Asian Journal of Research in Computer Science

11(1): 41-48, 2021; Article no.AJRCOS.69897
ISSN: 2581-8260

Internet Crimes- it's Analysis and Prevention Approaches

Mohammad Dawood Babakerkhell[1*] and Habibullah Slimanzai[1]

[1]Department of Information Technology, Computer Science Faculty, Shaikh Zayed University, Afghanistan.

Authors' contributions

This work was carried out in collaboration between both authors. Author MDB designed the study, managed the literature review, performed the statistical analysis, wrote the protocol, and wrote the first draft of the manuscript. Author HS managed the analyses of the study. Both authors read and approved the final manuscript.

Article Information

DOI: 10.9734/AJRCOS/2021/v11i130255
Editor(s):
(1) Dr. Francisco Welington de, Universidade Federal do Piauí, Brazi.
(2) Dr. Sherin Zafar, Jamia Hamdard University, India.
Reviewers:
(1) Nour El Houda GOLEA, University of Batna 2, Algeria.
(2) Noura Al Nuaimi , UAEU, United Arab Emirates.
(3) Velu Suresh Kumar, H.H. The Rajah's College, India.
(4) Hajar Mahfoodh, University of Bahrain, Bahrain.
Complete Peer review History: https://www.sdiarticle4.com/review-history/69897

Review Article

Received 25 April 2021
Accepted 30 June 2021
Published 13 August 2021

ABSTRACT

In the present period of computerized handling, high level of online information is looked with digital threats. There are unlimited dangers and difficulties to information existence online. Cyber-attacks which are considered the emerging and serious threats that are going on each second and investigation of those dangers and threats are exceptionally hard to confine and vanquish them. Cybercrimes have a terrible effect on governmental and non-governmental organizations, educational institutions, financial banks and economic infrastructures. Numerous worldwide societies, policy makers and intelligent agencies are trying to react and control cybercrimes. One of the most serious issue in the online processing is that how to secure and deal with our day by day information against digital misrepresentation and cybercrimes. To comprehend cybercrime and save our digital assets, this paper will analyze about various cybercrimes and addresses the effective prevention and detection ways and methods used for the avoidance, controlling, detection and combatting of those crimes.

Keywords: Cybercrime; cyber security; cyber-attack; cryptography; combating; cyber analysis.

**Corresponding author: E-mail: dawood.csf@gmail.com;*

1. INTRODUCTION

In this electronic world or simply e-world, individuals can do any sort of exchange through internet. Internet is the gathering of million and billion PCs which provides a network of different electronic connections to process user's data and information. Individuals are ready to internet constantly however opposite side of the coin is cybercrimes which are delivered by web. Cybercrime or e-crime (electronic crime) is the new phenomenon in the world of digital communication and internet which is mostly caused by the cyber-attackers. It is the quickly developing dangers to advanced and cloud information. Cybercrime, cyber terrorism, computer crime, and cyber fraud are the most serious electronic terms which are mostly used in the electronic world or cyber world. From one aspect, internet and innovation is assuming a critical part in human live and it has brought a lot of facilities to them, while from the other angle, the rate of cybercrime is increasing day by day with advancement of technology and internet. It is likewise imperative to think about the digital assaults and loses which occurred over the most recent couple of years in a portion of the created nations of the world.

In 1820 first cyber-crime was recorded, in 1976 first spam e-mail has transmitted over "Arpanet" and in 1982 apple computer was firstly captured by virus when the "EIK Cloner" has designed by a high school student [1]. As indicated by the research report conducted by the Center for Strategic and International investigations (CSIS) and McAfee that the assessed rate of worldwide misfortunes from cybercrime were more than $375 billion in the year 2004. It was occurring more quickly. Ponemon Institute cites that the U.S Companies annual costs were $12.7 million in 2014 which increased to $15 million in 2015 [2].

Likewise, the numbers of breaches made another record in 2016, the Identity Theft Resource Center pointed out, in 2015 it was happened about 780 breaks which drastically expanded to 1093 in the year 2016 while the numbers of records presented came down to 37 million from 169 million in 2015. In 2016 business segment was for the most part influenced 492 breaches, human services association 378, government/military were 72 and training area was about 98 breaks. Research has declared that one of five consumers in USA has been victims of cyber-attacks in the past two years [3].

