ACCOUNT DETECTION: AUTOMATED SYSTEM FOR BLOCKING MALICIOUS ACCESS

JEEVARATHINAM A[1] , KALAIYARASI B[2]

jeevarathinama@skasc.ac.in, kalaiyarasib22bss016@skasc.ac.in

[1] Assistant professor in Computer Science, Sri Krishna Arts and Science College, Tamil Nadu.

[2] Student, III B.Sc. Software Systems, Sri Krishna Arts and Science College, Tamil Nadu.

ABSTRACT

This initiative emphasizes a secure system for file sharing within an organization, allowing an administrator to oversee employee accounts, upload files specific to departments, and track employee activities. The system guarantees that employees can access only the files designated for them and logs their usage, including the times files are opened and closed. A vital security component is the use of a session key mechanism, whereby an employee receives a one-time session key through email when attempting to download a file. Access to the file is permitted solely through this key, ensuring regulated access. If an employee inputs an incorrect key, their account is promptly blocked, thwarting unauthorized entry. The administrator possesses the sole power to unblock these accounts, upholding rigorous security measures. This initiative improves data security and accountability within an organization, thwarting unauthorized access and the abuse of sensitive files.

Keywords: Security, Authentication, Monitoring, Access, Administrator, Files, Encryption

I.INTRODUCTION

In a corporate setting, safe file sharing and tracking employee activities are essential for data privacy and effective management. Conventional file-sharing systems frequently lack features to oversee access and deter unauthorized use, rendering them susceptible to security threats. This initiative seeks to develop a strong web-based application utilizing ASP. NET and SQL, wherein an administrator can set up employee accounts, control file distribution, and observe file interactions. Employees are able to log into their accounts and retrieve files allocated to them. However, the system adds an extra level of security by creating and dispatching a session key to the employee's registered email after file download. This key is essential to gain entry to the file, stopping unauthorized access. If a wrong key is input, the system automatically locks the employee's account, guaranteeing that only valid users can reach confidential information. The administrator has complete authority over employee accounts, including the capability to restore access when needed. This method enhances security, averts unauthorized file access, and offers comprehensive monitoring of file usage.[5]

II. RESEARCH GAP

Organizations face significant challenges in managing and protecting file access among employees, especially when handling sensitive data. Traditional file management systems lack the ability to monitor individual file access, restrict unauthorized use, and facilitate controlled distribution. Unauthorized access and data breaches can result in severe consequences, including data leaks and violations of confidentiality. Additionally, the inability to track employee interactions with files poses a risk of resource misappropriation. This project addresses these issues by developing a secure file access and monitoring system that allows employees to access only the files relevant to their department and assigned to them.

Moreover, the system automatically locks user accounts after multiple incorrect login attempts, thereby enhancing security when an invalid session key is entered. By incorporating admin-controlled unblocking and monitoring of file usage, the system provides a comprehensive solution for secure file sharing within an organization. [7] In conventional file-sharing systems, the control over file access is frequently inadequate or entirely absent, resulting in unauthorized access, data breaches, and security vulnerabilities.

Furthermore, these systems typically lack sophisticated security measures such as multi-factor authentication (MFA) or encryption, thereby exposing sensitive information to cyber threats. Employees often possess unrestricted access to files outside their specific departments, heightening the risk of data exposure and information leaks among various teams or unauthorized individuals. Collectively, these shortcomings render traditional systems ineffective, insecure, and ill-suited for managing sensitive organizational data in contemporary enterprises, underscoring the necessity for more robust, controlled, and traceable file- sharing solutions. [10]

III. RELATED WORK

Role-Based Access Control (RBAC): RBAC frameworks are extensively implemented in organizations to manage access to files and resources according to the roles assigned to users. These systems guarantee that employees can only access information pertinent to their job functions, akin to the departmental file distribution in your initiative. RBAC is frequently incorporated into enterprise security infrastructures to uphold stringent access regulations.

Secure File Transfer Protocol (SFTP) Implementations : SFTP-based projects focus on encrypting data during its transmission to facilitate secure file sharing. Although your project emphasizes access control and monitoring, both systems share the common goal of safeguarding sensitive files from unauthorized access and ensuring data integrity during file transfers.

Audit Logging and Monitoring Systems: Audit logging systems document user activities within software applications to ensure accountability and facilitate monitoring. In a manner similar to how your project records the times files are opened and closed, these systems assist administrators in observing employee behavior and detecting potential security threats based on usage trends..[9]

IV. METHODOLOGY

The project is constructed utilizing ASP.NET and SQL Server within Microsoft Visual Studio 2010, providing a well-organized and scalable web-based solution. The process commences with the creation of an administrator account, enabling the administrator to log in and oversee employee management. The administrator has the capability to establish employee accounts by inputting necessary information such as employee ID, email address, and department affiliation. After an employee is registered, the administrator uploads files pertinent to specific departments, ensuring that employees can only access documents relevant to their designated departments. When an employee logs into their account, they are able to view and download the files assigned to them.[8]

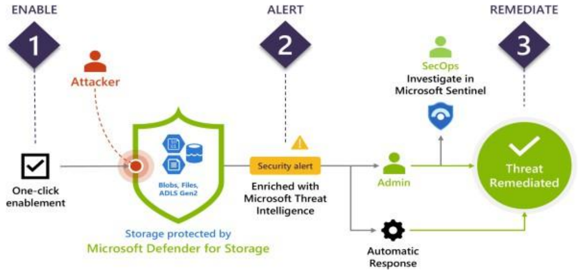


Fig.4.1 Process

Upon selecting the download option, a session key is generated automatically and dispatched to the employee’s registered email address. The employee must input the correct key to gain access to the file; failure to do so will result in their account being blocked. In the event of a block, only the administrator possesses the authority to restore access to the employee’s account, thereby maintaining stringent access control. Additionally, the system incorporates usage tracking, which logs the times files are opened and closed, providing the administrator with valuable insights into employee activity. The integration of role-based access control, session key authentication, and activity monitoring ensures a secure and effective organizational file management system. [8]

4.1 PROPOSED SYSTEM

The proposed system presents a robust solution for secure file access and monitoring, featuring sophisticated authentication and tracking mechanisms designed to uphold data confidentiality and regulate access within an organization. Employees will be granted access solely to files pertinent to their respective departments, thereby ensuring that sensitive information is disseminated strictly on a need-to-know basis. A notable aspect of this system is its session key authentication mechanism, which generates a unique one- time session key for each file. This key is automatically dispatched to the employee's registered email address, guaranteeing that only authorized personnel can access the requested files. To bolster security further, the system will automatically block an employee’s account after multiple incorrect session key entries, thereby thwarting potential brute-force attacks or unauthorized access attempts.[6]

The administrator maintains comprehensive control over account management, including the authority to unblock accounts when necessary, ensuring effective oversight and management of employee access rights. Additionally, the system features an extensive monitoring capability that logs all file interactions, including the timestamps for opening and closing each file. In summary, this solution not only fortifies organizational security but also enhances operational efficiency by providing a user-friendly interface and streamlined administrative controls..[3]

V. OBJECTIVES

The aim of this project is to establish a secure file access and monitoring system tailored for organizational purposes, with the primary goal of safeguarding sensitive information from unauthorized access. The system will empower administrators to efficiently manage employee accounts, encompassing their creation, monitoring, updating, and unblocking as required. Additionally, it will incorporate a department-specific file allocation framework, ensuring that employees can only access files designated for their respective departments.[4]

To further bolster security, a session key authentication protocol will be implemented, wherein a unique one-time session key is dispatched to employees via email for each file download request. This measure guarantees that only authorized personnel can access sensitive files. Furthermore, attempts at unauthorized access will be countered by locking accounts after several incorrect session key entries, thereby thwarting brute- force attacks or unauthorized efforts to access restricted information. Furthermore, the system will feature a comprehensive monitoring framework that records employee interactions with files, including timestamps for opening and closing, download histories, and session activities. In summary, this system is intended to deliver thorough data security, effective file management, and stringent access control for organizations, thereby promoting a secure and accountable work environment. [2]

