, "On iot services: Survey, classification and enterprise integration," in Green Computing and Communications (GreenCom), 2012 IEEE International Conference on. IEEE, 2012.

[8] M. Rudner, "Cyber-threats to critical national infrastructure: An intelligence challenge," International Journal of Intelligence and Counter Intelligence, vol. 26, 2013.

[9] R. Kozik and M. Choras, "Current cyber security threats and challenges in critical infrastructures protection," in Informatics and Applications (ICIA), 2013 Second International Conference on. IEEE, 2013.

[10] P.W. Singer, "Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons.", Case Western Reserve Journal of International Law, vol. 47, issue 1, 2015.

[11] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafind ralambo, "A survey on facilities for experimental internet of things research," Communications Magazine, IEEE, vol. 49, 2011.

[12] Y. Benazzouz, C. Munilla, O. Gunalp, M. Gallissot, and L. Gurgen, "Sharing user iot devices in the cloud," in Internet of Things (WF-IoT), 2014 IEEE World Forum on. IEEE, 2014.

[13] K. Dahbur, B. Mohammad, and A. B. Tarakji, "A survey of risks, threats and vulnerabilities in cloud computing," in Proceedings of the 2011 International conference on intelligent semantic Webservices and applications.

[14] R. K. Rainer and C. G. Cegielski, Introduction to information systems: Enabling and transforming business. John Wiley & Sons, 2010.

[15] A. J. Duncan, S. Creese, and M. Goldsmith, "Insider attacks in cloud computing," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE,2012.

[16] P. Baybutt, "Assessing risks from threats to process plants: Threat and vulnerability analysis," Process Safety Progress, vol. 21, no. 4, pp. 269–275, 2002.
[17] C. Tankard, "Advanced persistent threats and how to monitor and deter them," Network security, vol. 2011, no. 8, pp. 16–19, 2011.
[18] F. Li, A. Lai, and D. Ddl, "Evidence of advanced persistent threat: A case study of malware for political espionage," in Malicious and Unwanted Software (MALWARE), 2011 6th International Conference on. IEEE, 2011, pp. 102–109.
[19] S. Ansari, S. Rajeev, and H. Chandrashekar, "Packet sniffing: a brief introduction," Potentials, IEEE, vol. 21, 2002.
[20] M. De Vivo, E. Carrasco, G. Isern, and G. O. de Vivo, "A review of port scanning techniques," ACM SIGCOMM Computer Communication Review, vol. 29, 1999.
[21] Dr. L. Arockiam Lawrence, "A Survey of Denial of Service Attacks and it's Countermeasures on Wireless Network", International Journal on Computer Science and Engineering, vol. 02, 2010.
[22] I. Naumann and G. Hogben, "Privacy features of european eid card specifications," Network Security, vol. 2008.
[23] C. Wilson, "Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress." DTIC Document, 2008.
[24] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, "Scada security in the light of cyber-warfare," Computers & Security, vol. 31, 2012.
[25] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in scada networks," Computers & Security, vol. 25, no. 7, pp. 498–506, 2006.

Ali et al LGURJCSIT 2019

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 3 Issue 1, January - March 2019

Levels of the Depth of Web-Surface Web, Deep Web, Dark Web

Mohsin Ali
Digital Forensics Research and Service Centre
Lahore Garrison University, Lahore, Pakistan
mohsinaly@lgu.edu.pk

Abstract:
The bond between our lives and Internet is becoming stronger day by day, it is because of the fact that internet is now a necessity for living. There is a lot that we do over internet in our daily lives, whether its link to social activities, transferring or obtaining information, or purchasing items and services online all this is possible because of the advancement in web technology. This advancement is certainly not limited to the aspect we experience on web every now on then there is a lot more than this. There is an aspect of web which most us generally doesn't experience, it's the deep web and the dark net.
The article covers features related to surface web, deep web and dark web. Moreover, the article gives an overview of deep web and the dark web with aspect in relation to where, how and why it's been used. What are the factors that are responsible for abusing the technology when it comes to deep web and dark web? The purpose of this article is to highlight the topic that's been discussed every now and then but has been explored very rarely, and to draw the attention of readers to the laws which are available for the protection of victims and for punishing the culprits, since this part of web has adverse effect on people's lives. Finally, the author has given his opinion about this aspect of technology by comparing the rational factors discussed in the article.

Keywords: Information technology, Surface Web, Deep web, abuse of technology, dark web, surface web, Internet surfing, Anti-Cyber-crime laws.

1. Introduction

We have heard many times about the "deep" word in many aspects, mostly it refer to something that has value in depth because of the secrecy or wittiness behind that certain thing. In the world of Internet in particular World Wide Web (www) it refers to the sites that are not easily accessible through search engines, it's because these sites are not indexed by the search that's carried out by the search engines, those searches that are indexed by the search engines are called the surface web: it means that those search are easily accessible through search engines, whereas deep web is totally opposite of its functionality, it's not easily accessible by all browsers, and search engines. According to a survey the material that's visible to us is only tip of the ice berg there is a lot more material of which we are unaware, so the question that arise here is where is that material? Why can't we access it? What's so special about the content that's hidden from normal users? So, the answer to all this is deep web. Everything that we can't get access to is limited by the party who is handling this because the material/content which is available on it, is most of the time against the norms of the society we are living in. Child pornography, cyber terrorism, terrorist financing, smuggling of drugs, and many other explicit contents is available at these sites. The size of the deep web is not imaginable but according to few experts the rough idea of its size is 500 times more than the size of web which is available to us. The difficulty in searching these web pages is that the concept on which most of the web search engines are working on the mechanism of crawling which is indexing of the web pages. Just think of a virtual spider that starts from home page and moves to every single page associated to the search, and then bring the

information to the Google's index servers, and then its organized according to the pre-set algorithm and then finally it is presented to the user, this is how search engines actually work. [1]

2. Literature Review:

The content that is available on deep web is beyond the boundaries of search engines, it contains anything you may think of that is not available on Google. It contains variety of information that might not be available in your countries or some countries because it's been blocked by the censor board or the competent authority within those countries, such material includes unlisted articles, videos, and many other items. It is said that below the surface web there are treasure troves, and one just need to know how to actually trace it. Here are few basic terminologies that are used in this domain of technology, and one must know about these terms when talking about deep web.