The fundamental goal of this paper is to analyze the recent scientific research articles, identify different cyber threats and provide some of the effective security approaches used for the combating of internet crimes. Crimes against small as well as large businesses and enterprises are not new. In 1995, the SBCI overview discovered 35% of retailers announcing client burglary with comparable rates for assembling and wholesaling enterprises [4]. Instead of large enterprise and corporation small companies are more vulnerable to online crimes because they do not have strong safeguard system and high combating techniques to detect and prevent suspicious activities. From one aspect, the space of internet is becoming wide and wide and from other side the rate of cybercrimes also goes up so rapidly. In order to combat cyber-crimes and prevent cyber-attacks, strong effort is required to develop sophisticated framework and design advanced architecture by using modern algorithms to control those threat over internet. The following two diagrams will clearly explain the number of complaints which were recorded from the year 2007 up to the year 2016 in the USA.

1.1 Literature Survey

As we know there are a huge number of terms used to explain crime including cybercrimes. These terms are including online crime, high-tech crime, e-crime, web crime, online fraud, information crime and cybercrime [5]. Cybercrime is a kind of crime which is used to attack on computer data and system [5]. There are different views and definitions about cybercrime or internet crime. Some defined internet crimes which include the use of computer and other argued that cybercrime is by the existence of computer [6]. It is a kind of criminal activity where computer is the basic tool. Generally, there are two factors, one is computer and another is crime. Cybercrime has more impact on any organization and society. It is very essential to use advance techniques for the prevention and detection of internet crimes. Cyber prevention, is the way of limiting, controlling, avoiding, demolishing, of avoiding cyber-attacks in any electronic system such as computer, network and internet and cyber detection is the way of detecting suspicious issues regarding those electronic systems [7]. We know that computer, internet and software applications brought huge opportunities to business companies but they also introduced various risks and crimes. A great deal of business and data organizations are

