INTRUSION DETECTION & PREVENTION SYSTEM

[1]Yash Abhangrao, [2]Saurabh Isankar, [3]Sakshi Pawar, [4]Bhagwati Dudhkar
GUIDE: Prof.I.M.SHAIKH

PUNE VIDYARTHI GRIHA'SCOLLEGE OF ENGINEERING AND S.S. DHAMANKAR INSTITUTE OF MANAGEMENT, NASHIK

***Abstract*– In today's interconnected world, organizations rely on shared storage spaces to facilitate seamless collaboration among employees. However, ensuring the security of sensitive data in such an environment is of paramount importance. To address this challenge, we propose an Intrusion Detection and Prevention System designed for organizations where multiple employees have access to shared data. This system is equipped with a multi-layered authentication process to ensure data security. Each registered employee is granted access to a common storage space, and the system permits them to view data belonging to other users without providing access. To access data, a user must successfully complete a stringent three-tier authentication process, which includes email OTP, mobile OTP, and security questions. This multifaceted approach significantly enhances the security of data access. The Intrusion Detection and Prevention System continuously monitors authentication attempts. If a user fails in any one of the authentication steps, the system swiftly identifies this as a potential intrusion. In such cases, the system automatically triggers an alert and sends an email to the user whose data is being accessed without proper authentication. This email contains a change of password request, prompting the legitimate user to take immediate action to secure their account. Our system not only provides robust data protection but also ensures that intrusion attempts are promptly detected and mitigated, preventing unauthorized access and safeguarding the sensitive information stored within the organization. This abstract highlights the key features and benefits of our enhanced Intrusion Detection and Prevention System, which is essential in modern, collaborative work environments to maintain data security and privacy**

***Keywords*: Intrusion Detection and Prevention System Shared storage spaces Data security Multi-layered authentication Email OTP, Mobile OTP, Security questions.**

Published in IJIRMPS (E-ISSN: 2349-7300), Volume 11, Issue 6, Nove-Dec 2023

INTRODUCTION

In today's highly interconnected world, where organizations increasingly rely on shared storage spaces to facilitate seamless collaboration among employees, ensuring the security of sensitive data has become a paramount concern. With the proliferation of digital assets and the constant flow of information within an organization, it has become imperative to develop robust systems that protect against potential intrusions. To address this pressing challenge, we propose an advanced Intrusion Detection and Prevention System tailored for organizations in which multiple employees have access to shared data repositories. This system is designed with a multi-layered authentication process to ensure data security, offering a comprehensive approach that significantly enhances the safeguarding of critical information. This introduction sets the stage for understanding the significance of the proposed system in the context of modern collaborative work environments and the imperative need for data security and privacy.

LITURATURE SURVEY

Caiming Liu; Yan Zhang, "An Intrusion Detection Model Combining Signature-Based Recognition and Two-Round Immune-Based Recognition,"[1] 2021 - This paper examines In order to effectively utilize the advantages of the signature-based intrusion detection methods and immune- based intrusion detection

methods, an intrusion detection model combining signature-based recognition and immune- based recognition is proposed in this paper. The numerical data features of intrusion detection are defined. A numerical matching method based on sub features is designed. The feature recognition mechanism for detecting classic intrusions is realized. An intrusion detection method based on two-round immune recognition for antigens that miss detection is proposed. Immune principles are used to define the elements of intrusion detection and simulating the evolution process of immune elements. The collaborative intrusion detection mechanisms of feature recognition, the first-round and second- round immune recognitions are proposed. In this paper, a simulation experiment is carried out on the intrusion detection data set KDDCUP'99. The experimental results show that the proposed model has the common advantages of signature- based recognition and immune-based recognition, has effective intrusion detection capability

Zakiyabanu S. Malek, "User behavior Pattern -Signature based Intrusion Detection,"[2] 2020 – Technology advancement also increases the risk of a computer's security. As we can have various mechanisms to ensure safety but still there have flaws. The main concerned area is user authentication. For authentication, various biometric applications are used but once authentication is done in the begging there was no guarantee that the computer system is used by the authentic user or not. The intrusion detection system (IDS) is a particular procedure that is used to identify intruders by analyzing user behavior in the system after the user logged in. Host-based IDS monitors user behavior in the computer and identify user suspicious behavior as an intrusion or normal behavior. This paper discusses how an expert system detects intrusions using a set of rules as a pattern recognized engine. We propose a PIDE (Pattern Based Intrusion Detection) model, which is verified previously implemented SBID (Statistical Based Intrusion Detection) model. Experiment results indicate that integration of SBID and PBID approach provides an extensive system to detect intrusion.