2.1. Difference between Dark Web and Deep Web.

In contrast to what generally it's believed that dark web and deep web are the same thing, it's actually not. It is often noticed that people use these two words as synonym of each other and interchange it very often. This happens with people who are generally not aware of this topic. But the difference is quite simple and it worth's knowing it.
The concept of Surface web, Deep web and Dark web is further elaborated by comparing the concept of iceberg. As shown in figure 1 below.

Figure : How deep web works [2]

2.1.1 What is Surface Web according to visual perspective?

Above the surface of water all the content that is available to normal user on daily basis is available. E.g. facebook.com, gmail.com, justice.gov.pk, lgu.edu etc.

2.1.2. Deep Web

Keeping the iceberg analogy in mind, the position of deep web is just below the layer of water where the iceberg meets the under water. This is because the content that is available on the surface web is indexed that means that simple search using a search engine can display those result whereas, the content of deep web cannot be crawled by search engines because it's not indexed.
These links have same general hostnames as the other sites available on internet and have the same extensions as normal domains.
It can be specific URL of a certain communication thread that one might be having with his friend over Facebook Messenger, it can be page of archival material from department of justice, or some internal communication system of LGU. It is not wrong to say that deep web is actually the major part of the internet [3]. Deep web is discussed in detail from section 2.2 onwards.

2.1.3. Dark Web

Taking the analogy of iceberg ahead, Dark web content are those that are present at the bottom of the iceberg, the content of the dark web is only accessible through special software that guarantees anonymity of the users, this is one of the main reasons why entities that doesn't want to reveal their identity opt for this part of the web.
To further elaborate the dark web it is important to know about the domain structure of the dark web, unlike normal web extension like .com, .org, .edu, etc, the dark web extension end in .onion. The network in which these onion domains resides couldn't be accessed through normal browser, one use to access daily routine sites, all you need to access routine site is a Firefox, chrome, safari or any other browser that is available and is widely used, in contrast to daily internet surfing the software which is required for dark web to be accessed is TOR browser. It offers the user a special layer of anonymity, which user doesn't get when he is using surface web or deep web.
The activities that are cater on dark web are full of illegal trade markets, private communication between journalist, hacking communities,

whistle blower, and all other things one can think of [4].

2.2. How to Access the Deep Web

It's impossible for conventional search engines to fetch the data from the domain of deep web. It is because all the information that is displayed on these webs is stored in databases, making it difficult for users to directly search it.

As discussed in the introductory phase of this article, the mechanism which every search engine use for displaying search pages or for displaying the data which it has received from the surface of the internet is through index searching. Since the URL of the web are fixed its easier for Google's crawler bot to access data.

The functionality of search engine crawlers and indexing pages is based on Google's bot system, which prefers to look for the material that is available in first 2 sub-directory of the site, anything below two sub-directory levels is difficult to be furnished.

Let's visualize this concept with file storing folder hierarchy, which we adopt in order to manage our files, e.g. we store files within folders on our desktop to avoid complication with accessing data, from different routes, same strategy is applied here in deep web.

Bypassing password protected pages to access information is difficult as confidential data is kept there and accessing it through normal standard browser is certainly difficult task.

Since the size of data of deep web is huge, and the information that it possesses is in depth, there is no such clear way to access this information [5].

There are several ways which we use to access to our email address, bank accounts, online portals, or social media accounts, which depends on the route we take in order to reach it e.g. if we want to access our account just by entering the address of our mail provider in address bar or by clicking at certain links, which redirect to the desire site.

On the other hand, there is a lot of information that is on deep web and is publicly assessable by but there are no definite links to access it, or no hyperlinks to click on to get access to it, but it publically assessable unlike dark web, where user need to use particular browsers such as TOR browser to access it.

People who access dark web for any means follow the strict procedures to hide their identity or to stay anonymous, as there have been several cases in past where Tor browsing has been monitored by the authorities, or the real IP address of the user is revealed because of the occasional vulnerabilities [6].

2.2.1. Search Engines and its role in deep web:

One of the most prominent search engine that is used for browsing the content of deep web is “duckduckgo.com” (shown in figure 2). This browser is considered to provide information that is available at surface level and information that is deeper than the surface level [7]. Moreover, according to [8] it is one of the powerful search engines for semantic search. Considering the sensitivity deep web, this search engine is used by many users because of its favourable policy i.e. it provides the information to the user without keeping record of it and values the privacy of the user [9].

Figure : Search Engine "duckduckgo.com" [8]

Since it's commonly known that's the reason there is not much of information here.

2.2.2 Use of Dorks within search engines:

Another technique that is used by this community of deep web is use of dorks, it is used because it can further enhance the search and can look into the sub folders and directories of the website, dorks are the additional elements that are added to the keywords or searching material in the search box of a search engine. Its common practice of cyber attackers and practitioner to use dorks in order to look for the vulnerabilities within the web-based system e.g. for scanning

the ports [10].
There are several kinds of dorks and each dork is used on according to the situation. There is a clear difference when we search for the content without dork and with dork.
In order to proof that search engine only furnishes the index search, a random search was performed "dform delhi government", the screen (figure 3) clearly shows that instead of getting output for "dform" the search engine has changed the search to "form delhi government", and this search is navigating to the page that is having several forms.

Figure : Ordinary Search in search engine

On the other hand, if we make the same search using one dork it will navigate straight to the "dform" refer to figure 4 below.

