Access Control Application Prevention and Mitigation of Cyber Attacks

***Pawandeep Kaur[1], Farahlina[1], Aftab Alam[1], Sukhminder Kaur[1], Roheender Singh Sahota[2]**
[1]School of Computer Science, Taylor's University, Subang Jaya, Selangor, Malaysia
[2]School of Technology, Asia Pacific University of Technology & Innovation, Malaysia
***Corresponding Author**

DOI: https://doi.org/10.51584/IJRIAS.2023.81011
Received: 30 September 2023; Revised: 12 October 2023; Accepted: 18 October 2023; Published: 18 November 2023

ABSTRACT

In the rapidly evolving landscape of cyber threats, safeguarding digital assets has become paramount for organizations worldwide. This paper presents a comprehensive analysis of access control applications as a frontline defense against cyber intrusions. We delve into the mechanics of contemporary access control systems, highlighting their role in preventing unauthorized access and ensuring data integrity. Drawing on real-world case studies, we demonstrate the efficacy of robust access control measures in thwarting cyber-attacks and mitigating their potential impacts. Further, we explore the challenges faced in implementing these systems, such as ensuring scalability, managing user privileges, and maintaining system resilience. Our findings underscore the indispensable nature of access control applications in today's digital age. By offering actionable insights and best practices, this paper aims to guide organizations in fortifying their digital infrastructures against the ever-present threat of cyberattacks. To ensure the security of data, it's essential to update automation processes periodically. This not only safeguards the transfer of information, ensuring its authenticity and confidentiality, but also prevents tampering or misinformation. Incorporating access control into the security strategy can address this concern. Access control restricts data access to designated individuals within the organization. However, there's an inherent risk: permissions could inadvertently be granted to unintended parties. To mitigate this, we recommend several solutions, with multifactor authentication being a prominent option for future implementation.

Keywords: cyber-attack, mitigation, access control, permission privileges, authentication

INTRODUCTION

Cybercrime has evolved into a pervasive issue affecting individuals both domestically and internationally. Governments, businesses, institutions, and even individuals might inadvertently aid cybercriminals while simultaneously becoming their victims. This phenomenon is deeply rooted in cyberspace, illustrating how criminal activities have adapted to the realm of information and communication technologies. Cybercrimes, including hacking, malware distribution, identity theft, financial fraud, and medical fraud, infringe upon individuals' privacy. Moreover, offenses that involve unauthorized disclosure of personal information, messages, images, and audio or video recordings—such as cyberstalking, cyber harassment, and cyberbullying—compromise personal privacy and data security (Cybercrime module 10 key issues: Cybercrime that Compromises Privacy, 2019). The globally distributed nature of today's cyberspace, with its diverse infrastructure, services, and user groups, presents challenges in addressing cybercriminal activities. These challenges encompass information gathering on cybercrime-related incidents, identifying responsible parties, and determining applicable laws. Often, jurisdiction and responsibility are contentious issues. The same complexity applies to privacy, where diverse cultures, laws, and opinions make it challenging to establish internationally standardized approaches.

In both online and offline realms, various entities, from legitimate stakeholders to malicious actors, highly value data. This makes data a primary target for cybercriminals. One significant reason data is vulnerable to

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume VIII Issue X October 2023

cybercrimes is its inadequate protection, making it susceptible to unauthorized or illicit access. Factors contributing to data breaches include the loss or theft of devices like laptops and smartphones, weak system and data security measures, excessive or unauthorized database access, and inadvertent data disclosure (Moore, 2022).

Society remains vulnerable to security incidents, especially with potential high-risk targets like military organizations, security agencies, and nuclear plants. In today's borderless digital landscape, no target is immune to cyberattacks, irrespective of its geographical location. The intricate web of economic networks tightly interlinks businesses, often leading to interdependencies. An attack on a single entity within this interconnected framework can have ripple effects throughout the entire industry. The frequency and severity of these cyberattacks are escalating, with adversaries continually innovating their intrusion methods. Consequently, IT security professionals must adopt a proactive, preventative approach to enhance system security. As cyber threats become more sophisticated, companies are increasing their investments in information security, guided by a meticulous cost-benefit and priority analysis (Hamzah, 2022). The cornerstone of success lies in the forward-thinking mindset of security experts and a consistent financial commitment to cutting-edge security solutions.

