AVE Trends in Intelligent Computing Systems

Defend and Secure: A Strategic and Implementation Framework for Robust Data Breach Prevention

K. Daniel Jasper* **and M. N. Jaishnav**
Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India.
dk9127@srmist.edu.in, jm5101@srmist.edu.in

Mansura Ferdous Chowdhury
Department of Computer Science and Engineering, North East University Bangladesh, Sylhet, Bangladesh.
mansurafcr@neub.edu.bd

Rahman Badhan
Department of Computer Science and Engineering, Sichuan University, Chengdu, China.
mrrbadhan2018@stu.scu.edu.cn

R. Sivakani
Department of Artificial Intelligence and Data Science, Dhaanish Ahmed College of Engineering, Chennai, Tamil Nadu, India.
sivakani13@gmail.com

*Corresponding author

Abstract: A data breach is an event that results in confidential, private, protected or sensitive information being exposed to a person not authorized to access it. A security architecture has been introduced to prevent data breaches. Security alerts play an essential role. Availability of the organization after the alert prevents more damage or financial loss to the organization. Incident response and overall monitoring of unwanted access and performing vulnerability tests often to enhance the data security. This framework introduces technologies and proactive measures to avoid data breaches. Intrusion Detection Systems (IDS). These systems monitor network and system activities, analyzing patterns and behaviours to detect anomalies that may indicate a security incident. Rules can be defined on the firewall based on the necessity and security policies of the organization. From the perspective of a server, network traffic can be either outgoing or incoming. Modern cybersecurity relies on Intrusion Prevention Systems (IPS) to detect and stop network threats. IPS blocks unwanted access, attacks, and exploits in real-time, unlike intrusion detection systems. When an unauthorised attacker activates the canary tokens tool, security emails the authorised person with the message set as a parameter to secure data and avoid incident response management.

Keywords: Cybersecurity Attacks; Distributed Denial-of-Service (Ddos); Intrusion Detection Systems; Intrusion Prevention System; Incident Response; Vulnerability and Firewall; Monitoring and Compliance.

Cite as: K. D. Jasper, M.N. Jaishnav, M. F. Chowdhury, R. Badhan and R. Sivakani "Defend and Secure: A Strategic and Implementation Framework for Robust Data Breach Prevention," *AVE Trends In Intelligent Computing Systems*, vol. 1, no. 1, pp. 17 –31, 2024.

Journal Homepage: https://avepubs.com/user/journals/details/ATICS

Received on: 21/08/2023, **Revised on:** 11/10/2023, **Accepted on:** 19/11/2023, **Published on:** 05/03/2024

1. Introduction

Data breaches represent a pervasive and complex challenge in the rapidly evolving information technology landscape. The ubiquity of digital data, combined with sophisticated cyber threats, has placed organizations, governments, and individuals at

Copyright © 2024 K. D. Jasper *et al.*, licensed to AVE Trends Publishing Company. This is an open access article distributed under CC BY-NC-SA 4.0, which allows unlimited use, distribution, and reproduction in any medium with proper attribution.

an ever-increasing risk of unauthorized access, disclosure, or theft of sensitive information. A data breach occurs when an entity's confidential or protected data is compromised, jeopardizing that information's privacy, integrity, and security. This multifaceted issue encompasses many incidents, from malicious cyberattacks to inadvertent human errors, with potentially severe consequences for individuals and entities alike. A data security breach occurs when unauthorized individuals or groups, such as hackers or cybercriminals, access sensitive information held by an organization. Some confidential information accessed and stolen by bad actors during a data breach includes corporate assets and personally identifiable information (PII) like social security numbers (SSN), credit card numbers, email addresses, and other personal data.

A data breach occurs when unauthorised individuals gain access to someone else's data. Information leaking or data breach are synonyms. Any data can be collected, including sensitive information pertaining to health, businesses, or other areas. Someone could take advantage of it, whether on purpose or by accident, to hurt you financially or personally. Nowadays, data breaches are among the most common types of cyber-attacks. To hone their craft, many aspiring hackers test these kinds of attacks. Damage to the company's or an individual's reputation, as well as the company's customers, might result from a data breach.

2. Methods of Data Breaches

2.1. Social Engineering Attack

Malware Attacks: Malware attacks involve malicious software like viruses, worms, or ransomware. These programs exploit vulnerabilities to compromise systems and steal or encrypt data. Common infection vectors include phishing emails and unsecured downloads. Preventive measures include robust antivirus software and regular system updates. Effective cybersecurity strategies require a combination of prevention, detection, and response. Their types are viruses, worms, trojans, and ransomware, and their impact includes unauthorized access, data encryption, or destruction.

Phishing Attacks: Phishing is a deceptive cyber-attack that uses emails, messages, or websites. Attackers impersonate trustworthy entities to trick individuals into divulging sensitive information. Common methods include deceptive links, fake login pages, and urgent requests. Recognizing red flags, such as misspellings and suspicious URLs, helps in prevention. Prevention involves user education, email filtering, and multi-factor authentication, and their types are Email phishing, spear phishing, and vishing (voice phishing). Impact is a deceptive technique to trick individuals into divulging sensitive information.

Ransomware Attacks: Ransomware is malicious software that encrypts data, demanding payment for decryption. It spreads through malicious email attachments, infected websites, or software vulnerabilities. Once infected, files become inaccessible until a ransom is paid to the attacker. Preventive measures include regular backups, software updates, and robust cybersecurity practices. User awareness and training are essential to recognize and avoid ransomware threats. Characteristics are Malicious software that encrypts data demanding payment for decryption keys, and Impacts are data encryption, financial losses, and operational disruption.

SQL Injection: SQL injection is a cyberattack where malicious SQL code is injected. Attackers exploit vulnerabilities in input fields to manipulate database queries. This can lead to unauthorized access, data manipulation, or deletion. Prevention involves using parameterized queries, input validation, and proper access controls. Regular security audits help identify and mitigate potential SQL injection risks. Methods include injecting malicious SQL queries into input fields, and Impacts involve unauthorized access to databases and retrieval of sensitive information.