Figure 4: Searching in search engine using dork

Now that we have just modified the search by adding the dork "ext: doc" the output that we have received is the exact "dform" in doc format. This shows that there is significant improvement in the search output when the dorks is used, as it can help to search deep within the site. The dorks that can be possibly used for sub dir one [11]
Dorks are used for abusing the search engine, the hackers and the attacker use dorks for accessing the directories which are not visible through ordinary search [12].

2.2.3 Searching for Materials using the search bar within the social media sites and different online libraries:

This has been brought to law enforcement agencies that the black market usually advertise their products on social media, through different closed and secret groups, one such example was found on Facebook where a secret group was identified for selling the illicit, and illegal product such as details of stolen credit cards [13], after the identification these groups were removed and Facebook is advised to keep strict vigilance on creation of such group. One such example is shown in the figure 5 below

Figure 5 Facebook group involved in selling of fake credit card [13]

Apart from presence of deep web participants on social media, there has been significant number of users who are accessing it using database sources, that's the reason with the emergence of deep web activities the database sources have gain huge amount of consideration [14]. These databases somewhere deep have the folder that's catering the needs of the deep web activists.

2.2.4 Use of Deep Web Analyzer (DeWA):

Since it's not just matter of clicks that can land user to the web page or the content of deep web, there is a lot of hassle that one has to go through in order to reach the content of deep web, considering this a team [15] has presented at Black Hat Conference (One of the most prestigious conference for matter pertaining to information security and is widely attended by white/grey/black hackers and security

community) The purpose of this tool is to help investigating agencies in tracking down cybercriminals, tracking new cyber threats and for extracting useful information from web. E.g. the campaigns that are launched for new malware threats.
DeWA basically consists of 5 modules.

1) Data Collection: This module is responsible for collecting data and saving the new links (URLs) from different numerous sources.
2) A universal Gateway: This module is responsible for carrying out operation to unearth different darknet domains which run on TOR or I2P protocol, and by determining the custom Domain Name Server Address
3) Page scouting module: The task of this module is to crawl new URLs that are collected.
4) Data Enrichment Module: The function of this module is to utilize other available resources with information received from page scouting module.
5) A storage and Indexing module: The role of this module is to make data available for analysis in future or if more consideration is required on collected data [15].

2.3 Problems in unearthing activities that are carried out in deep web:

There are several challenges that law enforcement agencies have to go through in order to deal with the culprits dealing deep web and dark web.
Till the day law enforcement agencies are facing great challenge in exposing the culprits who have committed crime at international level on the "Surface web". So, when dealing with deep web there are several other elements which make the case more difficult for law enforcement agencies to sort. Technically there are three major issues which law enforcement agencies has to cater when dealing with dark web or deep web:

- The content which is available on deep web or dark web is encrypted, this shows that the criminals are more conscious of being trapped or monitor. So, encryption is the very first step which is taken by the criminals to secure themselves.
- Since everything of dark web is available on .onion domains, there is no clear way of routing that's done on these domains, this cause further hurdle in investigation to know about the criminal and to analyse the profile of the criminal.
- Because of the constant change in Deep Web, it's really difficult for investigator and for defence lawyer to proof that the content they are talking about actually exists. It is said that the illegal marketplaces on deep web changes its domain site every couple of weeks, and this change is not only within the URL address of the market place, but it is with the name as well. Unlike many of the marketplace sites that are constant. For the evidence gathered from deep web should be documented properly challenge is to take screenshot of every instance with timestamp, so that defence lawyer or advocate couldn't deny the arguments of the investigator [16].

2.4 How to protect your product to land into deep web:

There is no doubt about the fact that the growth of deep web is inevitable, therefore it's a need of hour for organisations to adopt technology and techniques that can protect organisation and companies from losses.
The new brand protection strategies of organisation must include policies of monitoring deep and dark web. For this particular technique there is need for the collaboration of IT security team with the marketing or sales team who can identify the product the security team should keep an eye on the cybercrime zones this includes market places where fraudulent mostly trade. Moreover, they should know about as many digital arenas as possible, where there is chance of the product that can be sold to the cyber squatters. This includes data paste sites, chat sites, social networks, Chat rooms) [17].
Organisations should have effective policies for guarding their product as well as for the situation when they find their product being misused on deep web.
Apart from the effective use of techniques it is important to use the tools that are available online which can secure your product from being misused or from being sold b illegitimate seller. These tools allow the legitimate owners to identify their product and stop it from being

abused by the cybercriminals on Deep web. The operations that are carried out by these tools includes process from identification of products by removing the proxy that creates proxy for the product till the process of removing the product from the identified domain. Such tools are mostly helpful in cybersquatting of domain name, where it identifies the legit domains and stop it from being sold by cyber squatter under Uniform Domain Name Dispute Resolution Policy (UDRP Procedure) [18].

2.5. Factors for abusing technology:

This is interesting aspect of this technology (the web technology) because abusing of web is not only used by the cybercriminals, but it's also used by the military, law enforcement agencies, human right activist and journalist. There is a long list of professionals from our society who use this. E.g. it's been used by journalists for leaking information in the form of WikiLeaks, where leaked information was submitted by the informer on a page of deep web [19]. Moreover, the law enforcement agencies have especially employed the White Hat Hacker in order to monitor and track down the activities of cybercriminal using deep web who are checking the web on routine bases to monitor this aspect of the technology, that is one of the reason for why FBI and Europol were successful in shutting down the famous silk road version 1.0 and silk road version 2.0 [20]

On the other hand, it is used by the terrorist organisations for spreading their propaganda, for launching recruitment drives and activities that can support their movement [21]. In addition to all this the deep web page are used for selling the exploit for vulnerability that are considered zero day [22].

Apart from the Interest of the cyber practitioner and law enforcement agencies there are technical factors that are also responsible for abusing this aspect of technology this includes not allowing file directory or page name specifically from being accessed by the crawler by making alteration to the robots.txt file of the web directory. Web Page being not linked to any other page of the site, for accessing this particular kind of page on deep web one needs to have full knowledge about the path and the directories of the particular website, another reason why crawler fails to reach certain pages is that there are specific conditions applied to that particular web page this means that for certain number of time web page is allowed to be accessed, so if this condition is met than its hard nearly impossible for crawler to retrieve this particular site [23]. In addition to all this deep web also uses the approach to hide the data using password protected websites, this means the person who intends to access this website should be a user, for these sites in particular there is no signup page member of these communities receives their credentials by some other means. Adding cherry on top, it's not mandatory that the data is saved as HTML content (on a webpage), in case of deep web it's not necessary the data can be saved in a form which can't be handled by search engine, it can be a text file encoded inside any multimedia file, in other words it could simply be non-HTML file.

These are the reason contributing to the growth of deep web day by day, according a statistic the deep web is 400 to 500 times more than surface web alone [24].

3. Laws against the Illegal use of Deep / Dark Web:

Till now most of the countries have law against the illegal use of computer and internet. Though the laws are not in direct relation to access of deep web or dark web, since accessing deep web or dark web is not illegal, abusing this aspect of technology in this way is certainly illegal, and there should be a proper way for dealing with this aspect, for this government has set laws, in order to make sure that the operations using computer system or internet in general does not harm any on.

As mentioned earlier though there are many countries that have laws against the abuse of this aspect of technology, but only Pakistan, USA, and European Union laws will be discussed in the preceding section of this article.

Laws that are directly or indirectly linked with deep web and dark web are mentioned in the following section. These clauses or sections have been highlighted with respect to the abuse of technology mentioned in (section 2.5)

3.1 Laws in Pakistan against the Illegal use of Deep/ Dark Web:

As every state has set some rules and regulations to ensure peace in the region and to provide justice to the weaker or the victim, Pakistan too

has set cybercrime laws under which culprits are punished. According Prevention of Electronic Crime Act (PECA) 2016 [18] there are strict punishment against the crime that are performed in deep web by the culprits the example of some of the crimes are as follow,

"Section 4: Unauthorised copying or transmission of data

Section 6: Unauthorised access to critical infrastructure information system or data.

Section 7: Unauthorised copying or transmission of critical infrastructure data.

Section 10: Cyber Terrorism

Section 11: Recruitment funding and planning of terrorism.

Section 15: Making, obtaining, or supplying the device for use in offence.

Section 16: Unauthorised use of identity information.

Section 18: Tampering etc. of communication equipment.

Section 20: Offence against the dignity of the natural person.

Section 22: Child pornography.

Section 23: Malicious code

Section 25: recognition of offences committed in relation to information system." [25]

Above mention sections are all subject to punishment, and the intensity of punishment may vary according to the intensity of the crime, this ranges from a imprisonment of six months to 7 years, with cash fine or both. In deep web many of the offences are committed which falls under the section mentioned above.

3.2 Laws in USA:

The United States is one of the pioneer to have laws for computer related crime. These laws were first seen in early 80s, when congress had added provision to Comprehensive Crime Control Act of 1984, this provision was added to deal with unauthorised access and use of computer and computer network. Congress decided to introduce an Act which solely deals with computer related crimes, so they have introduced Computer Fraud and Abuse Act (CFAA), 18 U.S.C 1030 in 1986. As the crime related to computer became more sophisticated over the time the changes were made to CFAA, and the current amended version of CFAA is 2008 one, which is in implementation in United States [26].

CFAA 18 U.S.C 1030, highlight criminal act that abuses computer system. It is a law protecting the cyber space, which includes any computer that is in connection with internet, computer linked to a banking system, and federal computer.

Though this law carries in depth clauses for guarding the computer system but clauses can be applicable to the crimes related to deep web and dark web falls under the these categories.

Computer trespassing (e.g., hacking) in a government computer, 18 U.S.C. 1030(a)(3);

Computer trespassing (e.g., hacking) resulting in exposure to certain governmental, credit, financial, or computer-housed information, 18 U.S.C. 1030(a)(2);

damaging a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce (e.g., a worm, computer virus, Trojan horse, time bomb, a denial of service attack, and other forms of cyber-attack, cybercrime, or cyber terrorism), 18 U.S.C. 1030(a)(5);

committing fraud an integral part of which involves unauthorized access to a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce, 18 U.S.C. 1030(a)(4);

accessing a computer to commit espionage, 18 U.S.C. 1030(a) (1) [27]

3.3 Laws in Europe:

European Union has been active in guarding the interest of its members since 2002, and over the time it has made amendments according to needs. Currently the DIRECTIVE 2013/40/EU is enforced all over Europe. This directive bounds the member for cooperation for dealing with crimes related to computer, since these crimes are not limited to one certain premises. Moreover, the Budapest convention on cybercrime in 2001 [28] allows EU member to extend cooperation with non-members this is the reason EU and United States have a joint working group, which is working effectively and efficiently for counter the cybercrimes. This was acknowledged at the summit in 2011 held at white house United States. The joint working force is working for combating the issues pertaining to the domain names, child pornography and working on reaching

international agreement which can protect members of EU and USA [29].
The DIRECTIVE 2013/40/EU is one of the most concise and relevant laws that deals with cybercrimes across the boards. The charges are imposed on the offender by the virtue of following articles.

"Article 3: Illegal access to information systems
Article 4: Illegal system interference
Article 7: Tools used for committing offences
Article 8: Incitement, aiding and abetting and attempt
Article 9: Penalties
Article1 10: Liability of legal persons
Article 11: Sanctions against legal persons" [30].

Though this directive has mentioned the penalties according to the offenses, but it also takes in account the National laws of the countries that are member of EU.

