European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 11 , 2020

CRIME DATA ANALYSIS USING HADOOP ECOSYSTEM

PVN RAJESWARI[1], CHENNAREDDY SIRICHANDANA[2]

[1]Associate Professor, Dept of CSE, Visvodaya Engineering College, Kavali, AP, India.
Email id: phdpvnr@gmail.com

[2] PG Scholar, Dept of CSE, Visvodaya Engineering College, Kavali, AP, India.
Email id: sirichandana.chennareddy22@gmail.com

Abstract: Cybercrime is inescapable, ubiquitous, and an increasing number of related with one of a kind components and regions of crook environs. This evolution and network gave upward push to cyber area which controls and manages to provide identical possibilities and centers to all of the humans to access any kind of statistics. Due to the gradual increase of internet customers and netizens, the abusage of technology is broadening regularly which tends to cybercrimes. Cybercrime is largely an unlawful act that ends in a criminal pastime. Cyber Security, a mechanism via which laptop data and the types of equipment are covered from unauthorized and unlawful access. This paper illustrates and makes a specialty of cybercrime, its effect on society, forms of threats, and cyber safety. Nowadays Computer crime troubles and thefts have ended up especially excessive-profile, mainly those surrounding copyright.

Keywords: Infringement, Hacking, Child pornography, Child grooming and Spoofing.

1 . INTRODUCTION

Computer fraud can be an untrustworthy misrepresentation of the truth proposed to prompt some other to abstain from doing something that causes loss. Computer crime may be summarized as a crook pastime which entails statistics era infrastructure, further to unauthorized get entry to, unlawful interception, any statistics interference, laptop or structures interference, abusage of devices, forgery, blackmail, embezzlement, and some digital fraud. There exist privacy problems every time any exclusive facts or statistics are hijack or misplaced, either lawfully or otherwise. The very first crime that turned into recorded befell in 1820 in France, Joseph-Marie Jack quad, a fabric producer, produced a device particularly loom which allowed the non-stop repetition of collection of steps involved within the weaving of a few unique fabrics. This leads to a type of fear in worker's minds and they devoted sabotage. Cybercrime cells are there in states essentially to handle these crimes and to expel or punish the netizens or criminals committing any of the cybercrime. It tiers from the theft of a man or woman's identification complete disruption of a rustic's Internet and community connectivity because of large assaults throughout its networking assets. In this virtual age, on-line communication now ends up a norm, the net customers and the authorities are at an enlarged threat of becoming the bull's-eye of the cyber-attacks. Cybercrime can reason damage to any organization.

To combat the short-spreading cybercrime, governments & organizations have to have collaboration globally essentially to expand any amazing model that someway controls the threat. The net is essentially used for the betterment of life, to make humans privy to global-wide activities, complements the speed of existence as properly, and makes customers technically sturdy and up-to-the-mark. As the usage of an era is growing day-by means of-day, crime is likewise increasing progressively. It covers all of the kinds of crimes and thefts associated with laptop networks. Some of the criminals are technically expert and knowledgeable having deeper and incredible information regarding the era. Hacking of the ATM password, shifting the money through hacking the financial institution account info of the victim's account to theirs, some pornography issues, and so forth. Are some of the thefts which can be handled by using educated people? There is an urge to enforce a number of the policies and policies, to tackle and cope with these crimes governing cyber area specifically referred to as Cyber Law. Cybersafety requires worldwide co-operation to deal with the security of the cyber area. It protects computer gadgets, resources of laptop or machine, records, and statistics from any unauthorized get entry to and the disclosure. During this paper, unique types of assaults and threats are overviewed. Each assault is described firmly; class of hackers is also reviewed.

2. CYBERCRIME

Digital generation is encompassing in all walks of existence, everywhere in the world, and has brought the real meaning of globalization. At the only stop cyber device presents a possibility to speak and at the opposite stop, some individuals or communities make the most its electricity for crook functions. Criminals exploit the Internet and different community communications which are worldwide in scope. The situation is alarming; Cybercrime is upcoming and is speaking of the city in every subject of the society/system. Theoretically and almost this is a new problem for researchers and is growing exponentially. A lot of work has been performed and countless need to be move because the invention or up-gradation of the recent era leads to the technical crime i.E. The digital or we can say the cybercrime or e-crime. This is due to the fact each day a new method is being evolved for doing the cybercrime and often we are not having the proper investigating method/ version /approach to address that new cybercrime. In the prevailing-day global, India has witnessed a remarkable index of cybercrimes whether or not they pertain to Trojan attacks, salami attacks, electronic mail bombing, DOS attacks, facts robbery, or the most common offense of hacking. Despite technological measures being adopted by corporate agencies and people, we have witnessed that the frequency of cybercrimes has improved over the last decade. Since customers of a pc system and internet are increasingly global in the big range each day, where it is easy to access any data without difficulty within a few seconds by way of the usage of the internet that's the medium for big statistics and a huge base of communications round the arena. Certain precautionary measures must be taken by everybody while the use of the internet to help in difficult this major threat cybercrime. In this paper, we have discussed various classes of cybercrime and cybercrime as a danger to character, assets, government, and society and we've got recommended numerous preventive measures to be taken to snub the cybercrime

3. CYBER CRIME AND SECURITY

1. In this numerous assault together with phishing, Denial of Service (DOS), Botnets, Malware, and plenty of greater and describing methods to avoid such attacks with the aid of installing antivirus and firewalls. As we understand not all antivirus can prevent all assaults and further we also cannot build a device that could prevent all describe assaults. So, we are trying to simulate and save you DOS assaults where an attacker will ship a large number of requests to

the server, and the server will get busy in processing such huge request facts and get crashed and services to regular customers might be denied. To overcome such difficulty, we will connect a community packet display to a server which will inspect all incoming request and if the request size is in server processing limit then it will ahead request to a server in any other case screen will discard the request to save the server from getting crash and from DOS assault.

2. To monitor community traffic, we have used the Bigdata Hadoop MapReduce programming version to evaluate all packet requests and then tell the server whether or not a request is a normal packet size or attack. MapReduce will study enter packets after which take a look at whether or not request length is in server potential or now not and if a request is in server capability then report may be ahead to a server for storage else discarded.

3. To enforce this venture, we've designed three modules

4. Server module: In this module server will run in a countless loop and await customer request and if the consumer sends any facts then it'll acquire and keep it and if the clientship request to download a document then the server will ship that file lower back to the patron.

5. Network Monitor module: This is a MapReduce software to check out all incoming packets and then analyse them and if all packets are server potential restrict then it'll ahead packets to a server for storage else discard them.

6. Three) User's module: This is a simulation module in which users will send the request to a server for file upload or download if any malicious person ship the massive size of a file then the network display will discard such file from storage at a server.

4. SYSTEM ARCHITECTURE

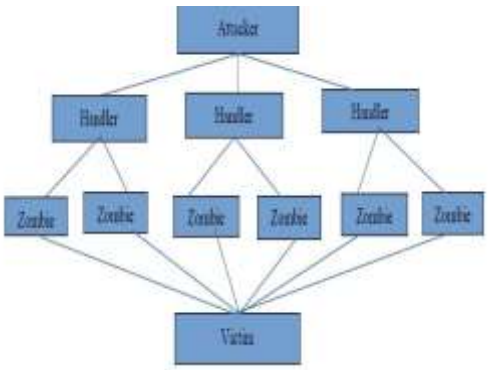


Fig 1: System Architecture

5. EXISTING SYSTEM

Cloud structures may be used to permit records sharing competencies, and this may provide numerous benefits to the consumer and enterprise whilst the information is shared in the cloud. Since many users from various agencies make a contribution to their statistics to the Cloud, the time and value can be less compared to the manual exchange of facts. Google Docs affords information-sharing abilities as agencies of college students or groups running on a venture can share documents and may team up with each other effectively. This lets in

higher productiveness compared to previous strategies of regularly sending updated variations of a report to participants of the institution via electronic mail attachments. People are waiting for statistics sharing functionality on their computer systems, phones, and laptop, and so forth. People like to share their data with others such as their own family, colleagues, pals, or the world. Students additionally get gain whilst working on institution projects, as they can group up with contributors and get work performed successfully.

6. PROPOSED SYSTEM

In this proposed gadget commonplace temp secret is shared to lessen the statistics leakage from cloud storage in big information. To minimize safety and privacy risks some limits have been supplied that are time limit, length limit, and credit score point limit. Information turned into encrypted to provide extra protection (AES, DES set of rules). The temp key can be utilized by an individual who requests to retrieve data for once. If other than the request man or woman tries to apply temp key, then that secret is eliminated, and alert notification maybe ships to records proprietor. Temp key provider sends the important thing to the requesting person with the aid of mail the usage of the SMTP protocol. (Gmail -high comfy) The main gain of the proposed system is to split and commercial enterprise etc. That manages massive statistics global need to be polished in future.