Cross-Site Scripting (XSS): Cross-Site Scripting (XSS) is a cyber attack injecting malicious scripts into websites. Attackers exploit vulnerabilities to deliver scripts executed by unsuspecting users' browsers. This can lead to unauthorized access, session hijacking, or data theft. Prevention includes input validation, output encoding, and implementing secure coding practices. Regular security audits help identify and address potential XSS vulnerabilities. Methods include injecting malicious scripts into web applications, and impacts include compromised user data and unauthorized access to web resources.

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks: Denial-of-Service (DoS) is a cyber attack that overwhelms a system and disrupts service. Distributed Denial-of-Service (DDoS) involves multiple sources, intensifying the attack's impact. Attackers flood the target with traffic, rendering services unavailable to legitimate users. Mitigation strategies include traffic filtering, load balancing, and distributed server networks. DDoS attacks can be financially motivated, politically driven, or used for extortion. Methods include overloading systems with traffic to disrupt service, and impacts include service disruption, system unavailability, and diversion of resources.

2.2. Insider Threat

Insider threats pose a significant risk to organizational security, involving individuals who exploit their access for malicious purposes. These threats can be categorized into two main types: malicious insiders, driven by motives such as revenge or

financial gain, and negligent insiders, who unintentionally compromise security through negligence or lack of awareness. Activities associated with insider threats include unauthorized access, data theft, sabotage, and espionage. Mitigation strategies include strict access controls, continuous monitoring, employee training, and establishing insider threat programs. Balancing security measures with respect for employee privacy remains a challenge in addressing this complex and evolving threat landscape.

3. Objective

A data breach occurs when unauthorised individuals gain access to someone else's data. Information leaking or data breach are synonyms. Any data can be collected, including sensitive information pertaining to health, businesses, or other areas. Someone could take advantage of it, whether on purpose or by accident, to hurt you financially or personally. Nowadays, data breaches are among the most common types of cyber-attacks. To hone their craft, many aspiring hackers test these kinds of attacks. Damage to the company's or an individual's reputation, as well as the company's customers, might result from a data breach.

3.1. Steps to perform a breach

Collecting target information is the first stage in conducting a data breach because it will aid in subsequent actions. An organization's cybersecurity budget, customer preferences, and the specific hardware and software used by the organisation are all pieces of information that these attackers collect (Figure 1).

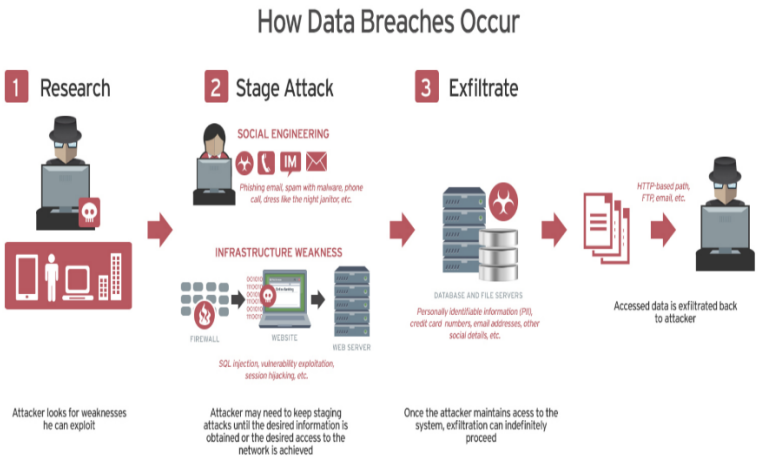

Figure 1: How Data Breaches Occur [12]

4. Review of Literature

Some confidential information accessed and stolen by bad actors during a data breach includes corporate assets and personally identifiable information (PII) like social security numbers (SSN), credit card numbers, email addresses, and other personal data.

Raja and Ravi [1] evaluate the efficacy of Software Defined Network (SDN) based prevention of phishing attacks in cyberspace using deep machine learning with the Cantina approach (DMLCA). It assesses the performance of this approach in mitigating phishing attacks, a prevalent cyber threat. The study explores the effectiveness of SDN coupled with deep machine learning techniques, specifically the DMLCA, in detecting and preventing phishing attempts. The results highlight the potential of SDN-based prevention strategies in enhancing cybersecurity defences against phishing attacks. Overall, the paper contributes to the understanding of innovative approaches for combating cyber threats, particularly in the context of phishing, and underscores the importance of leveraging SDN and deep learning technologies for proactive defence measures.

Rao et al. [2] introduce a heuristic technique for detecting phishing websites, employing a TWSVM (Twin Support Vector Machine) classifier. The focus may be on enhancing the accuracy of phishing detection using a heuristic approach, which involves leveraging domain-specific knowledge or rules. The TWSVM classifier is likely applied to analyze features or patterns associated with phishing websites. The research contributes to the field of cybersecurity by proposing an innovative method for identifying and mitigating the threat of phishing attacks.

Tan et al. [3] discuss a graph-theoretic approach for identifying phishing web pages. Graph theory, a mathematical framework, may be employed to model relationships among various elements on web pages. The focus is likely on developing a method or algorithm to detect phishing attempts based on these graph models. The approach may involve analyzing the structure or connections within web content to distinguish legitimate from malicious pages. Such research contributes to enhancing cybersecurity measures, particularly in the context of web-based threats like phishing.

Ali & Malebary [4] introduce a novel approach to improve intelligent phishing website detection by employing Particle Swarm Optimization (PSO) for feature weighting. The focus is likely on optimizing the contribution of different features to enhance the accuracy of phishing detection algorithms. The utilization of PSO suggests a method for dynamically adjusting the importance of features in the detection process. This research contributes to cybersecurity by proposing an intelligent and adaptive method to improve the effectiveness of phishing website detection systems.

Haynes et al. [5] present a lightweight approach for detecting phishing URLs on mobile devices utilizing natural language processing (NLP) transformers. It addresses the challenge of identifying phishing links efficiently on resource-constrained mobile platforms. The study explores the application of NLP transformers to analyze URL text content and extract features indicative of phishing behaviour. Results demonstrate the proposed method's effectiveness in accurately detecting phishing URLs while minimizing computational overhead on mobile devices. Overall, the paper contributes to advancing phishing detection techniques tailored for mobile platforms, enhancing cybersecurity measures for smartphone users.