VI. ALGORITHM

6.1MULTIPLY-WITH-SHIFT(MSWS) ALGORITHM

The Multiply-With-Shift (MSWS): This algorithm is a lightweight pseudorandom number generator that utilizes a combination of multiplication and bitwise shifting to create random sequences. It initiates with a seed value, which acts as the foundation for generating random numbers. The seed is multiplied by a significant prime constant to introduce variability, followed by a bitwise right shift to further enhance the mixing of bits. This methodology guarantees that the produced numbers demonstrate statistical randomness while ensuring computational efficiency. As MSWS operates in a deterministic manner, its output is entirely reliant on the initial seed, rendering it suitable for applications that necessitate reproducibility, such as simulations and procedural content generation. However, it does not provide cryptographic security, which means that its sequences can be anticipated if the seed and algorithm parameters are known. Despite this drawback, MSWS is extensively utilized in non-secure environments where speed and efficiency take precedence over unpredictability. Its straightforward design and minimal computational demands make it an appealing option for applications that require rapid and scalable random number generation.. [5]

6.2 FORTUNA ALGORITHM

Fortuna is a cryptographically secure random number generator specifically engineered for high-security applications where unpredictability is paramount. In contrast to MSWS, which depends on mathematical computations, Fortuna continuously collects entropy from a variety of unpredictable sources, including user interactions, system events, and hardware-generated randomness. These entropy values are maintained in an internal pool, guaranteeing a consistent supply of fresh randomness. The algorithm periodically processes this entropy and reseeds itself, thereby thwarting potential attackers from forecasting future outputs, even if they have access to previous values. Fortuna employs a block cipher, typically AES, to generate random numbers, which ensures a robust level of security and resilience against statistical analysis. A notable advantage of Fortuna is its self- healing capability; even if a portion of its state is compromised, new entropy can gradually restore its security. Unlike conventional pseudorandom number generators, Fortuna does not depend on a single seed, rendering it highly resistant to state compromise and backtracking attacks. Although it is more computationally intensive than MSWS, it is the preferred option for security-sensitive applications such as cryptographic key generation, secure communications, and authentication systems. Its dependence on diverse entropy sources significantly enhances its security, ensuring that outputs remain genuinely unpredictable and resilient against cryptographic threats. [1]

VII. IMPLEMENTATION

The project is developed as a web-based application utilizing ASP.NET and SQL Server within Microsoft Visual Studio 2010, facilitating organized data management and secure file sharing. The administrative module empowers administrators to oversee employee accounts, upload files pertinent to specific departments, monitor file interactions, and unblock accounts that have been locked. Employees are able to log into their accounts, access and download files assigned to them, and must input a session key sent to their registered email to retrieve files. Should an incorrect session key be entered multiple times, the account will be automatically locked to prevent unauthorized access.[1]

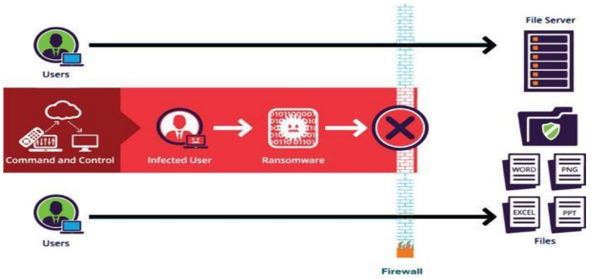
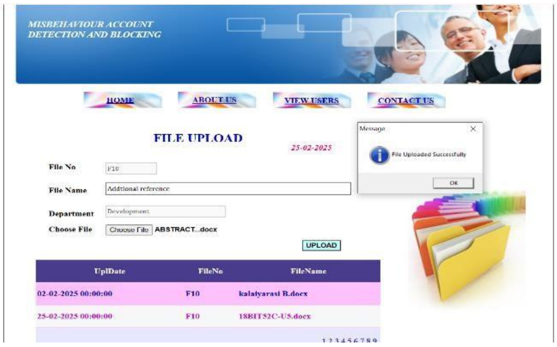


Fig 8.1 Implementation

The system employs session key authentication through the Multiply-With- Shift (MSWS) algorithm for generating random keys, thereby enhancing security. Employees are restricted to accessing only the files designated for their respective departments, thereby enforcing stringent role- based access control. The SQL Server database is responsible for managing employee records, file logs, and account statuses, including tracking file access times and locked accounts. The administrator maintains complete authority over the unblocking of accounts, ensuring that only authorized personnel can regain access. This implementation significantly improves security, access control, and data tracking, offering a comprehensive solution for organizational file management.[5]