4. Conclusion:

There is no doubt about the search that legitimate information seekers will go to any extent to get the information from web, regardless of data being available on surface web, deep web or dark web, it depends on the type of the user. It's not just the criminals who use deep web to accomplish their goals, there are many law enforcement agencies, which are using deep web or dark web for communication purposes, since it's a platform which can't be accessed by anyone, direct query is needed to be executed to get access to the information. Moreover, it provides level of anonymity which is very important for law enforcement agencies, and same goes for the criminal network using deep web or dark web. On the other hand as discussed earlier there are challenges for law enforcement agencies too, when it comes to investigation of criminal act, as the volume of deep and dark web is huge, their (site) address, name, and identity changes very frequently, it is very challenging for law enforcement agencies to target criminals, but the positive aspect for law enforcement agencies is that there are laws for this aspect of web, which can bring the criminals behind the bar. As there are pros and cons of technology this aspect has pros and cons too.

According to the opinion of author it is recommended for the users to be vigilant specifically to those who are aware of the threat of Deep web, and are working at critical positions in organisations, they should make sure that they have implemented tools and techniques within their company's infrastructure that can help them use technology safely and securely. There is very crucial role of Law enforcement agencies, cyber security experts and people dealing with technology. For Law enforcement agencies and Government, it is important to have contract and international bounding with other countries, as EU has incorporated with those who are not part of EU, so that it's easy for law enforcement agencies to carry out investigations which are across the border, as crime related to computer has no boundaries and anyone can attack Critical Infrastructure from anywhere. In addition to all this they should make custom crawler like DeWA or any tool that can fulfil the need of custom crawler, which can then be integrated with custom search engine for getting the desirable results.
For Cyber Security experts, and for the domain administrator of Government sites, bank and private companies it is recommended to make sure that they know about all the files and directories that are placed on their website, and this should be audited very frequently. So that if there is any unnecessary folder or directory or page, a proper action could be deal with it.

5. References:

[1] "Deep Web – The Ultimate Guide".(2017) DARKWEB NEWS; Available at: https://darkwebnews.com/deep-web/
[2] RILEY RAUL REESE "How Does the Dark Web Work?" (2017) Available at: https://01.media/how- does-the-dark-web-work
[3] Jamie Bartlett. "The Dark Net Inside the Digital Underworld". (2014) Wiliam Heinemann: London.
[4] Nathan Chandler "How the Deep Web works". Howstuffworks. Available at: https://computer.howstuffworks.com/internet/basics/how-the-deep-web-works.htm
[5] Open Education Database "The Ultimate

Guide to the Invisible Web" (2017) Available at: oedb.org/ilibrarian/invisible-web/
[6] F. Zhao, J. Zhou, C. Nie, H. Huang and H. Jin, & quot;SmartCrawler: A Two-Stage Crawler for Efficiently Harvesting Deep-Web Interfaces," (2016) in IEEE Transactions on Services Computing, vol. 9, no. 4, (pp. 608-620). doi:10.1109/TSC.2015.2414931
[7] G. Madhu and Dr. A. Govardhan, Dr.T.V.Rajinikanth, "Intelligent Semantic Web Search Engines: A Brief Survey," International journal of Web Semantic Technology (IJWesT) Vol.2, Issue No.1, (2011).
[8] wikiHow Staff, "How to Access the Deep Web" Available at: https://www.wikihow.com/Access-the-Deep-Web (2019) visited on 07/04/2019
[9] Debajyoti Mukhopadhyay ; Manoj Sharma ; Gajanan Joshi ; Trupti Pagare ; Adarsha Palwe, "Experience of Developing a Meta-semantic Search Engine", 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies, Pune, India (2013)
[10] Zhou Li, Sumayah Alrwais, XiaoFeng Wang, Eihal, Alowaisheq, "Hunting the Red Fox Online: Understanding and Detection of Mass Redirect-Script Injections" 2014 IEEE Symposium on Security and Privacy, (2014)
[11] Javed Ahmad Khan ; Deepak Sangroha ; Masroor Ahmad ; Md. Tanzillur Rahman, "A performance evaluation of semantic based search engines and keyword based search engines" 2014 International Conference on Medical Imaging, m-Health and Emerging Communication Systems (MedCom), Greater Noida, India. (2014)
[12] Victor Benjamin ; Hsinchun Chen, "Developing understanding of hacker language through the use of lexical semantics ", 2015 IEEE International Conference on Intelligence and Security Informatics (ISI), Baltimore, MD, USA, (2015)
[13] Krebsonsecurity, Deleted Facebook Cybercrime Groups Had 300,000 Members, Available at: https://krebsonsecurity.com/2018/04/deleted- facebook-cybercrime-groups-had-300000- members/ ,(2018)
[14] Aditya Telang, Chengkai Li, and Sharma Chakravarthy. "One Size Does Not Fit All: Toward User- and Query-Dependent Ranking for Web Databases" IEEE Transactions on Knowledge and Data Engineering, Volume: 24, Issue: 9, pp. 1671 – 1685, 2012
[15] Balduzzi M., Ciancaglini V. (Trend Micro); "Cybercrime in the Deep Web" (2015) Black Hat EU, Amsterdam
[16] Sumit Bindal, Himank Singh: "Deep Web" (March 2010), Researchgate. Available at: https://www.researchgate.net/publication/261773660_Deep_Web
[17] MarkMonitor. "Understanding the Deep and Dark Web: mitigating risk and protecting your brand" (May 2017) Available at: Lexology : https://www.lexology.com/library/detail.aspx?g=e4df a17e-9764-4ba2-b6ce-724690e0ab9d
[18] IPzen Team. "DEEP WEB AND DARKNETS: ENFORCING YOUR IP RIGHTS." (August 2016). Retrieved from ipzen: http://ipzen.com/deep-web-and-darknets-enforcing-your-ip-rights/
[19] Dr. Vincenzo Ciancaglini, Dr. Marco Balduzzi, Robert McArdle, and Martin Rösler. "Below the Surface: Exploring the Deep Web" (2015) A TrendLabsSM Research Paper
[20] Iflah Naseem, Ashirr K. Kashyap and Dheeraj Mandloi, PhD "Exploring Anonymous Depths of Invisible Web and the Digi-Underworld" (2016) International Journal of Computer Applications. (PP 21-24)
[21] Kaukab Jamal Zuberi. "Use of Cyber Space by Terrorist Organizations"; IJECI: International Journal for Electronic Crime Investigation Volume 2, Issue 1,; January-March 2018, (PP 11-16). [22] John Robertson , Ahmad Diab , Ericsson Marin , Eric Nunes , Vivin Paliath , Jana Shakarian , and Paulo Shakarian Frontmatter; "Darkweb Cyber Threat Intelligence Mining"; (2017) Cambridge University Press
[23] Brett Hawkins. "Under The Ocean of the Internet - The Deep Web"(2016) The SANS Institute