PROBLEM BACKGROUND

The access control security method restricts who or what can access resources in a computing environment. It's a fundamental security principle that mitigates risk for companies and organizations. Access control is bifurcated into two types: logical and physical. Physical access control limits access to campuses, buildings, rooms, and tangible IT assets. In contrast, logical access control restricts access to data, system files, and computer networks.

Organizations utilize electronic access control systems to oversee employee access to restricted business locations and sensitive areas, such as data centers. These systems rely on user credentials, access card readers, auditing, and reports to secure a facility. Some systems incorporate alarms, lockdown capabilities, access control panels, and other features to deter unauthorized access or operations (Global Fraud Report 2021 – Cybersource, 2022).

A security issue known as broken access control vulnerability allows unauthorized individuals to access restricted resources. By exploiting this vulnerability, attackers can bypass standard security measures and gain unauthorized access to sensitive data or systems. Often, weak authentication and authorization procedures result in broken access control vulnerabilities, granting attackers unauthorized privileges (Clancy, 2022). Ensuring the security of your systems and data hinges on preventing such vulnerabilities.

An application exhibiting an access control vulnerability, which allows users to view or modify sensitive data without proper authentication, poses a significant security risk. Malicious actors can exploit this vulnerability to access or alter confidential data without the necessary permissions. For example, an application might improperly restrict access to certain functions based on user roles. A standard user account shouldn't have the capability to add new users, but if the application doesn't limit this function, a regular user might add users, potentially with administrative privileges. Attackers can exploit such vulnerabilities to modify data without permission or access confidential information. To mitigate the risks associated with these vulnerabilities, organizations should implement robust security controls.

Logical access control systems authenticate and authorize users and entities by analyzing essential login credentials, which might encompass passwords, personal identification numbers, biometric scans, security tokens, or other authentication factors (Global Fraud Report 2021 – Cybersource, 2022). Multifactor authentication (MFA), requiring two or more authentication factors, is often a vital component of a layered defense strategy.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume VIII Issue X October 2023

Access control is crucial for protecting both physical and logical systems from unauthorized breaches. Its primary objective is to minimize security risks by actively defending sensitive data, such as customer information. Access control is foundational in several security compliance initiatives.

In the business realm, access control is typically employed to regulate access to networks, computer systems, specific applications, files, and sensitive data. However, as IT ecosystems evolve, merging traditional on-site systems with contemporary cloud services, managing access control becomes more complex. With the surge in high-profile security breaches, many tech vendors have shifted from basic single sign-on systems to comprehensive unified access management, bolstering security across both on-premises and cloud platforms.

Access control operates by verifying the identity of an individual or entity, ensuring the individual or application is genuine, and granting the appropriate access level associated with the username or IP address (Global Fraud Report 2021 – Cybersource, 2022). Directory services and protocols, such as the Lightweight Directory Access Protocol and Security Assertion Markup Language, facilitate access controls. They allow users and entities to connect to computer resources, like distributed applications and web servers, by authenticating and authorizing them. Organizations adopt various access control strategies based on their compliance requirements and the IT security levels they aim to protect.

LITERATURE REVIEW

This section of the paper reviews literature related to cyber-attacks and access control.

A. Related Works

The rapid digital transformation catalyzed by the Covid-19 pandemic has unveiled numerous vulnerabilities, creating opportunities for cybercriminals. A 2020 report emphasized the significant cybersecurity challenges that emerged during the pandemic, noting that the increase in cyberattacks was tied to the heightened anxieties and fears surrounding the pandemic. Healthcare organizations were primary targets (Pranggono & Arabo, 2020). Another study highlighted the challenges the healthcare information system faced during the pandemic, especially the rise in cyberattacks targeting various health organizations (He et al., 2021). This research emphasized the urgent need for enhanced cybersecurity measures in the healthcare sector to counter the escalating cyber threats during such crises.

While the Covid-19 pandemic has introduced many uncertainties, it has given cybercriminals an advantage in targeting vulnerable individuals and systems. According to an article by Pranggono and Arabo (2020), there is a positive correlation between the pandemic and an increase in cyberattacks. This suggests that the shift to remote working, often without adequate training or security measures, led to an increase in attack vectors and security risks. During the pandemic, new forms of attacks, such as scams and phishing, became commonplace. The article discussed three major cybersecurity issues during the pandemic: types of cyberattacks, attacks on the healthcare sector, and mitigation strategies. The most common types of cyberattacks during this period included scams, phishing, malware, and distributed denial-of-service (DDoS). Healthcare entities, like pharmaceutical companies and research and development (R&D) organizations, were primary targets for cyberattacks, often due to their limited security measures and budgets. The article suggests several mitigation strategies, including user education, the use of virtual private networks (VPNs), multi-factor authentication, adherence to security policies, and regular software updates (Pranggono & Arabo, 2020).