Barraclough et al. [6] introduce intelligent cyber-phishing detection methods for online environments to enhance cybersecurity measures against phishing attacks. It explores innovative approaches to detect and mitigate phishing threats using intelligent algorithms and techniques. The study emphasizes the importance of proactive measures in safeguarding online users from phishing attempts. Results indicate promising outcomes in detecting and preventing phishing incidents, contributing to improved cybersecurity resilience. Overall, the paper underscores the significance of intelligent cyber-phishing detection systems in bolstering online security.

Zhang et al. [7] explored SMAKA, a secure many-to-many authentication and key agreement scheme for vehicular networks. It addresses the complex authentication and key management needs in vehicular communication, enhancing security and ensuring safe and efficient vehicle data exchange.

Shukla et al. [8] examine the impact of data breaches on firm performance, particularly focusing on stock market reactions. Through empirical analysis, it investigates how data breaches influence stock market reactions and firm value. The study sheds light on the financial consequences of data breaches, providing insights into their implications for firm performance. Results suggest that data breaches significantly negatively affect firm value, highlighting the importance of cybersecurity measures in protecting shareholder interests. Overall, the paper contributes to understanding the financial repercussions of data breaches and underscores the need for robust cybersecurity strategies.

Kim et al. [9] conducted a meta-analysis to investigate the impact of data breaches on organizational reputation. By synthesizing findings from multiple studies, the cumulative effects of data breaches on organizational reputation across various industries and contexts are explored. The study provides insights into the magnitude and consistency of the impact of data breaches on organizational reputation. Results suggest that data breaches significantly and detrimentally affect organizational reputation, highlighting the importance of effective reputation management strategies post-breach. Overall, the paper contributes to understanding the broader implications of data breaches on organizational image and stakeholder perceptions.

Ji & Guo [10] examine the relationship between data breaches, strategic disclosure, and firm value in the U.S. market. Through empirical analysis, it investigates how firms strategically disclose information about data breaches and their impact on firm value. The study sheds light on the dynamics of strategic disclosure practices following data breaches and their implications for firm performance. Results suggest that firms strategically manage the disclosure of data breaches to mitigate negative impacts on firm value. Overall, the paper provides insights into the strategic response of firms to data breaches and their effects on market valuation.

Jasper et al. [11] strongly enhance data security with encryption protocols, new algorithms, and multi-factor authentication implementations to improve data security from brute force attacks. Multi-factor authentication is a useful method of strengthening authentication to avoid brute force attacks and make a strong layer of protection. Cryptographic Algorithms Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it. By substituting the alphabet and numerals and managing a key manually, only authorized persons can use it to make the data more protected and private. The second verification includes A steganography technique that involves hiding sensitive information within an ordinary, non-secret file or message so it will not be detected.

5. Proposed Method

5.1. Implementing Strategies to Reduce Social Engineering Attacks

The layered methodology is used to prevent and add security to the database management so that attackers and other cyber threat risks add security features to the overall architecture of the security measure implemented. This method is used to detect unwanted events that occur in the network using (IDS). Certain parameters are set so that only authorized persons can access the data (FIREWALL). Monitoring security alerts and preventing high risk with the organization's policies and prevention methods (IPS). Steps can be taken to prevent data loss using (DLP) concept. Hence, the overall security architecture with the block diagram (Figure 2).

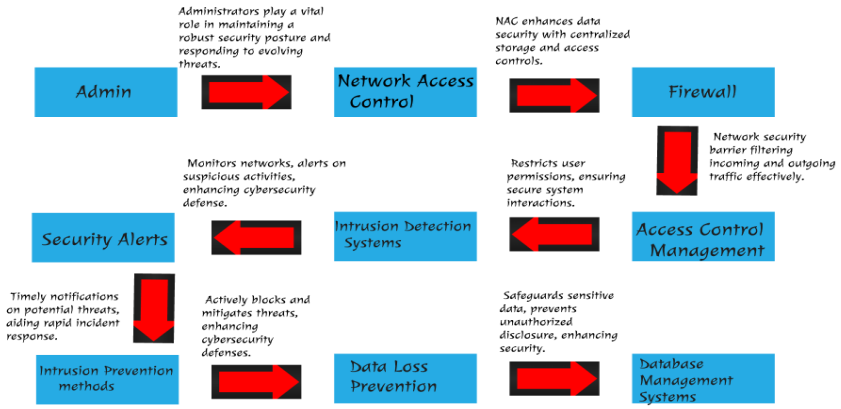

Figure 2: Security Architecture Protecting from Data Breaches

All these layers are connected to form a strong data security force and protect from data breaches. Continuous monitoring involves systematically observing networks, systems, and applications to detect irregularities, potential security incidents, or vulnerabilities. This proactive approach allows security teams to identify unauthorized activities, unusual patterns, or signs of compromise in real time. Monitoring encompasses various aspects, including network traffic analysis, log file analysis, and endpoint monitoring. Incident response is a structured approach to managing and mitigating the impact of a security incident. It involves well-defined processes and procedures to identify, contain, eradicate, recover from, and learn from security incidents. A well-established incident response plan is crucial for minimizing the damage caused by a security breach. Incident response teams, often comprised of cybersecurity experts, follow predefined protocols to investigate and remediate security incidents.

5.2. ADMIN

The role of an administrator in cybersecurity is crucial for protecting against data breaches. Administrators, often called system administrators or IT administrators, perform various tasks to ensure the security and integrity of an organization's data. Here are some key responsibilities of administrators in the context of data breach prevention: Admins control user access to systems, networks, and sensitive data. Strong access controls, including user authentication and authorization, help prevent unauthorized access and potential data breaches. Admins set up monitoring tools to track system activities and generate logs. Analyzing these logs helps detect anomalies, potential security incidents, or unauthorized access, enabling a swift response to mitigate risks. Admins play a key role in developing and testing incident response plans (Figure 3).

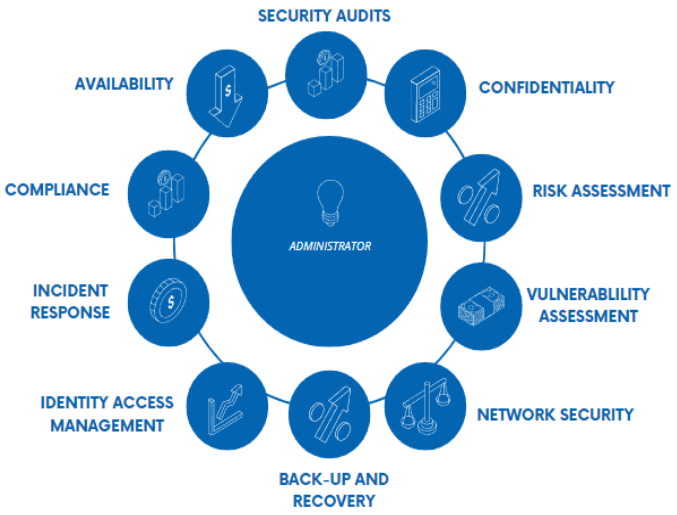

Figure 3: Lifecycle of an Administrator

5.3. Network Access Control

Network Access Control (NAC) is a critical component of modern cybersecurity strategies, designed to manage and secure the access of devices to a network. The primary goal of NAC is to ensure that only authorized and compliant devices gain entry to the network, preventing unauthorized access and mitigating potential security risks. NAC operates by enforcing security policies based on factors such as user identity, device health, and security posture. Before granting access, NAC systems assess the compliance of connecting devices with predefined security policies, checking for up-to-date software, antivirus protection, and adherence to network guidelines. If a device meets the required criteria, it is granted access; otherwise, it may be placed in a restricted or quarantined network segment.

5.4. Components of Network Access Control Scheme

Restricted Access: It uses authentication and authorization control to limit who can access the network. For instance, the user needs authorization to access a protected resource on the network.

Network Boundary Protection: It keeps an eye on and manages how networks connect to other networks. Controlled interfaces, intrusion detection systems, and antivirus software are all part of it. Perimeter defence is another name for it. An example of this would be the firewall's ability to block external, unauthorised access to internal network resources.

Algorithm

1. Authenticate the access the network
   Authenticate ("Network information = True or False")
   If user(network_infomation = true)
   Return ("ACCESS GRANTED")
Else,
   Return ("ACCESS DENIED")
2. Security posture assessment checking for updates firewall enforcement, operating systems
3. Access policy enforcement to determine whether access should be granted or denied
4. results,
   If user = network_information ("ACCESS GRANTED")
   If user =! network_information ("ACCESS DENIED")

5.5. Firewall

Firewalls can be either software-based or hardware-based, and their primary function is to monitor all traffic entering and leaving a network. It decides whether to accept, reject, or remove the traffic based on a predefined set of security standards. Proceed with accepting or rejecting the traffic or with blocking it and responding with an "unreachable error" Do not respond;

instead, block the traffic. In order to prevent unauthorised access from untrusted networks like the Internet, a firewall is set up to separate protected internal networks from the outside world.

Algorithm

1. Set IP, port number, packets, protocols, src_ip, dst_ip

    allowed_ip = 192.168.x.x

    allowed_port = xxx

    allowed_protocol = xxx

2. Define firewall type (packet):

  If IP in packet:

    src_ip = packet [IP].src

    dst_ip = packet [IP].dst

    src_port = packet [IP].src.port

    dst_port = packet [IP].dst.port

3. Add Firewall rules:

    if src_ip, src_port == allowed_ip, allowed_port:

        Access (Traffic Allowed from src_ip to dst_ip)

    else:

        Access ("Traffic Blocked")

5.6. Access Control Management

Access Control Management is a fundamental aspect of information security that strategically regulates access to computer systems, networks, and sensitive data within an organization. This multifaceted discipline encompasses various policies, processes, and technologies to ensure that only authorized individuals can access specific resources while preventing unauthorized users from compromising critical information's confidentiality, integrity, and availability. At its core, Access Control Management is about defining and enforcing rules and restrictions regarding user permissions and system interactions. This involves specifying who can access what resources, under what conditions, and in what manner. Role-Based Access Control (RBAC) is a commonly employed framework in which access permissions are tied to roles, facilitating efficient management by associating user responsibilities with specific roles rather than individual permissions.

One key element of Access Control Management is Authentication, which verifies the identity of users or systems attempting to gain access. This process often involves using usernames, passwords, multi-factor authentication (MFA), or biometric methods to ensure that individuals are who they claim to be. Authorization complements authentication by determining the level of access granted to authenticated users. This involves defining permissions and privileges based on roles, responsibilities, or specific attributes. Access control lists (ACLs) and policies are commonly used to delineate the scope of access for users or systems, ensuring that each entity operates within predefined boundaries. Security Information and Event Management (SIEM) solutions aggregate and analyze log data from various sources, offering insights into access patterns and anomalies that may indicate security risks. This layered approach contributes to overall data integrity, reduces the risk of unauthorized access, and supports compliance with regulatory standards (Figure 4).

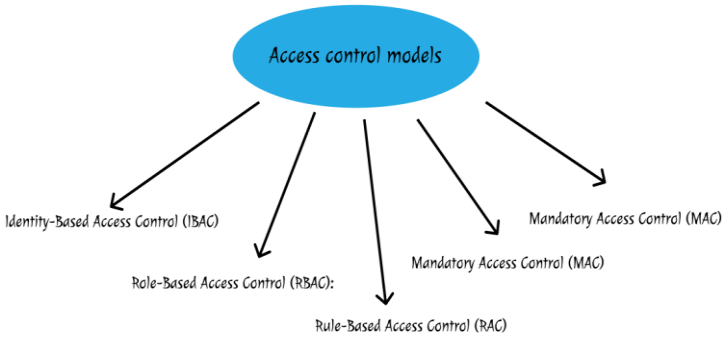

Figure 4: Access Control Models

5.7. Intrusion Detection Systems

When an intrusion detection system (IDS) detects suspicious activity in a network, it immediately notifies the appropriate parties. Security software can detect and prevent malicious activities or policy breaches on a network or system. Intrusion Detection Systems (IDS) keep an eye out for any suspicious behaviour on a network and prevent unauthorised users, even those within the company, from gaining access to the network. A classifier or prediction model that can differentiate between "bad connections" (intrusions/attacks) and "good connections" (normal connections) is the goal of the intrusion detector learning challenge.

5.8. Network-based Intrusion Detection Systems (NIDS)

NIDS monitors network traffic for unusual patterns or anomalies that may indicate a security threat. It analyzes network packets in real-time and compares them against predefined signatures or behavioural baselines. It triggers an alert if it detects suspicious activity, such as known attack patterns or deviations from normal behaviour.

5.9. Host-based Intrusion Detection Systems (HIDS)

Individual hosts or devices in a network are the primary emphasis of HIDS. Among other host-specific tasks, it keeps an eye on system logs and file integrity. Intrusion detection systems (HIDS) are able to identify harmful activity, like insider threats or attacks on individual systems, that could otherwise go undetected at the network level. It allows you to see specific actions taken by each host at a finer level.

Algorithm:

1. Detect intrusion from packets:

```
Detect_intrustion(packets):
    if, malicious_activity(packets):
        return ("INTRUSION DETECTED")
    elif,
        abnormal_behaviour(packets):
            return ("ABNORMAL ACTIVITY DETECTED")
    else,
        return false
```

5.10. Security Alerts

Security alerts are notifications generated by security systems and tools to inform organizations about potential threats, vulnerabilities, or suspicious activities within their information technology infrastructure. These alerts are crucial in maintaining an organisation's security posture by providing timely information that allows for rapid response and mitigation of potential risks. Effectively managing security alerts involves prioritizing and responding to them based on severity and relevance. Security teams analyze alerts to determine the nature of the threat, assess its potential impact, and initiate appropriate

incident response measures. Automated responses or playbooks are often implemented to streamline the handling of routine alerts, while more complex or severe incidents may require manual intervention. Regularly reviewing and fine-tuning alerting mechanisms is essential to maintain a proactive and effective security posture (Figure 5).

Algorithm:

Step 1: Create a canary token of your choice

Step 2: Enter the mail id in which you the alert triggers

Step 3: Copy and paste the token and attach the token

Step 4: Place it where the attacker couldn't find it

Step 5: When the data is been attacked

Step 6: Security alerts are made

6.1: Else

Step 7: Your data is free from attackers

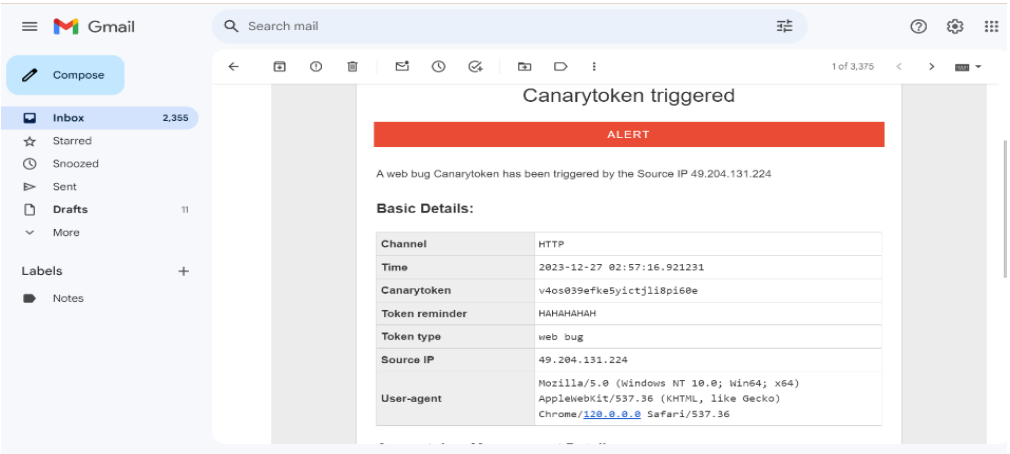

Figure 5: Security Alert

5.11. Intrusion Prevention Systems

An Intrusion Prevention System (IPS) is a vital component of modern cybersecurity, designed to proactively identify and thwart potential security threats within a computer network. Unlike intrusion detection systems that solely flag suspicious activities, IPS immediately prevents unauthorized access, attacks, or exploits in real-time. Deployed strategically within a network's architecture, IPS monitors incoming and outgoing traffic, inspecting packets for malicious content and responding swiftly to mitigate risks. IPS's continuous monitoring, adaptability, and rapid response capabilities make it indispensable in safeguarding networks and critical digital assets from evolving cybersecurity challenges.

Algorithm:

1. Monitor database activities for anomalous

    If any anomalous occur,

        Return ("Respond to Intrusion")

    Else,

        Return ("sleep")

2. Prevention methods would take place if anomalous enter

3. Responding to intrusion:

Block source_ip()

Log_attempt()

Notify_admin (“Intrusion Detected”)

Update firewall_rules

5.12. DLP Algorithms and Mechanisms

Content Inspection: DLP uses content inspection algorithms to analyze data for patterns, keywords, or regular expressions that match predefined criteria. This ensures that sensitive information is detected, regardless of the file format.

Contextual Analysis: Contextual analysis considers the context in which data is used. For example, DLP systems may analyze the relationship between a user’s role and the data type they are attempting to access or share.

Fingerprinting and Hashing: DLP may use fingerprinting or hashing mechanisms to create unique identifiers (hashes) for specific files or data patterns. This allows the system to recognize sensitive data despite minor modifications.

Machine Learning and Behavior Analytics: DLP solutions may incorporate machine learning and behaviour analytics to understand normal data usage patterns. Deviations from these patterns can trigger alerts or enforcement actions.

Database Scanning: DLP systems can scan databases to identify and protect sensitive information. This involves using algorithms to recognize data patterns associated with sensitive content. Implementing DLP requires a holistic approach, combining policy definition, user education, and technology solutions to safeguard sensitive data effectively. The algorithms and mechanisms used in DLP systems are designed to adapt to evolving threats and provide organizations with proactive protection against data breaches.

5.13. Database Management

Securing data stored in databases is crucial for protecting sensitive information and preventing breaches. Several key security measures are essential to ensure data confidentiality, integrity, and availability in a database (Figure 6).