[24] Daniel Sui, James Caverlee, and Dakota Rudesill; "THE DEEP WEB AND THE DARKNET: A LOOK INSIDE THE INTERNET'S MASSIVE BLACK BOX" (2015). Wilson Center

[25] National ASSEMBLY SECRETARIAT. (2016). "Prevention of Electronic Crime Act" May 2016. Islamabad. Available at: http://www.na.gov.pk/uploads/documents/1472635250_246.pdf.

[26] H. Marshall Jarrett, Michael W. Bailie, Ed Hagen, Scott Eltringham. "Prosecuting Computer Crimes" (2015) OLE Litigation Series. Published by Office of Legal Education Executive Office for United States Attorneys.

[27] Charles Doyle "Cybercrime: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws" (2014) Congressional Research Service.

[28] Council of Europe "European Treaty Series 185- Convention on Cybercrime". (2001). Budapest http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

[29] The European Union. "Cybercrime law" Available at: https://www.cybercrimelaw.net/EU.html [30] THE EUROPEAN PARLIAMENT "DIRECTIVE 2013/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA" (2013). Official Journal of the European Union.

Tariq et al LGURJCSIT 2019

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 3 Issue 1, January - March 2019

The Evolution & Growth of Ransomware

Muhammad Arslan Tariq,
Lahore Garrison University, Lahore, Pakistan
arslan.tariq@lgu.edu.pk

Abstract:
In Information and Communication Technology, communication performs an imperative job in the present period of technology. These days, ICT is being utilized by the peoples for various purposes. For security purpose, many security techniques are taken as standard in various communication devices. As to interrupt these communications and block user access from his /her data, many advanced malwares are used in the cyber world. Ransomware is an advance type of malicious software that has the capability of interrupting and blocking the working of a computer or user access to its confidential data and certain programs till ransom amount to be paid by the user to get access data. Ransomware leaves no space for intruders, they have to pay the attackers so they could have the access of the data. There are three types of Ransomware scareware, locker and crypto ransomware. The ransomware execution is carried out through various steps distribution, infection, communication, file search, encryption and ransom demand. Ransomware has developed since 2005 and there are a few kinds of ransomware, which are continually being developed by attackers. Currently it has affected a numerous country that has main aspect as technology.

Keywords: Ransomware, Advance Malicious Software, Ransom amounts, Ransomware types

1 Introduction:

There is a possibility of occurrence of a security breach in computer network, when to damage or harm a user, a vulnerability in connection or network is utilized. Mostly there are two types of attacks, active and passive attacks. The attack is either performed actively or inactively to abduct user's data, id or money by applying a number of techniques and method.

Ransomware is some sort of advance malware which is capable of interfering in the working of computer or able to approach user's data and programs till the job is accomplished. For the access of data, a ransom amount is demanded. Ransomware is an advance malware that bolts your PC or keeps your information utilizing private key encryption until the point that you pay a payoff. That delivery is typically paid in Bitcoin. Information based coercion has been around since around 2005 yet the advancement of payoff encryption programming and Bitcoins have incredibly encouraged the plan [8].

Now a Days, a famous thing which is Ransomware is as service often called RaaS. This makes bad actors very easy to attack the systems and unlock them .Experienced hackers write ransomware code .after writing it they usually make the code available as service on the cost of Virtual money. Other less experience hacker mostly takes interest in this, reduce the effort to hack the systems and their exploiter. Ransom ware attack encrypts the system locks up. Victim has to pay to unlock the screen [5].

As Raas is new in the market but it is highly popular in cyber criminals and bad actors in this field.

So there was report in FBI according to their deep digging they came to know that somebody which was in their custody he was accused of working and getting hand dirty in BOTNET which helpful in ransomware attack, he offered $500 to send a lot of message the person. As far as Check point is concerned they have idea that at least 0.2 % have capacity to pay the bills but

there is other report and according to it in 2016 there was demand of 689USD [6].

2. Types of Ransomware

Famous types of Ransomware are as follows:

A. Cerber

Cerber is tools used for RaaS. just like many of other it is more famous and stand tall among others, it gives offline workability, it also deadly for destroying the databases. cerber is fully available to the attacker and the hackers [9].
According to statistics cerber has affected the 15000 window users in July 2016.
According to researches cyber attackers have earned roughly $195,000 in 2016 ,which is $2.3 million per annual.

B. Satan

Satan is a next level tools to for ransomware attack. Satan is only one time opened in the windows and locks the files of the windows. It is a remarkable and very notorious among the hackers. It is fully available to the public, actors behind that made it accessible to everyone but not free of cost.it has very user friendly GUI which makes him very easy to use.
According to a security advisory on PC Risk, once a system has been infected with Satan through phishing campaigns or malicious links, the malware encrypts files and tacks on the .stn extension before placing an HTML file on the desktop of compromised systems which instructs victims on their next steps[3].
Satan have HTML data have claim that locked files are highly encrypted and going back or getting them in original form is Mission Impossible.
So there is consensus among all stall word of IT that malware in the Satan is RSA-2048 and other high cryptography Do or Die only one is out there ,that is giving the money and get your data back[4].