FILE UPLOAD

25-02-2025

File No: F10

File Name: Addtional reference

Department: Development

Choose File: ABSTRACT...docx

Message

File Uploaded Successfully

UplDate	FileNo	FileName
02-02-2025 00:00:00	F10	kalaiyarasi B.docx
25-02-2025 00:00:00	F10	18BIT52C-U5.docx

1 2 3 4 5 6 7 8 9

VIII. SIGNIFICANCE AND IMPACT

This initiative is essential for improving secure file access and monitoring within organizations by thwarting unauthorized access and facilitating controlled data distribution. By employing session key authentication and automatic account blocking, it significantly mitigates the security risks inherent in conventional file-sharing systems. The adoption of role-based access control guarantees that employees can only access files pertinent to their departments, thereby preserving data integrity and confidentiality. Furthermore, tracking employee activities allows administrators to oversee file interactions, thereby enhancing transparency and accountability in data usage. The admin-controlled unblocking feature strikes a balance between security and operational efficiency, enabling secure access recovery when necessary.[7]

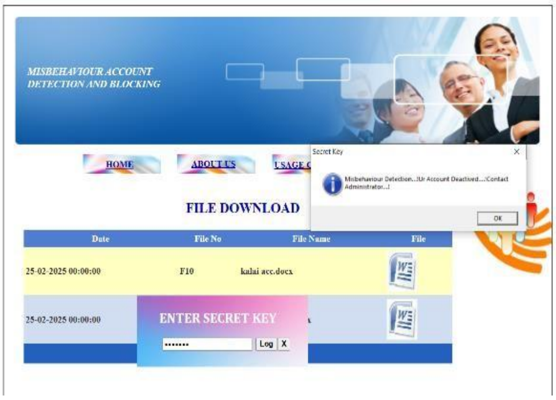
The implementation of the MSWS algorithm offers an effective approach to generating session keys, while the Fortuna algorithm bolsters security by incorporating cryptographic randomness as needed. By merging lightweight random number generation with robust access control mechanisms, the project delivers a comprehensive and secure file-sharing solution. Its influence extends to enhancing data security, preventing misuse, and ensuring adherence to confidentiality standards, rendering it highly beneficial for organizations managing sensitive information. [9]

IX. RESULT AND ANALYSIS

The outcome of this initiative is a robust file access and monitoring system aimed at overseeing and regulating employee interactions with sensitive organizational documents. This system features an administrative dashboard that enables the administrator to create and manage employee accounts by assigning distinct employee IDs, email addresses, and access rights tailored to specific departments. Furthermore, the system permits the administrator to upload files pertinent to each department, ensuring that employees can only access the files designated for them. [8]

Fig.10.1 File uploaded

The administrator also has the capability to monitor employee activities, including login times, file downloads, and comprehensive usage logs that document when files are accessed or closed. In the event of any unauthorized actions, such as multiple unsuccessful session key attempts, the administrator receives notifications and can take necessary actions to unblock accounts.[3]



MISBEHAVIOUR ACCOUNT DETECTION AND BLOCKING

Secret Key

Misbehaviour Detection...!Ur Account Deactived...!Contact Administrator...!

FILE DOWNLOAD

Date	File No	File Name	File
25-02-2025 00:00:00	F10	kalai acc.docx	
25-02-2025 00:00:00			

ENTER SECRET KEY

•••••••

Fig.10.2 Misbehaviour Account blocked

The employee portal facilitates secure login for employees, granting them access to files pertinent to their respective departments. When a file download is initiated, a session key is generated and dispatched to the employee's registered email address. This one-time key must be accurately entered to access the file, thereby ensuring that only authorized personnel can retrieve it. Should incorrect session keys be entered multiple times, the system will automatically suspend the employee's account to avert unauthorized access [1]