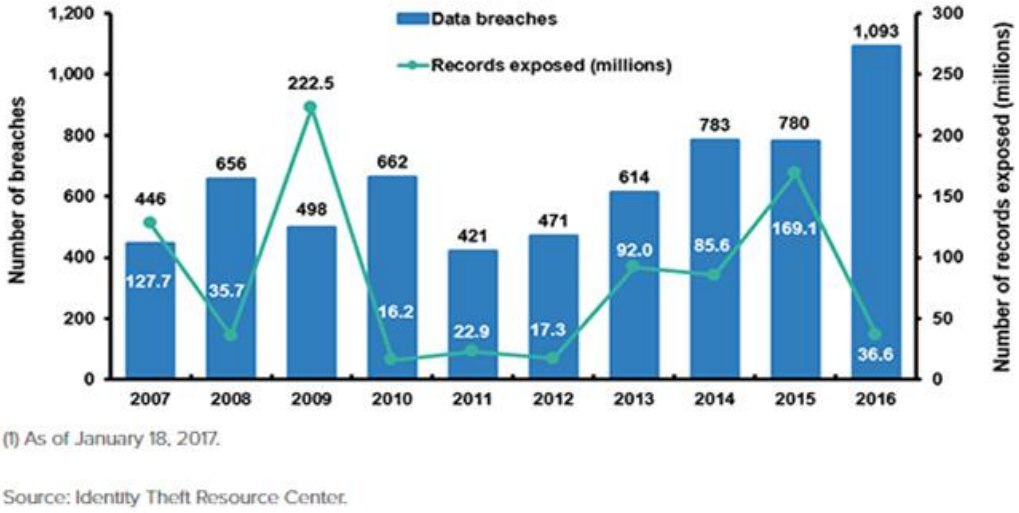

Fig. 1. Numbers of breaches from the year 2007 up to 2016

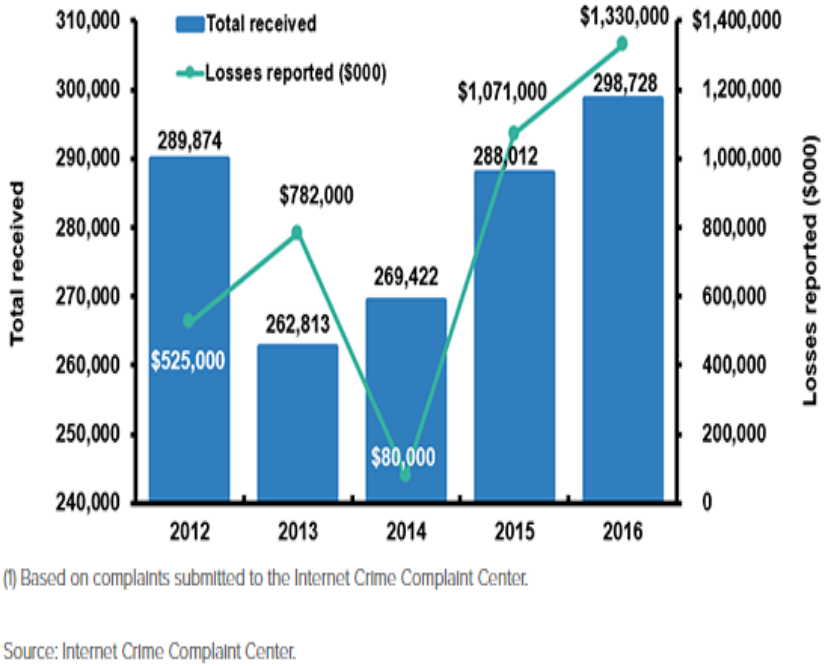

Fig. 2. Numbers of complaints from the year 2007 up to 2016

experiencing cybercrimes. As indicated by UK National Hi Tech Crime Unit (NHTCU), the estimation rate of cybercrime was almost 4.61 US$ for those organizations which were situated in UK in 2004 [8]. The primary reason of cybercrime was the lack of implementing cyber security standards [8]. Cybercrimes are the riskier and modern issues for open and private organization and large business enterprises. There are two groups of cybercrimes, the computer networks which attacks on other computer networks, example a virus or code which is used to witched off the system, the second type of crime is that when population come under the attack of computer networks, fraud, intrusion (Svensson, 2011) [9]. Essentially, cybercrime and PC crime are distinctive terms, though cybercrime includes web and system while PC crime might be included or not but rather cybercrime is utilized to characterized all [9]. Consistently we hear and encounters the new assaults which are riskier and damage to

the confidentiality, accessibility and integrity of our web. The one expansive effects and enormous concerns would be the disturbance of the overall monetary market [2].

The fast spreading of cybercrimes over the web put down all items, machines, servers, systems and so forth in danger. The well-known cybercrime mishap which was occurred at the South Carolina at the "Department of Revenue" in 2012, about 3.6 million security numbers and 387000 credit/charge cards were stolen [8]. In addition, in today's cyber world, cybercrimes are the most buzzword of any business company and organization. More development has been done against cybercrime but we still we need to work on different techniques and cryptographic structures to combat cybercrime. It is justifiable that there is a genuine requirement for the combatting of criminal exercises in the digital world.

Data can be monitored and modified by attackers from the targeted computers or any other systems over internet. It is essential to keep privacy of conversations to ensure that data cannot be read or observer during transmission by intruders. A report generated from Better Business Bureau Online (BBBO) that more than 80% online customers are faced with security problems while doing business over internet and early 75% of them are ending their shopping when credit card information is requested [10]. Sending information over internet needs strong security policy and structures. In 2009 the survey which was conducted by Identify Theft Resource Center(ITRC) in USA showed that 85% of people answered that they have deep concerns about transferring information over internet and 59% expressed that improvement is required for keeping their data secure over webpages [3]. The literature review of different articles shows that there are huge numbers of internet crime cases, happened in the digital world and the victims of those crimes are people and electronic devices. Lack of cyber security is one of the issue which open the door for online crimes to arise and broadcasted.

1.2 Types of Cyber Crimes

In today's commercial and enterprise world, there are huge numbers of cybercrime which bring more challenges and difficulties to human online data, computer and internet system [11]. These are some of the most available threats in digital world such as Hacking, Credit card fraud, Salami attack, Phishing, cyber stalking, spoofing pornography, virus dissemination, IRC crimes, Denial of service attack, SQL injection, Logic bombs, web jacking, money laundering, phishing payroll fraud and so on.