Xinnan Cai, "A comparative study of machine vision-based rail foreign object intrusion detection models,"[3] 2023 - Due to the lack of track foreign body intrusion dataset, classical target detection models are rarely used in the field of foreign body intrusion on railway tracks, and model comparison experiments are also insufficient. Aiming at these problems, this paper makes a comparative study on the application of yolov5 and fast RCNN in railway foreign object intrusion detection. First, the train and test dataset was established by image preprocessing, data cleaning and data labeling of UAV aerial images. Second, the canny edge detection algorithm combined with Hough transform was used to extract the track features for delineating the detection area. Finally, Yolov5 and fast RCNN, two widely used models, were used to train and test respectively based on our dataset for comparative studies. Experiment results show that YOLOv5 has better comprehensive performance in detection rate and detection speed, and Faster RCNN model cannot meet the requirements of real-time detection of track foreign objects intrusion

AIM & OBJECTIVES

Increasing Collaboration: Enhancing data security is essential to enable organizations to collaborate effectively while keeping their valuable data safe from breaches.

Customer Trust: Motivation stems from the desire to protect sensitive customer information, ensuring their trust and loyalty remain intact

Financial Impact: The financial cost of data breaches is staggering, and it includes not only direct losses but also costs associated with recovery, legal actions, and reputation management. Our project aims to mitigate these financial impacts.

Employee Productivity: Secure collaboration tools improve employee productivity and job satisfaction.

Protecting National Interests: In sectors such as defense, healthcare, and critical infrastructure, data security is a matter of national interest. Our project contributes to the protection of vital national assets.

MOTIVATION

The motivation behind the development of our Intrusion Detection and Prevention System stems from the ever-evolving landscape of modern business operations and the critical importance of data security in this context. In today's interconnected world, organizations of all sizes rely on shared storage spaces and collaborative work environments to streamline productivity, foster innovation, and enhance communication among employees. However, this increased connectivity also brings forth a heightened risk of unauthorized access, data breaches, and cyber threats. The exponential growth of digital data and the prevalence of sensitive information within organizations have made it imperative to proactively address these security challenges.

Our project is motivated by the need to create a robust and proactive solution that not only protects sensitive data but also detects and mitigates potential intrusion attempts swiftly, thereby safeguarding the integrity and privacy of vital organizational information. By providing enhanced data security in a collaborative work environment, our system aims to empower organizations to embrace modern ways of working without compromising the confidentiality and integrity of their data assets.

APPLICATION:

- Corporate Environments
- Government Agencies
- Educational Institutions
- Healthcare Industry
- E-commerce Platforms
- Cloud Service Providers

SYSTEM ARCHITECTURE

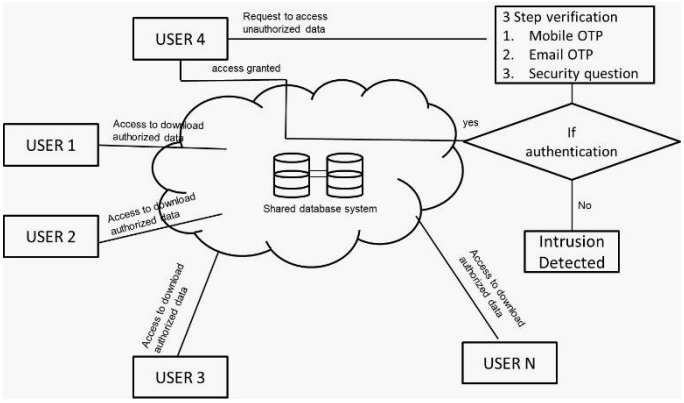

Fig -1: System Architecture Diagram

ADVANTAGES

- Enhanced Data Security
- Real-Time Intrusion Detection
- User-Friendly Interface
- Scalability
- Compliance Features
- Integration Capabilities

.