7. MODULES

1) **Server module**: In this module server will run in infinite loop and wait for client request and if client send any data then it will receive and store it and if client send request to download a file then server will send that file back to client.
2) **Network Monitor module**: This is a MapReduce application which will inspect all incoming packets and then analyses it and if all packets are server capacity limit then it will forward packets to server for storage else discard it.
3) **User's module**: This is a simulation module where users will send request to server for file upload or download; if any malicious user sends huge size of file then network monitor will discard such file from storage at server.

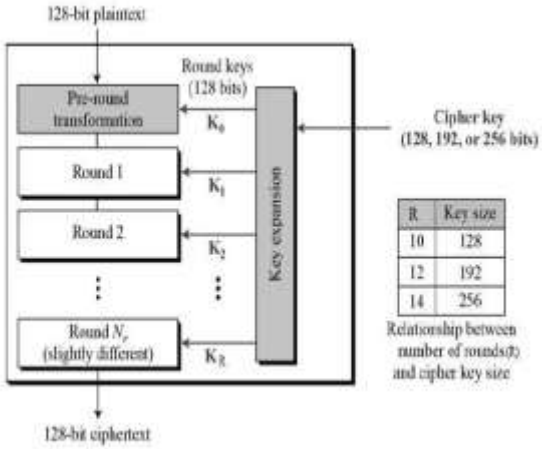
1. AES ALGORITHM

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The schematic of AES structure is given in the following illustration



R	Key size
10	128
12	192
14	256

Fig 2: Encryption Process

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below figure 3. .

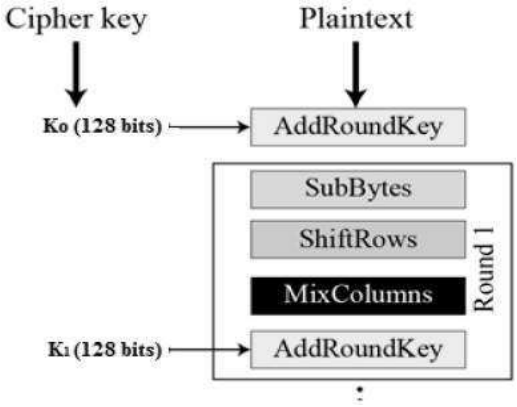


Fig 3:Each round steps in Encryption process

Byte Substitution (SubBytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

Shift rows

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows −

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

MixColumns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes,

which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

Addroundkey

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round

Decryption Process

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order

- Add round key
- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms need to be separately implemented, although they are very closely related.