1.3 Combating Cyber Crime

There are unlimited number of methods and techniques which are to control and combat cybercrime. Different organizations use varieties of models and architectures with targeted characteristics and goals for reducing and combatting cybercrime. Multilayer security considerations including physical Security, hardware security, software security, Interpol like internetpol agency and various measures are play a major role in defeating online crime [12]. It is important to use modern techniques and new cryptographically models to prevent the developing issue of Cybercrime throughout the globe. To prevent cybercrime and reduce the rate of cyber attacking, the following specifications are required to be considered.

1.4 Legislation Enforcement

This is a critical advance towards battling digital crime. Government and other large non-government organization ought to have an exceptionally powerful enactment that stipulates the appropriate discipline for these digital lawbreakers. The issue is that most countries are not implementing laws properly and subsequently permit these digital offenders to strike from anywhere and stay undetected. In fact, right when perceived these law breakers swear off being rebuked or evacuated to a country, for instance, the US, that has made laws for arraignment. While this shows different once in a while organization, for instance, the FBI, have used misleading and subterfuge to get law breakers. Representation: Two Russian software engineers have been evading the FBI for a long time. The FBI set up a fake figuring PC situated in Seattle, Washington. They kept on goading the two Russians in the US by offering them office work in this association. Endless supply of the gathering, the suspects were caught outside their building and office [13].

1.5 Awareness

As new technological devices developing very rapidly and more individuals depend on the Internet to store their data, for example, managing an account or debit/credit cart data,

criminals are attempting to steel this data**.** Digital crime is ending up to a greater degree a risk to individuals over the world. There must be a rising mindfulness about how data is being ensured and the strategies hoodlums use to take data. The government and non-government, agencies should ensure that the general population are made to know the exercises of these crimes and how to secure their documents, frameworks, systems from unauthorized users. Additionally, anti-crime agencies must take more consideration to aware people, societies and enterprise companies.

1.6 Utilization of Cryptography

This is a strategy for keeping and delivering data in a particular manner for those who are the real recipients. cryptography joins strategies, for instance, microdots, combining words with pictures, and distinctive ways to deal with concealing information and data. Cryptography is commonly depending on two factors, an algorithm and the key. Besides that, cryptography is regularly related with scrambling plaintext (customary data) into secret message (an operation called encryption), so that it would once again (called as decryption) [13]. Individuals who sharpen this area are known as cryptographers and those who are attempting to disclose the cipher text are known cryptanalysis.

- **Confidentiality:** The information can't be fathomed by anyone for whom it was unintended.
- **Integrity:** The information can't be modified away or deliver among sender and expected beneficiary without the adjustment being perceived.
- **Non-repudiation:** The sender of the information can't deny at a later stage his or her desires in the creation or sending of the information**.**
- **Authentication:** The sender and recipient can insist each other's character and the beginning stage/objective of the information.

2. CRYPTOGRAPHY ALGORITHMS

The security of a cryptosystem relies upon the design of the algorithm. This segment investigation the cryptosystems in the fundamentals of key age, key length, square size and number of rounds utilized for encryption and decryption process. The rate at which a specific algorithm scrambles the information is a basic parameter in analyzing the performance of encryption algorithm.

2.1 Data Encryption Algorithm (DES)

DES is the most popular symmetric encryption algorithm created by IBM and received by U.S national government as a standard encryption method. DES utilizes 64 bits' plaintext pieces and a key length of 56 bits. DES utilizes the 8 bits as equality bit for blunder discovery. DES depends on Feistel structure (f) which partitions the squares into two parts, applies 16 rounds of handling to encode the information. Security in DES is a significant concern on the grounds that of the 56-bit key length and brute force attack is possible to DES [14].

2.2 Triple Des

Triple DES was proposed to override the main Data Encryption Standard (DES) calculations, which software engineers definitely made sense of how to vanquish without break-ing perspiration. At one time, Triple DES was the endorsed standard and the widely used symmetric estimation in the business world. Triple DES uses three individual keys with 56 bits each. The total key length connotes 168 bits; in any case, experts would battle that 112-bits in key quality is more like it. Despite step by step being removed, Triple DES still makes sense of how to make a dependable gear encryption answer for money related organization and different enterprises [15].

Fig. 3. Encryption and Decryption Process

2.3 RSA

RSA is an open key encryption computation and the standard for scrambling data delivered over the internet. Dislike Triple DES, RSA is asymmetric calculation count because of its usage of a paired keys. You have your open key, which is the thing that we use to encode our message, and a private key to unscramble it [13].

2.4 Blowfish

Blowfish is one more estimation proposed to override DES. This symmetric consider parts messages along with squares of 64 bits and encodes them only. Blowfish is famous for the two its massive speed and generally large sufficiency a similar number of the case that it has never been vanquished. At that point, dealers have taken the full great position of its free openness publically. It's positively one of the more versatile encryption techniques available [15].

2.5 Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is the main principle trusted as the standard by the U.S. Government and different affiliations. It is a square figure feistel structure framework. Although it is incredibly successful in 128-piece outline, AES in like manner uses keys of 192 and 256 bits for generous commitment encryption purposes. AES is commonly seen as invulnerable to all strikes, with the special instance of brute force, which tries to decode messages using all possible blends in the 128 192, or 256-piece figure. AES provides high level security because of lengthy key variables [16]. AES consists of the following operations:

- Key expansion
- Sub byte generation
- Add-round key, Column mix

2.6 Comparisons of DES, 3des, RSA, Blowfish &AES Algorithms

From the various numbers of cryptographic algorithms, the below famous algorithms in Table 1 are selected for comparison and contrast which are most effective in the field of cryptography. It is important to compare them on the bases of security, architecture, and flexibility to expand in future and cover their limitations [14]. The basic unit is security that shows how the algorithm is secure against the various cyber attackers and intruders. The algorithm structure defines the performance for example, size of block, rounds, duration of time and the length of the key are the major elements which effects the algorithm security. Block size is directly proportional to the security, if the block size is large, the algorithm will be highly secured if the block size is small it will be less secure. Another element of encryption and decryption is the round process. When the number of round increasing the strengths of security will be increased. Blowfish and DES has 16 rounds while 3DES has 48 rounds. Length of key is another important part of algorithm security. DES has a key of 56 bits while 3DES has 168 bits' key with great protection against assault. AES has variable key lengths of 128, 192, and 256 which give a bigger number of key mixes. BLOWFISH utilizes 448 piece keys which are thought to be longest and most powerful to the extent that brute force attacks are concerned. In the following Table 1 some of the important measurement for the famous cryptographic algorithm will disused.

3. DISCUSSION

The very important point is that to recognize and determine internet crimes and understand how it happened and enter to our system. Besides the above different techniques and approaches that we have discussed, the four prevention strategies, development, situational, community and criminal justification are playing an essential role regarding to online crimes. The developmental strategy is used to determine the deep cases of electronic crimes. Alarm, survelinence techniques, video supervising is done in the situational strategy. The third one related to community experiences and monitoring neighborhood activities and the last one strategy is the connection and development of relationship between societies and the law organization which is called crime justification strategy [4]. The implementation and deployment of various cryptographic algorithms like DES, AES, RSA, and etc in online transactions and processes also help to keep our information from any kind of intruders secure and stable. Individual, private and public organizations are impacted by online fraud and they have million and billion loses while doing online business and online transactions. Detection techniques are more helpful in determining suspicious activities before the crime happened. The good method for combating internet crimes are to know the crimes, deploy law and regulations and provide high security frameworks. If anyone has committed with online crime, forensic technology is the another option for checking and investigating the crimes.

Table 1. Algorithms measurement

Algorithm	Flexibility	Structure	Attacks
DES	No	Feistel	Brute Force
3DES	Yes, from 56 to 168 bits	Feistel	Brute Force Attack, Known Plaintext
RSA	Yes, Multi prime RSA	Factorization	Factoring the Public Key
Blowfish	YES,64-448 key length, multiply by 32	Feistel	Dictionary Attack
AES	Yes,256 key length, multiply by 64	Substitution-permutation	Side Channel Attack