FUNCTIONAL & NON-FUNCTIONAL REQUIREMENTS

Functional Requirement:

System Feature:

1. User Registration and Authentication: Users must be able to register for the system. A multi-layered authentication process, including email OTP, mobile OTP, and security questions, should be implemented for user access.

2. Data Storage and Access: The system should provide a secure shared storage space for registered employees. Users must be able to upload, download, and manage their data within this storage space.

3. Intrusion Detection: Continuous monitoring of authentication attempts for unusual patterns or failures.

4. Password Change Request: An email with a change of password request should be automatically sent to the affected user when an intrusion is detected.

Nonfunctional Requirements

Security:

Security 1. All sensitive data stored in the various components of the system must be encrypted before they are stored. 2. The system must be able to use facility of qualified electronic signature of all documents uploaded in the system. 3. System must support appropriate security controls, including user roles with pre-

defined access rights which control the data and functionality each user has access to. 4. For all sensitive communications with clients, communication protocols with encryption must be used. 5. System must provide anti-virus protection. 6. System must be protected against known security threats.

Auditability

1. For critical system events (e.g. tender bid submission, auction bid submission, etc.), System must support methods with which the sender of data can be provided with evidence of delivery. Such evidence will be implemented by means of e-Mail. 2. System must be able to audit all system and user actions. System should ensure that all actions performed on received/stored data are recorded, keeping track of actors, date/time, input/output data and any other information necessary to allow specialized personnel to monitor and fully reconstruct a transaction.

Extendibility:

1. System must be built in a modular approach that will allow the addition of new functional modules without impacting the overall system functionality. The need for this SW type of architecture is to allow the development of the system by different SW vendors, to avoid possible lock-downs or delays in system implementation and deployment cycle.
2. System must be based in an architecture that will allow the addition of extra

Portability:

1. System must be designed in a manner that will not be coupled to any hardware specific technologies.
2. System must be possible to be deployed on different HW and SW infrastructures and not dependent on the software technology used for implementation. However, it is preferable to be implemented in one of the major and proven technology.

Performance System must follow state-of-the-art interoperability standards so that its integration or communication with external systems can be achieved. System should be developed following Service Oriented Architecture (SOA) and Open standard architecture. System needs to be developed in a way that will allow the creation and support of 'Web Services' to exchange information between the system and external systems.

SYSTEM REQUIREMENTS

Software Used:

1. Operating System : Windows xp/7/8/10
2. Software Version : Python 3.10
3. Tools : Notepad++ /pycharm/VScodeF rontEnd : Django

Hardware Used:

1. Processor - Pentium IV/Intel I3 core
2. Speed - 1.1 GHZ 3. RAM - 512 MB (min) 4. Hard disk - 20 GB 5. Keyboard - Standard Keyboard 6. Mouse - Two or Three Button Mouse 7. Monitor - LED Monitor

CONCLUSION

In conclusion, the development of the Intrusion Detection and Prevention System for multi-user data sharing environments represents a significant step toward fortifying data security in modern organizations. This project introduces a multi-tiered authentication process, real-time monitoring, and automated alerting mechanisms to ensure the protection of sensitive information while enabling efficient collaboration. By addressing the shortcomings of existing systems, it significantly enhances user accountability and safeguards shared data. The proposed system's user-friendly interface, scalability, and compliance features make it well-suited to the dynamic needs of today's workplaces. As the digital landscape evolves, this project not only offers a robust solution for data security but also holds the potential to adapt to emerging technologies and regulations, ensuring its relevance and efficacy in an ever-changing environment. Ultimately, the Intrusion Detection and Prevention System empowers organizations to strike a balance between data accessibility and security, assuring the privacy and integrity of their data assets.

REFERENCES:

1. Caiming Liu, An Intrusion Detection Model Combining Signature-Based Recognition and Two-Round Immune-Based Recognition, 2021 17th International Conference on Computational Intelligence and Security (CIS).
2. Zakiyabanu S. Malek, User behavior Pattern -Signature based Intrusion Detection, 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)
3. Xinnan Cai, A comparative study of machine vision-based rail foreign object intrusion detection models, 2023 IEEE 3rd International Conference on Power, Electronics and Computer Applications (ICPECA)
4. Jiyong Li, Network Intrusion Detection Algorithm and Simulation of Complex System in Internet Environment, 2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA)