INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

THREAT DETECTION AND DEFENCE MECHANISM IN CRIMINOLOGY USING DATA MINING

C. Jayapratha[1], Dr. J. M. Gnanasekar[2]

[1]Research Scholar, Bharathiar University, Coimbatore, Tamilnadu, India.
[2] Professor, Department of Computer science, Sri Venkateswara College of engineering, Sriperumbudur, Kancheepuram, Tamilnadu.

Abstract: - In the recent database storage systems with trending devices that handles big data in distributed file system used efficiently in tamilnadu criminology system. Nowadays in the digital world huge data from our internet oriented system takes backups for all our pictures, videos and documents etc. backups could be taken even for searches made by us, chats and phone call records. Thus we require detection and defendant algorithm for threats based on these backups taken. In prevailing big data storage system overall management and accessing of unlimited data storage has random read and write access towards them which will be less flexible. In our algorithm we provide metadata that refers the redundant messages and links them instead of having multiple copies occupying the data storage space. Thus by eliminating redundant data we can afford huge storage space, time efficiency and cost efficiency. Our chief purpose is to detect the attack or threat contents in the backup storage space and defend them by providing secured storage space. More than a cybercrime which will be taken action after the threat has taken place by searching criminal threats in the backup storage of big data database server detects and defends efficiently.

Keywords: Criminology database system, distributed file system, detection and defendant algorithm, metadata, redundant messages

1. Introduction

Advancements in information technology have raised considerations concerning the risks to knowledge associated with weak IT security, as well as vulnerability to viruses, malware, attacks and compromise of network systems and services. Inadequate IT security might lead to compromised confidentiality, integrity, and availability of the info thanks to unauthorized access. To make sure that individual privacy remains rigorously Protected, native and state education agencies ought to implement progressive info security practices [1].

More than the ever-evolving threat of a knowledge breach needs diligence on the part of the education community in understanding and anticipating the risks. In short outlines crucial threats to instructional knowledge and knowledge systems [2].

Threats area unit divided into 2 categories: technical and non-technical. A short description of every threat is followed by a suggestion of applicable risk mitigation measures. As a rule, a corporation will greatly scale back its vulnerability to security threats by implementing a comprehensive privacy and knowledge security set up.

Some organizations don't have a long time security architecture in situ, feat their networks prone to exploitation and also the loss of personally identifiable information [3].

At times, thanks to an absence of resources or qualified IT staff, organizations' networks area unit connected to the net directly, or area unit connected mistreatment out-of-the-box network appliances with default configurations connected, with no extra layer of protection.

This is necessary to notice that having a firewall alone isn't adequate to ensure the safety of a network [4].

Inadequate network protection leads to exaggerated vulnerability of the info, hardware, and package, as well as condition to malicious package (malware), viruses, and hacking. If the network contains sensitive info or PII, such as students' Social Security numbers, it's crucial that even during very restricted resource setting, minimal user, network and perimeter security protection mechanisms (such as anti-virus) area unit implemented, as well as ensuring that anti-virus package is correctly designed [5].

Robust security design is crucial and provides a roadmap to implementing necessary knowledge protection measures. Computers run a range of package Applications, as well as older versions of that will generally contain vulnerabilities which will be exploited by malicious actors [6].

Maintaining with package updates and upgrades, additionally to applying manufacturer-recommended patches, minimizes several of the vulnerabilities.

To scale back the flexibility of malicious actors to compromise or destroy associate degree organization's security system, implement a sturdy patch management program that identifies vulnerable package applications and frequently updates the package security to make sure in progress protection from massive threats [7].

2. Database Handling and Backup Storage

Malicious code often transferred to a pc through browsing web pages that haven't undergone security updates. Therefore, merely browsing the net and visiting compromised or unsecured websites might end in malicious software system being downloaded to an organization's computers and network [8].

To stop threats from compromised websites, use firewalls and antivirus software to assist establish and block probably risky web content. Any computer connected to the network, whether or not at work or at home, that doesn't follow configuration management policy, is prone to an attack. Weak knowledge security protection measures that don't prohibit that machines will hook up with the organization's network create it susceptible to this kind of threat. Establish a configuration management policy for connecting any hardware to the network. The policy ought to specify security mechanisms and procedures for numerous kinds of hardware, together with computers, printers, and networking devices. The implementation of a Network Access management resolution to enforce configuration policy necessities use of mobile devices, like laptops or hand-held devices, including smart phones, is exploding; but, the flexibility to secure them is insulation behind [9].

The case is sophisticated by the actual fact that these devices are typically accustomed conduct work outside the organization's regular network security boundaries. Knowledge breaches will occur in an exceedingly range of ways: devices are often lost, stolen, or their securities are often compromised by malicious code invading the OS and applications. to market knowledge security just in case a tool is lost or taken, code knowledge on all mobile devices storing sensitive data (i.e., knowledge that carry the danger for harm from an unauthorized or unintended disclosure). Till additional encryption, user authentication, and anti-malware solutions become accessible for mobile devices, the most effective protection strategy is to implement a strict mobile device usage policy and monitor the network for malicious activity. Empowerment the majority of information protection services to a 3rd party shifts enterprise security design.