Algorithm:

1. Monitoring the data base in case of any unwanted access

2. User authentication:

Authenticate_user (username, password)

If user credentials = vaild (username, password)

Return (“Access granted to the database”)

Else,

Return (“Access failed”)

3. Security alert triggered:

Security_triggered (protocol, time, date, dst_port, src_port, permitted, failed, event type”)

Log security message is triggerd to the administrator

security_msg (“SECURITY ALERT” <detail> <event type>”)

4. Encrypt and decrypt the data inside the database

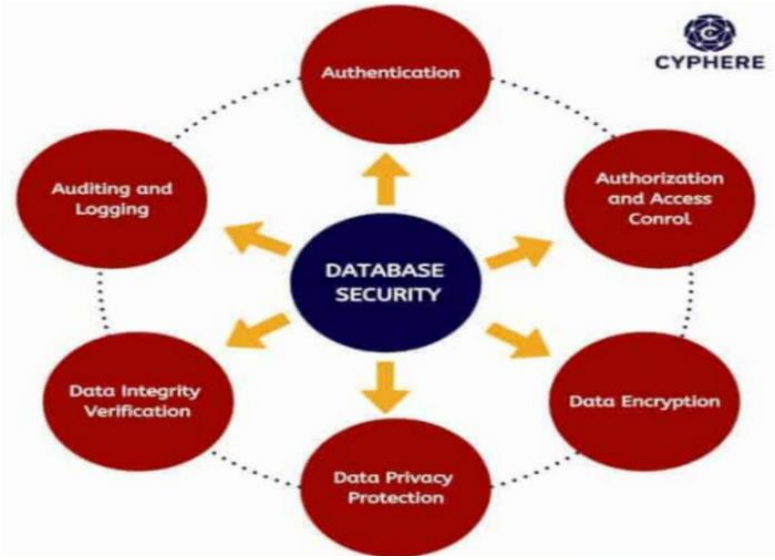

Figure 6: Database Security [13]

6. Future Scope

The future scope for improving data breach prevention involves embracing advanced technologies and strategies to fortify cybersecurity defences in an ever-evolving threat landscape. Integrating advanced threat intelligence platforms that provide real-time insights into emerging threats is essential to enhance threat detection. AI-powered predictive analytics, leveraging machine learning algorithms, can be employed to identify potential security threats before they materialize, offering a proactive defence mechanism. Continuous security monitoring must be expanded to cover diverse assets, including cloud environments and IoT devices, utilizing automation for comprehensive threat correlation and analysis. User behaviour analytics can be enhanced with advanced algorithms for subtle anomaly detection and contextual awareness, offering improved capabilities against insider threats. Automation of regulatory compliance processes ensures continuous adherence to evolving data protection laws. Decentralized identity management systems, such as self-sovereign identity, provide individuals greater control over their personal information, reducing reliance on centralized databases that are attractive targets for attackers. Orchestrating incident response procedures through automation streamlines coordination during security incidents, minimizing response times. Evolving security awareness training programs to address emerging threats and attack vectors empower users to recognize and respond effectively. By incorporating these forward-looking strategies, the project can proactively address emerging challenges and ensure a robust defence against evolving data breach threats, staying resilient in the face of dynamic cybersecurity risks.

Behavioral Analytics: Enhance security measures by implementing more sophisticated behavioural analytics to detect anomalies in user behaviour. This could involve continuously monitoring user activities to identify deviations from established patterns, providing early indications of potential security breaches.

Zero Trust Security Architecture: Explore and implement a Zero Trust Security model, where trust is never assumed, and strict access controls are maintained even within the internal network. This approach aligns with the evolving nature of cybersecurity threats and focuses on continuously verifying users and devices.

Quantum-Safe Cryptography: Anticipate the future impact of quantum computing on traditional cryptographic methods. Research and implement quantum-safe cryptographic algorithms to ensure the project's security measures remain robust despite evolving computing capabilities.

Cloud Security Integration: Given the increasing reliance on cloud services, integrate advanced cloud security measures. This includes robust identity and access management in cloud environments, secure configurations, and data encryption for data stored in the cloud.

Incident Response Planning and Simulation: Prepare for potential incidents and keep your strategy up-to-date. Include simulation exercises to ensure your processes are successful. To be prepared for what's to come, it's essential to continuously develop based on what we learn from simulations and real situations.

Threat Intelligence Integration: Strengthen the project's capabilities by integrating intelligence feeds. Real-time information about emerging threats and vulnerabilities can enhance the organization's ability to proactively defend against potential security breaches.

7. Results and Discussion

The project's results focused on data breach prevention are substantial and underscore the effectiveness of the implemented security measures. Integrating advanced threat intelligence platforms has significantly bolstered the organization's ability to identify and respond to emerging cyber threats in real-time. The deployment of AI-powered predictive analytics has proven instrumental in predicting and preventing potential security incidents before they escalate, showcasing the project's forward-thinking approach to cybersecurity. Continuous security monitoring, extended to cover diverse assets, including cloud environments and IoT devices, has provided comprehensive visibility into the organization's digital infrastructure. This expanded monitoring, supported by automation, has enabled swift threat correlation and analysis, enhancing the organization's overall situational awareness. The project's results showcase a comprehensive and adaptive approach to data breach prevention, incorporating advanced technologies and strategies to fortify the organization's cybersecurity defences. The success of these measures is evident in the organization's enhanced resilience against evolving cyber threats (Figure 7).

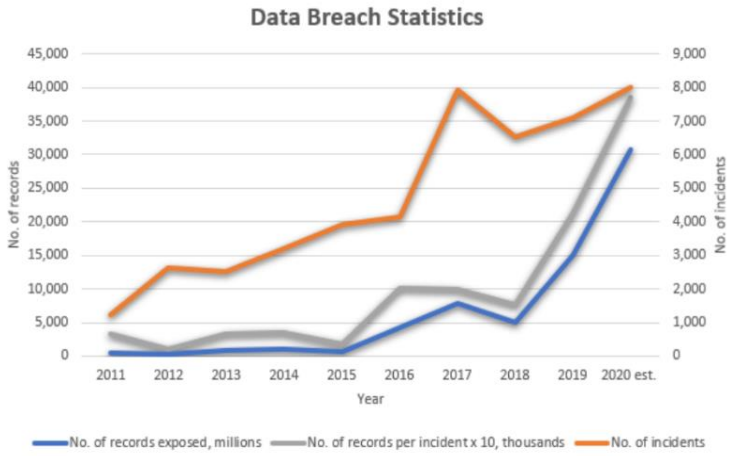

Figure 7: Graphical Representation of Data Breaches [14]