Fig. 10.3 Account Activated

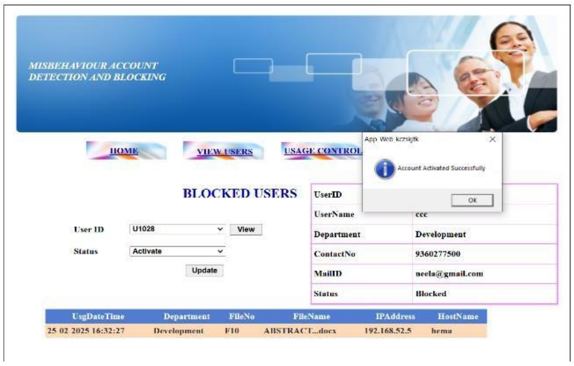
An integrated account detection system oversees all activities and flags any irregularities, such as repeated failed login attempts or unauthorized file access. This functionality aids in the real-time identification of potential security threats. Additionally, the system logs all file interactions, equipping the administrator with detailed reports on the timing and manner of employee file access. Developed using ASP.NET and SQL Server, the platform guarantees efficient data management and offers a robust, scalable solution for organizations seeking to protect sensitive information while ensuring controlled and monitored file distribution..[5]

X. CONCLUSION

This initiative establishes a secure and effective system for file access and monitoring within organizations, facilitating controlled data distribution and safeguarding against unauthorized access. By utilizing session key authentication, the system bolsters security by necessitating that employees input a one-time key sent to their email prior to file access. An automatic account blocking feature mitigates the risk of brute-force attacks and unauthorized usage, thereby enhancing data protection. The access management, overseen by administrators, allows for thorough monitoring of employee activities, including the times files are opened and closed. The integration of ASP.NET and SQL Server guarantees both scalability and reliability, while the application of the MSWS algorithm supports efficient session key generation. In summary, this project markedly enhances data security, access control, and accountability, rendering it an invaluable solution for organizations managing sensitive information.[4]

REFERENCES

[1] Alazab A, Hobbs M, Abawajy J, Khraisat A, Alazab M (2014) Using response action with intelligent intrusion detection and prevention system against web application malware. Information Management & Computer Security 22(5):431–449



MISBEHAVIOUR ACCOUNT DETECTION AND BLOCKING

App Web krzsjtk

Account Activated Successfully

BLOCKED USERS

User ID: U1028
Status: Activate

UserID	
UserName	ccc
Department	Development
ContactNo	9360277500
MailID	neela@gmail.com
Status	Blocked

UsgDateTime	Department	FileNo	FileName	IPAddress	HostName
25 02 2025 16:32:27	Development	F10	ABSTRACT...docx	192.168.52.5	hema

[2] H. Ichise, Y. Jin, K. Iida and Y. Takai, "NS record history based abnormal DNS traffic detection considering adaptive botnet communication blocking", *IPSJ J. Information Processing*, vol. 28, pp. 112-122, Feb. 2020.

[3] Alcaraz C (2018) Cloud-assisted dynamic resilience for cyber-physical control systems.
IEEE Wirel Commun 25(1):76–82

[4] D. Plohmann et al., "A comprehensive measurement study of domain generating malware", *Proc. USENIX Security Symp*, pp. 263-278, Aug. 2016.

[5] K S Adewole , N B Anuar , A Kamsin , K D Varathan , S A Razak Malicious accounts: Dark of the social networks J. Netw. Comput. Appl , volume 79 , p. 41 - 67 Posted: 2017

[6] Ara A, Louzada F, Diniz CAR (2017) Statistical monitoring of a web server for error rates: a bivariate time-series copula-based modeling approach. J Appl Stat:1–14

[7] M Egele , G Stringhini , C Kruegel , G Vigna Towards detecting compromised accounts on social networks IEEE Trans. Dependable Secure Comput , volume 14 , issue 4 , p. 447 - 460 Posted: 2017-08

[8] Australian. (2017, November). Australian cyber security center threat report 2017. Available:https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf

[9] S. Axelsson, "Intrusion detection systems: a survey and taxonomy," technical report 2000 Bajaj K, Arora A (2013) Dimension reduction in intrusion detection features using discriminative machine learning approach. IJCSI International Journal of Computer Science Issues 10(4):324–328

[10] Bhuyan MH, Bhattacharyya DK, Kalita JK (2014) Network anomaly detection: methods, systems and tools. IEEE Communications Surveys & Tutorials 16(1):303–33