In cloud computing, as an example, giant amounts of client data are keep in shared resources, which raise a range of information cryptography and convenience issues. Further, the cloud supplier faces an equivalent knowledge security responsibilities and challenges as the organization that owns the information, as well as mending and managing their applications against malicious code.

3. Threat Detection Algorithm Implementation

An insider is outlined as somebody with legitimate access to the network. Because information accessed by insiders are often simply taken, copied, deleted, misfiled, or changed, insider threats are often a number of the foremost damaging, despite whether or not they occur thanks to user carelessness or malicious makes an attempt. To mitigate this kind of threat, establish and enforce a well-defined privilege rights management system, limiting users' access to sure info and permitting them to solely perform specific functions. Audit programs are helpful in imposing access controls and monitoring suspicious activity. Additionally, it's counselled that organizations conduct annual coaching and awareness programs to teach users regarding corporate executive threats. Implementing a policy on robust user passwords is crucial to knowledge protection. It is particularly necessary for users with access to the foremost sensitive info.

Modern password-cracking programs will simply break weak passwords, like those containing common words or word teams found in an exceedingly wordbook. For this reason, user-selected passwords are usually thought-about to be weaker than randomly-generated passwords. User-generated passwords typically follow a foreseeable pattern or association to one thing within the user's life (city, family, or pet names for example) and additional susceptible to password-cracking programs. Whereas randomly-generated passwords could also be tougher to recollect, they are relatively safer. Lack of a strong knowledge backup and recovery resolution puts an organization's knowledge in danger and undermines the effectiveness of its IT operations.

Data and system recovery capabilities permit a company to cut back the danger of harm related to a data breach. It's essential to conduct routine backups of crucial knowledge and store backup media in a safe and secure manner. Paper documents, like reports and catalogues, could contain sensitive data. Unless these documents square measure destroyed properly (for example, by shredding or incinerating), they will be salvaged and misused. Discarded electronic devices, such as computers or moveable drives, that are utilized in process and storing sensitive knowledge,
remain vulnerable unless the information erased properly. An information breach will occur if recovery tools are accustomed extract improperly erased or overwritten knowledge.

In our algorithm we provide metadata that refers the redundant messages and links them instead of having multiple copies occupying the data storage space. Thus by eliminating duplicate data we can afford huge storage space, time efficiency and cost efficiency. Our chief purpose is to detect the attack or threat contents in the backup storage space and defend them by providing secured storage space. More than a cybercrime which will be taken action after the threat has taken place by searching criminal threats in the backup storage of big data database server detects and defends efficiently. Backup storage should be scrutinized consistently for contents prone to threat or attacks. Any type of criminal activities like theft, murder, sexual abusive videos etc can be detected from the backup storage in external servers thus avoid any type of criminal attacks using photos, videos etc.

4. Conclusion

Hackers are planning malware to be a lot of subtle than ever. Through packing, encryption, and polymorphism, cyber criminals are able to disguise their attacks to avoid detection. Zero day threats and advanced malware simply lapse antivirus solutions that are just too slow to retort to the constant stream of rising threats. Organizations of all sizes want an answer that leverages an exemplary approach to security from the network to the end. Thus we propose a threat detecting mechanism that handles data mining and provide security in database. It also finds the data that are prone to attacks and the records will be used for detecting any types of criminal activities from the scrap level

.

REFERENCES

[1] Randazzo, M., Keeney, M., Kowalski, E., Cappelli, D. M., & Moore, A. P. (2005). Insider threat study: Illicit cyber activity in the banking and finance sector. TECHNICAL REPORT CMU/SEI- 2004-TR-021.

[2] Rogers, M. (2003). The role of criminal profiling in the computer forensics process. Computers & Security, pp. 292-298. Schultz, E. (2002).

[3] A framework for understanding and predicting insider attacks. Computers & Security, pp. 526-531. Schultz, E., & Shumway, R. (2001).

[4] Incident response: a strategic guide to handling system and network security breaches. Indianapolis: Sams. Shaw, E., & Fischer, L. (2005).

[5] Ten Tales of Betrayal: The Threat to Corporate Infrastructure by Information Technology Insiders Analysis and Observations. DEFENSE PERSONNEL SECURITY RESEARCH CENTER. Shaw, E., Ruby, K. G., & Post, J. M. (1998).

[6] The Insider Threat to Information Systems. Security Awareness Bulletin. Issue 2 , pp. 170–186. iii Solarz, A. (1987).

[7] Computer-related embezzlement. Computers & Security. Volume 6. Issue 1 , pp. 49–53. Taylor, R., Caeti, T., Loper, K., Fritsch, E., & Liederbach, J. (2006).

[8] Digital crime and digital terrorism: Chapter 3 - The Criminology of Computer Crime. Pearson/Prentice Hall. Trzeciak, R., Moore, A. P., Cappelli, D. M., Caron, T. C., & Shaw, E. (2009).

[9] Insider Theft of Intellectual Property for Business Advantage: A Preliminary. 1st International Workshop on Managing Insider Security Threats (pp. PP. 1-22). West Lafayette: Purdue University.