8. OUTPUTS

Fig 4: Server Machine

Fig 5: User Machine

Fig 6: File Uploaded to serve

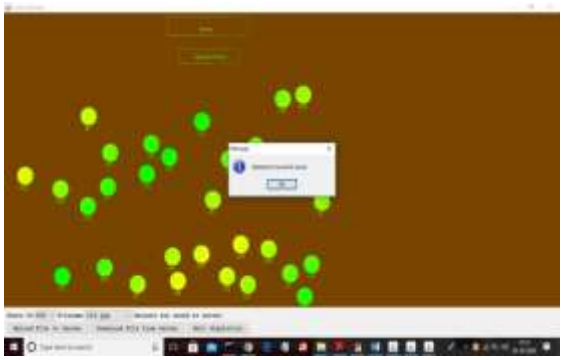


Fig 7: .txt file uploaded at Server

Fig 8: Status for Network Monitor

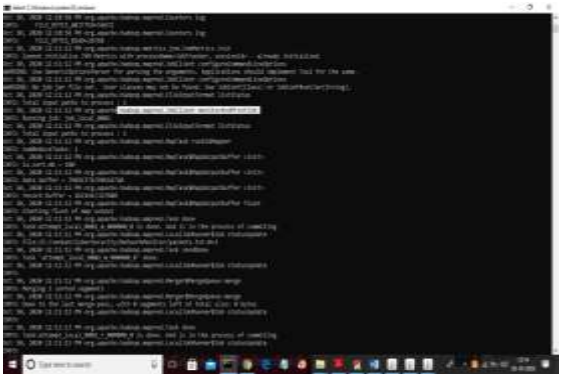


Fig 9: Map Reduce Monitoring Job

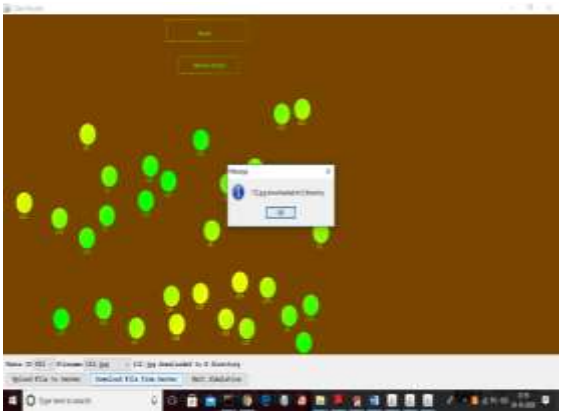


Fig 10: The uploaded file is downloaded successfully

Fig 11: Graph that represents the packet type and count of the packets

9. CONCLUSION

In this modern generation of technology, the position and usage of the internet are growing worldwide swiftly, therefore it turns into clean for cybercriminals to get admission to any statistics and statistics with the assist of their expertise and their know-how. Cybercrime is an unlawful act or a risk that wishes to be tackled firmly and efficiently. There is a want to create extra consciousness many of the people and, customers of the net about the cyber area, diverse sorts of cybercrime and a few preventive measures as "Prevention is continually better than therapy", so it is significantly cautioned to take some previous precautions at the same time as working the net. Security in recent times is becoming an outstanding and major concern. In the subsequent paper, some protection issues are introduced, threats, Trojans, and assaults over the internet. Computer protection will become vital in many of the era-driven industries which operate on laptop systems. Computer security is not anything extra than pc protection. Countless vulnerabilities and computer or network-primarily based issues are acts as a crucial a part of preserving an operational industry

References

[1] Pooja Aggarwal , Neha, Piyush Arora , Poonam "Review On Cyber Crime And Security", IJREAS, Vol. 02, Issue 01, Jan 2014.

[2] Ammar Yassir and Smitha Nayak, "Cybercrime: A threat to Network Security", IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.2, February 2012.

[3] Atul M. Tonge, Suraj S. Kasture, Surbhi R. Chaudhari, "Cyber security: challenges for society- literature review", IOSR Journal of Computer Engineering (IOSR-JCE) , Volume 12, Issue 2 (May. - Jun. 2013), PP 67-75.
[4] C. Catlett (ed.), "A Scientific Research and Development Approach to Cyber Security", Report submitted to the U.S. Department of Energy, December 2008.
[5] Seema Vijay Rane & Pankaj Anil Choudhary, April 2012-September 2012, "Cyber Crime and Cyber Law in India", Cyber Times International Journal of Technology and Management, Vol. 5 Issue 2.
[6] Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. London: Academic Press, 2011: Pp. 5-19.
[7] Richards, James. Transnational Criminal Organizations, Cybercrime, and Money Laundering: A Handbook for Law Enforcement Officers, Auditors, and Financial Investigators. Boca Raton, FL: CRC Press, 1999: Pp. 21-54.
[8] Ravi Sharma, Study of Latest Emerging Trends on Cyber Security and its challenges to Society, International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1 ISSN 2229-5518 IJSER © 2012.
[9] BinaKotiyal, R H Goudar, and Senior Member, A Cyber Era Approach for Building Awareness in Cyber Security for Educational System in India Prothixene, IACSIT International Journal of Information and Education Technology, Vol. 2, No. 2, April 2012.
[10] B.T. Wang and H. Schulz Rinne, "An IP traceback mechanism for reflective DoS attacks", Canadian Conference on Electrical and Computer Engineering, Vol. 2, 2-5 May 2004, pp. 901 – 904.

Author's Profile:

PVN Rajeswari, has received her B.Tech in CSE from Andhra University and M.Tech degree in CSE from Andhra University in 2004 and Allahabad University in 2006 respectively. Presently she is pursuing PhD from Andhra University. She is dedicated to teaching field from the last 14 years. She has guided 22 P.G and 41 U.G students. Her research areas included Artificial Intelligence and Data Mining. At present she is working as Associate Professor in Visvodaya Engineering College, Kavali, Andhra Pradesh, India.

Chennareddy Sirichandana has received her B.Tech Degree in Computer Science & Engineering from Sri Venkateswara College of Engineering, affiliated to JNTUA in 2018 and Pursuing M.Tech degree in Computer Science & Engineering in Visvodaya Engineering College, Kavali, affiliated to JNTUA, Ananthapur in 2021.