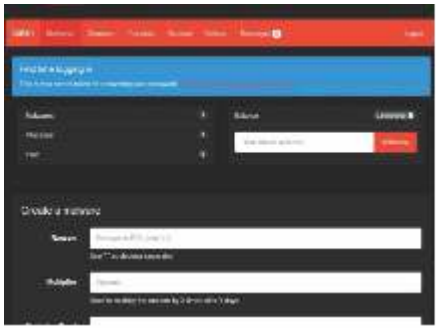


Fig.1 Satan Example

C. Hostman

Hostman is probably new sheriff in the town, it is very much effective, but hackers have to pay in order to use it. almost $49 to use unlimited. This has an extra edge for victims, it provides victims automatically decryption of files after payment. this makes victims comfortable because it's all happening runtime.it has online workability [7].

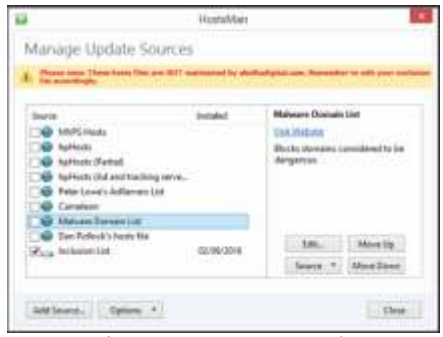


Fig.2. Hostman Example

3. Ransomware Working

The Ransomware attack is executed in six steps. The first step is distribution, it utilizes old traps of spam messages and phishing, downloads, bargained sites, social building, bot contamination, SMS message, and so on. Since distribution isn't simple, they have likewise begun utilizing Pay per Install (PPI) plans of action. In PPI demonstrate, each time ransomware programming is introduced on host delicate product, the specialist gets paid. This is a rewarding offer as digital crooks don't need to compose any code without anyone else. They just need to catch the market and convey the product to clients. The second step is 'Infection', As the malicious program/software is downloaded and installed onto user's computer (who's being victimized by that malware) or reaches the system by other means of communication, its capable of blocking user from accessing the data [7]. The third step is 'Communication', to collect the public-key required to encrypt the confidential data, the ransomware system will communicate with encryption key server. Mostly RSA, RC4 or related encryption algorithm are used. Fourth step is “File Search”, the files that have similar extensions (like PDF, PPTX, JPG etc) which are crucial and meaningful to the user are searched

through ransomware process. These files are selected by software to encrypt and claim ransom. 'Encryption' is the fifth step; the encryption of the searched and selected file is carried out through encryption key provided by the servers. Those file are replaced, renamed and again encrypted. The whole process includes changing name and extension of files and utilizing another encryption algorithm. Final step is "Ransom Demand", as the fifth step (Encryption) is completed, the computer displays a pop up and ransom amount is claimed. The user who is being victimized through this whole process left no choice rather than to pay the ransom demand. Paying ransom demand doesn't assure of the decryption key, but data recovery chances increases [3].

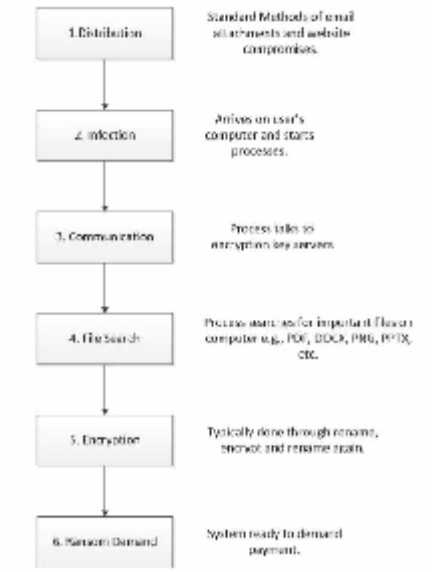


Fig.3. Ransomware Execution Steps

4. Evolution of Ransomware

Ransomware has developed since 2005 and there are a few kinds of ransomware which are continually being developed by attackers. Figure 4. demonstrates the level of new groups of fake AVs, deceiving applications, lockers and crypto ransomware distinguished somewhere in the range of 2005 and 2015 [8]. The figure 4 has a differing number of the families. It very well may be noticed that at first just crypto ransomware and deluding applications were found. Deluding applications mostly made utilization of phishing and other such exercises. Crypto ransomware couldn't make due in that time due to antivirus applications investigating and distinguishing such malware. By 2009, the deceptive applications were supplanted by phony antivirus programming programs. They would tell the client that some infection has been recognized or some issue has occurred. To redress a similar premium rendition of a paid solution is to be obtained. Compromised for security, unfortunate casualties would pay the equivalent. A similar period saw the ascent of lockers. Lockers essentially bolted the PC screen and requested that the victim make a payment with the goal that the access to the data would be given back. They didn't encode any information however rendered the PC futile to the unfortunate casualty till the payment request was satisfied. As lockers, deceiving applications and phony antivirus programming programs were being distinguished, crypto ransomware made a rebound with a more grounded encryption calculation and different families. There are such a significant number of ransomware families and variations present that it is hard to contemplate every one of them. They all incorporate some minor changes in the code with the goal that discovery isn't simple. The consistent advancement in the ransomware families is intended to handle any security highlights antivirus programming genius grams may install. Antivirus programming programs work by dissecting and making a note of ransomware families and afterward examining new downloads for a similar code. So, the creators of ransomware always make changes to the code so it won't be recognized and any key, whenever found for the past adaptations, would not work any longer [9].

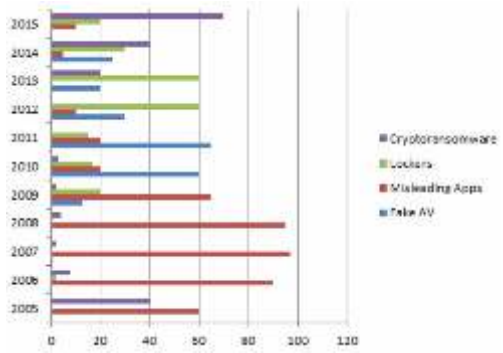


Fig.4. Percentage of New Families of crypto ransomware, Lockers, Misleading Apps & Fake AV between 2005 and 2015

5. Growth of Ransomware

The appearance of Ransomware as a benefit

(RaaB) has given a stage to individuals who couldn't build up their own ransomware yet are prepared to obtain it. These cybercriminals get paid more than the creator as they chance being gotten all the while. This has also extended the number of cybercriminals. Moreover, this has pulled in numerous people who need to obtain money viably. RaaS does not work like distinctive organizations given by the cloud. Or maybe, it is just named so in light of the way that the maker of the ransomware is simply setting up the ransomware to be used by anyone. There is a little candid portion required for acquiring the ransomware. The individual securing the result item direct offers his advantages with the maker (20%). This encourages him achieve various markets and socioeconomics without risking being gotten. It additionally uses the time accessible to him as numerous individuals are currently spreading the malware. Around 43 percent of ransomware unfortunate casualties were workers in associations. Since the appearance of ransomware, the sum requested in coercion has nearly multiplied from US$ 294 to US$679 toward the finish of 2015 to US$1077 in 2016. The sum is additionally expected to increment as blackmail sum is multiplied in the event that it isn't paid in a predefined period and information is erased after a specific period slip. Thus, revenue has expanded [5].

6. Conclusion

In the present situation of security in PC systems, vulnerabilities are being found and abused each day. Attacks are going on regular bringing about bargaining of protection and uprightness of information. Among such Attacks, a variation of assault is the utilization of pernicious programming. In spite of the fact that pernicious programming programs are of numerous sorts, they are together classified as ransomware as they request a payoff from the person in question. Numerous variations of ransomware are accessible in the market, with fluctuating qualities. To add to the blasting business of ransomware, "ransomware-as-a-benefit" (RaaB) was additionally presented. Cybercriminals are utilizing RaaS to achieve new targets and thusly, win colossal benefits. Albeit different sorts of malicious attacks can be distinguished and ceased, there is still no way to stop or recognize a ransomware attack. Just some counteractive action can be taken with the goal that PCs are not contaminated. In such conditions, familiarity with clients is of most extreme significance as social building is additionally utilized. A few analysts have endeavored to create against ransomware programming programs yet their acknowledgment and value is yet to be seen.

As ransomware is very notorious for exploitation but this news addition RaaS is very destructive because this hand it over to layman which is harmful because it will make very vulnerable and everybody will try it to earn the money. Because it billion-dollar industry and still it's growing. Making the money is very easy by using RaaS and that s cyber security expert have to go deeper in order to handle this issue.

Because it is growing very fast, earning in this is other big issue.

7. References

[1] R. Richardson and M. North, “Ransomware: Evolution, Mitigation and Prevention,” Information State Department. Kennesaw State University, GA USA, vol. 13 No. 1, 2017.

[2] H. Sultan, A. Khalique, S. I. Alam and S. Tanweer, “A Servey on Ransomware: Evolutiobn, Growth, And Impact,” in Department of Computer Scince, School of Engineering Sciences &Technology Jamia Hamdard: vol 9, No. 2, March-April 2018.

[3] G. O' Gorman, G. McDonald, “Ransomware: a growing me-nace”, White Paper, 8th November 2012, Symantec.

[4] J. Crowe, “Ransomware growth by the numbers: ransomware statistics 2017”, June 2017, Barkley.

[5] Rouse, M. (2019). What is ransomware? - Definition from WhatIs.com. [online] SearchSecurity. Available at: https://searchsecurity.techtarget.com/definition/ransomware [Accessed 6 Mar. 2019].

[6] Research, B. (2019). Cerber Ransomware: Everything You Need to Know. [online] Blog.barkly.com. Available at: https://blog.barkly.com/cerber-ransomware-statistics-2017 [Accessed 6 Mar. 2019].

[7] Researcher, J. (2019). Ransomware as a Service Princess Evolution Looking for Affiliates - TrendLabs Security Intelligence Blog. [online]

Blog.trendmicro.com. Available at: https://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-as-a-service-princess-evolution-looking-for-affiliates/ [Accessed 6 Mar. 2019].

[8] Tavares, P. (2018). Mechanics Behind Ransomware-as-a-Service. [online] InfoSec Resources. Available at: https://resources.infosecinstitute.com/mechanics-behind-ransomware-as-a-service/#gref [Accessed 6 Mar. 2019].

[9] Osborne, C. (2017). Satan ransomware-as-a-service starts trading in the Dark Web | ZDNet. [online] ZDNet. Available at: https://www.zdnet.com/article/satan-ransomware-as-a-service-starts-trading-in-the-dark-web/ [Accessed 6 Mar. 2019].

LAHORE GARRISON UNIVERSITY

Lahore Garrison University has been established to achieve the goal of excellence and quality education in minimum possible time. Lahore Garrison University in the Punjab metropolis city of Lahore is an important milestone in the history of higher education in Pakistan. In order to meet the global challenges, it is necessary to touch the highest literacy rates while producing skillful and productive graduates in all fields of knowledge.

VISION

Our vision is to prepare a generation that can take the lead and put this nation on the path to progress and prosperity through applying their knowledge, skills and dedication. We are committed to help individuals and organizations in discovering their God-gifted potentials to achieve ultimate success actualizing the highest standards of efficiency, effectiveness, excellence, equity, trusteeship and sustainable development of global human society.

MISSION

At present, LGU is running Undergraduate, Graduate, Masters, M.Phil. and Ph.D. programs in various disciplines. Our mission is to serve the society by equipping the upcoming generations with valuable knowledge and latest professional skills through education and research. We also aim to evolve new realities and foresight by unfolding new possibilities. We intend to promote the ethical, cultural and human values in our participants to make them educated and civilized members of society.

Contact: For all inquiries, regarding call for papers, submission of research articles and correspondence, kindly contact at this address:
Sector C, DHA Phase-VI Lahore, Pakistan

Phone: +92- 042-37181823
ijeci@lgu.edu.pk

Published by: Digital Forensics Research and Service Center, Lahore Garrison University