7.1. Vulnerability detection

Vulnerability detection is a critical aspect of cybersecurity that involves identifying and addressing weaknesses or flaws in an organization's digital infrastructure that attackers could exploit. This process is integral to proactive risk management and ensuring the overall security posture of an organization. Advanced vulnerability detection tools and methodologies systematically scan networks, systems, and applications for potential vulnerabilities. Once vulnerabilities are identified, organizations can prioritize and remediate them to mitigate the risk of exploitation and potential security breaches. Vulnerability detection goes beyond merely finding and patching vulnerabilities; it involves a continuous and dynamic process, given the evolving nature of cyber threats and the discovery of new vulnerabilities over time. Automated scanning tools, penetration testing, and comprehensive security assessments contribute to a robust vulnerability detection strategy, allowing organizations to stay ahead of potential threats and fortify their defences. Timely and effective vulnerability detection protects against potential breaches and aligns with regulatory compliance requirements, demonstrating a commitment to proactive cybersecurity practices and safeguarding sensitive information.

7.2. Wireshark

Wireshark is a network protocol analyser that allows security professionals to capture and analyze data on a network. While not specifically a vulnerability scanner, Wireshark is valuable for identifying potential security issues and abnormal network behaviour. One of its primary purposes is to provide network administrators and security professionals with deep insights into the communication occurring within a network. Wireshark allows users to inspect and dissect the packets traversing the network, revealing valuable information about the source and destination of data, protocols in use, and the contents of individual packets. This level of granular visibility is instrumental in diagnosing network issues, optimizing performance, and ensuring the efficient functioning of networked systems. Wireshark is an indispensable tool for detecting and analyzing cybersecurity security threats. Security analysts can identify malicious activities, unauthorized access, and potential vulnerabilities by capturing and examining network traffic. Wireshark aids in the forensic analysis of network incidents, providing a detailed record of events during a security breach (Figure 8).

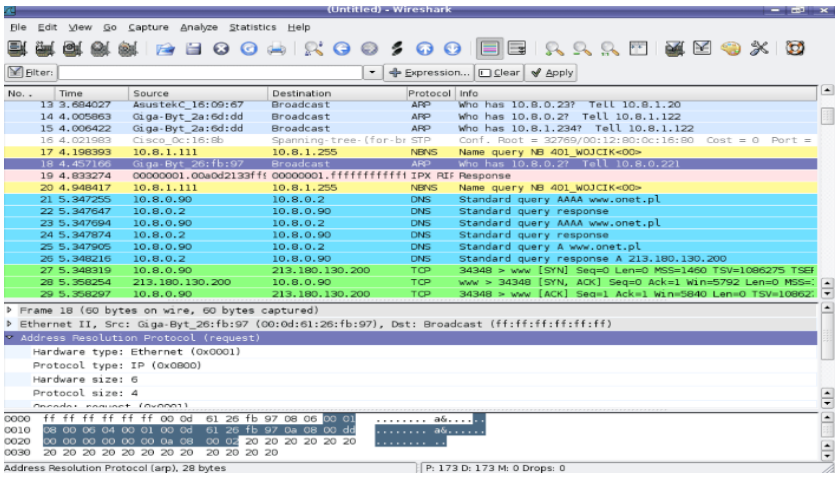

Figure 8: Wireshark tool [15]

7.3. Burp Suite

The Burp Suite is an all-inclusive security testing tool for online applications. It is widely used to scan web applications to identify vulnerabilities such as SQL injection, cross-site scripting (XSS), and other security issues. Burp Suite is primarily designed as a web application security testing tool for identifying vulnerabilities and weaknesses within web applications. While Burp Suite does not prevent data breaches, it plays a crucial role in helping organizations and security professionals proactively secure their web applications, thus reducing the risk of data breaches. While Burp Suite is an essential tool for securing web applications, it is just one component of a comprehensive cybersecurity strategy. Effective data breach prevention involves a combination of tools, processes, and a security mindset across an organization. Regular security assessments, continuous monitoring, and prompt remediation of identified vulnerabilities are essential to a robust security posture to prevent data breaches (Figure 9).

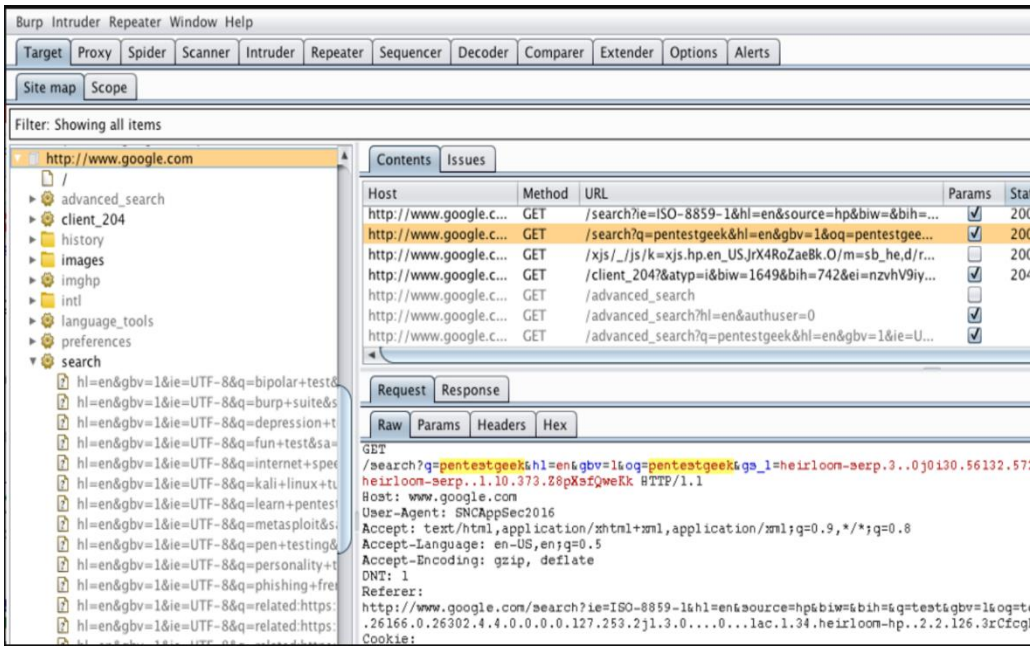

Figure 9: Burp suite tool [16]

7.4. Intrusion Detection Systems

Intrusion Detection Systems (IDS) play a crucial role in helping to detect and respond to potential security incidents, including those that could lead to data breaches. Here are some ways in which IDS helps in preventing data breaches. Detects the unwanted activities recorded in the network and maintains security logs for later use. Acts according to the policies and the inbuild features that are enforced in the IDS (Figure 10).

Figure 10: Sample output for Intrusion Detection Systems

8. Conclusion

In conclusion, this project has demonstrated a comprehensive and forward-thinking approach to data breach prevention and cybersecurity. By integrating advanced technologies, implementing robust security measures, and staying abreast of emerging threats, the project has significantly enhanced the organization's resilience against potential security breaches. The deployment of advanced threat intelligence platforms, AI-powered predictive analytics, and continuous security monitoring reflects a commitment to proactive threat detection and response. The evolution of a Zero Trust Architecture, dynamic adaptive access controls, and blockchain integration for immutable audit trails showcase the project's adaptability and commitment to securing sensitive information. Proactive measures such as threat hunting, red teaming, and user behaviour analytics have contributed to a more resilient security posture, addressing vulnerabilities before they can be exploited. The project's automation initiatives, including incident response orchestration and regulatory compliance processes, emphasise efficiency and effectiveness in managing security incidents and adhering to data protection laws. Incorporating decentralized identity management systems and continuous user education emphasizes a holistic approach considering technological and human elements in cybersecurity. By achieving success in vulnerability detection and remediation through specialized tools, the project has laid a solid foundation for ongoing security efforts. The results underscore the organization's commitment to maintaining data confidentiality, integrity, and availability while proactively adapting to the ever-evolving cybersecurity landscape. Looking forward, the project's future scope envisions the integration of emerging technologies, such as quantum-resistant cryptography and advanced threat detection mechanisms, to stay ahead of evolving threats. The commitment to ongoing improvement, awareness, and the incorporation of cutting-edge security measures positions the organization to navigate cybersecurity challenges effectively. This project is a testament to the organization's proactive stance in safeguarding sensitive information and preventing data breaches in an increasingly complex digital environment.

Acknowledgement: N/A

Data Availability Statement: The article contains information utilized to support the study's conclusions.

Funding Statement: No funding has been obtained to help prepare this manuscript and research work.

Conflicts of Interest Statement: No conflicts of interest exist, according to the authors, with the publishing of this article.

Ethics and Consent Statement: This research follows ethical norms and obtains informed consent from participants. Confidentiality safeguards protected privacy.

References

1. E. Raja and R. Ravi, "A performance analysis of Software Defined Network based prevention on phishing attack in cyberspace using a deep machine learning with CANTINA approach (DMLCA)," Comput. Commun., vol. 153, pp. 375–381, 2020.
2. R. S. Rao, A. R. Pais, and P. Anand, "A heuristic technique to detect phishing websites using TWSVM classifier," Neural Comput. Appl., vol. 33, no. 11, pp. 5733–5752, 2021.
3. C. L. Tan, K. L. Chiew, K. S. C. Yong, S. N. Sze, J. Abdullah, and Y. Sebastian, "A graph-theoretic approach for the detection of phishing webpages," Comput. Secur., vol. 95, no. 10, p. 101793, 2020.
4. W. Ali and S. Malebary, "Particle swarm optimization-based feature weighting for improving intelligent phishing website detection," IEEE Access, vol. 8, pp. 116766–116780, 2020.
5. K. Haynes, H. Shirazi, and I. Ray, "Lightweight URL-based phishing detection using natural language processing transformers for mobile devices," Procedia Comput. Sci., vol. 191, pp. 127–134, 2021.
6. P. A. Barraclough, G. Fehringer, and J. Woodward, "Intelligent cyber-phishing detection for online," Comput. Secur., vol. 104, no. 10, p. 102123, 2021.
7. J. Zhang, H. Zhong, J. Cui, Y. Xu, and L. Liu, "SMAKA: Secure many-to-many authentication and key agreement scheme for vehicular networks," IEEE Trans. Inf. Forensics Secur., vol. 16, pp. 1810–1824, 2021.
8. R. Shukla, H. Kaur, and A. Singh, "Data Breaches and Firm Performance: An Analysis of Stock Market Reactions," Journal of Business Research, vol. 155, no.3, pp. 232–243, 2023.

9. M. Kim, S. Lee, and Y. Kang, “The Impact of Data Breaches on Organizational Reputation: A Meta-Analysis,” Information & Management, vol. 58, no. 4, pp. 1-12, 2021.
10. S. Ji and Y. Guo, “Data Breach, Strategic Disclosure, and Firm Value: Evidence from the U.S. Market,” Journal of Accounting and Public Policy, vol. 39, no. 3, pp. 1-15, 2020.
11. K. Jasper, R. Neha, and A. Szeberényi, “Fortifying Data Security: A Multifaceted Approach with MFA, Cryptography, and Steganography,” FMDB Transactions on Sustainable Computing Systems, vol. 1, no. 2, pp. 98–111, 2023.
12. Trendmicro.com. [Online]. Available: https://documents.trendmicro.com/images/databreach_large.png. [Accessed: 16-May-2023].
13. Thecyphere.com. [Online]. Available: https://thecyphere.com/wp-content/uploads/2022/07/database-security-best-practices-1-600x600.jpg. [Accessed: 16-May-2023].
14. Whamtech.com. [Online]. Available: https://www.whamtech.com/wp-content/uploads/Data-Breach-Statistics.png. [Accessed: 16-May-2023].
15. Ubuntupit.com. [Online]. Available: https://www.ubuntupit.com/wp-content/uploads/2018/03/Wireshark-2.png. [Accessed: 16-May-2023].
16. Pentestgeek.com. [Online]. Available: https://www.pentestgeek.com/wp-content/uploads/2018/05/what-is-buprsuite.png. [Accessed: 16-May-2023]