4. CONCLUSION

It is clear that internet is as needed for our lives as food, water and electricity and the internet crime is also as danger as the traditional crime. The presented information in the paper demonstrates the significances of specialized techniques of information i.e encryption and cryptography to control digital crime and the different schema which is used for the prevention of cyber-crimes. It is also concluded that if we have powerful base of mathematics, it yields in solid cryptographic architecture and might bring about better security. The comparison of some essential and prominent cryptographic algorithms such as DES,3DES, RSA, Blowfish and AES utilized as a part of the encryption methods. The different preventative strategies through which we can manage the different threats occurred to our system. It also pointed out that asymmetric algorithms are more strong and superior than symmetric algorithm. Besides these all, governments still have an essential task to carry out, yet a large portion of the avoidance should be carried out by business corporation creating powerful software and those with the capacity to stop extortion. So more works are required for individuals, private and public organizations, enterprises, institutions to improve and enhance the existence security framework and define new model to control online crimes and attacks.

FUTURE WORK

The researchers can extend and designed modern methods and strategies based on the specialized techniques and they can get encouragement to analyze, bring, and advance these techniques by creating solid wall between the intruder, hacker and common information which is the essential of creativity, advancement and innovation. For detection, measurement and remediation of online crimes and attacks, business enterprises, software companies, educational institutional and other large organizations are required to enhance the measurement techniques for detection and prevention of internet crimes and designed more sophisticated structures to defeat internet crimes.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Srikanth TN, Aishwarya JS, Irshadn, Shruthi, B., Bhoomika, G. Y., Explicit Study On Cyber Crimes Using Internet, International Journal of Management and Applied Science, ISSN: 2017; 3(9):2394-7926.
2. HS, Rao YS, Panda TC. (n.d.). Cyber-Crimes and their Impacts: A R view. International Journal Engineering Research. 2018;2(2):2248-9622. Available:www.ijera.com
3. Sumanjit. D, Tapaswini.N, Impact of Cyber Crime:Issues and Challenges, International Journal of Engineering Sciences & Emerging Technologies, October 2013. ISSN: 22316604 Volume 6, Issue 2, pp: 142-153 ©IJESET
4. Martin B. The Impact of Crime on Business: A model for prevention, Detection and Remedy, Research gate.
5. Sultan AO, AL kaabi. Combatting computer crime: An international perspective.UAE;2010.
6. Legal Info. Crime Overview aiding and abetting or Accessory; 2009. Available:http://www.legalinfo.com/content/criminal-law/crime-overview-aiding-and abetting-or-accessory. html, Visited: 28/01/2012
7. Magallah A, Security, prevention and detection of cyber crime, Tumaini university Iringa university college;2013.
8. Available:https://www.iii.org/ fact-statistic/facts-statistics-identity theft- and-cybercrime

9. Lecure MA, Chauhan DM. (n.d.). Preventing cyber crime: study regarding awareness of cyber crime in Tricity. International Journal of Enterprise Computing and Business Systems. 2018;2(1). Available:http://www.ijecbs.com
10. Saini D, Raeo SY, Panda CT. Cyber-crimes and their impacts: A review. International Journal of Engineering Research and Application(IJERA), ISSN: 2248-9622 www.ijera.com 2012;2(2):202-209
11. Chintal LP. Study of Cyber Threat and Data Encryption Techniques to Protect National Information Infrastructure. International Journal of Research in Computer and Communication Technology, 2014;3(3). Retrieved March 10, 2018.
12. Pathak DP. Cybersecurity: Model for Cybercrime Prevention and Controlling. International Journal of Novel Research in Computer Science and Software Engineering. 2016;3(1):58-61. Available:www.noveltyjournals.com
13. Dambo I, Ezimora AO, Nwanyanwu M. Cyber Space Technology: Cyber Crime, Cyber Security and models of Cyber Solution. International Journal of Computer Science and Mobile Computing. 2017;6(11):94- 113. Available:www.ijcsmc.com
14. Hercigonia Z, Gimnazija D, Groatia V. Comparative Analysis of cryptographic algorithms. International Journal of Digital Technology & Economy. 2016;1(2):127-134.
15. Kahate A. Cryptography and network security (Third Edition ed.). Delhi, New Delhi: McGraw Hill Education (India) Private Limited; 201.
16. Gupta DH. Network Security and Cryptography. Noida, Amity University;2018-2019.

Peer-review history:
The peer review history for this paper can be accessed here:
https://www.sdiarticle4.com/review-history/69897