Contact tracing has raised questions regarding its impact on privacy rights. A 2022 article by Alshawi et al. noted that as the virus spread in 2020, there was an increase in digital surveillance technologies, especially contact-tracing apps. Many of these apps collected a variety of user data, such as location and health details.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume VIII Issue X October 2023

However, the way this data was used was often unclear and not properly communicated to users. This lack of transparency raised concerns about user privacy and potential misuse of personal information. It's crucial for app developers and companies to ensure users are well-informed about how their data is used, stored, and shared to foster trust and ensure compliance with data protection regulations. The article identified several general privacy concerns, including disclosure, compliance, storage, retention, access, monitoring, and integrity. Contact tracing apps from countries like India, the US, Japan, Germany, and South Korea were found to have significant privacy issues, such as retaining user data, not adhering to privacy policies, lacking data control, and using third-party APIs. The article hypothesized that the primary reason users were hesitant to download these apps was concerns over privacy, potentially leading to 'technostress'—anxiety and negative emotions caused by technology. To protect user privacy while using digital surveillance technologies, the article suggested several methods, including adhering to privacy rules and policies, avoiding redundant data storage, using blockchain encryption, and implementing feedback systems. The study concluded that any technology handling data and privacy should comply with protection laws, be ethical, uphold strong values, and avoid privacy-related issues (Alshawi et al., 2022).

Cybersecurity and information security have undergone significant changes during the recent pandemic. Georgescu (2021) pointed out that the pandemic brought about major transformations in two key areas: personal life and work. The digitization of sectors like e-commerce, communications, entertainment, news, and education has had a profound impact on individuals' personal lives. In the realm of work, the adoption of remote work, the transition to new and unfamiliar technologies, the use of cloud-based solutions, and increased reliance on videoconferencing were the most notable professional changes. However, several types of cybersecurity incidents became more prevalent during the pandemic, including ransomware, phishing, brute-force attacks, remote desktop protocol attacks, and supply chain attacks, among others.

Cyber security is an important practice of research and training due to the rise of usage in digital devices which are connected to each other in a network. This interconnectivity provides convenience to people, but it also increases the vulnerability risks in security. Chin et al. (2020) highlight that the COVID-19 pandemic led to a significant rise in the use of technology due to increased adoption of e-learning, e-commerce, and work-from-home practices, stemming from movement restrictions. This surge also corresponded with a heightened rate of cyber-attacks, including phishing, malware, ransomware, and identity theft. A prevalent cyber-attack during the 2020 pandemic was "Zoom Bombing," where unauthorized individuals intruded Zoom conference calls. These intruders often utilized tools like WarDial to identify unsecured meeting IDs. Furthermore, Zoom faced a credential stuffing attack, where attackers assumed that existing Zoom account holders used identical passwords across various services. Zoom emerged as a primary target, with cybersecurity firm Cyble discovering about half a million compromised Zoom accounts being sold on dark web forums. To address such challenges, the authors suggest the deployment of advanced artificial intelligence capable of preemptively identifying threats by scanning, verifying, and alerting about suspicious system packets (Chin, Yong, Li, Qi, & Fatima, 2020).

Educational institutes are also at risk in the cybersecurity department in securing their networks from any possible threats. In reality it is easier to cyber-attack a target rather than defending which is essentially for schools having to defend against multiple kinds of cyber threats and these attackers design their attack to point towards any apparent weak point in the security system. This problem as institutes having to allow a vast flow of sharing of information on the internet while ensuring that the information is safe and secure is a big challenge for many security administrators in universities out there. In contrast to businesses and organizations that can tighten their security system, universities need to make it more accessible for their students and staff. For this problem, educational institutes are more vulnerable to protect their data. Cyber threats will continue to persist until this balance can be adjusted. According to an article by Professor Gary Rogers in 2015, the University of Wisconsin gets about 90,000 to 100.000 attempts per day to penetrate their system. The University of Delaware had resulted in a cyber-attack having a breach of data with about 72,000 staff and students' information. For this exact reason they have encouraged an institute to have login

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume VIII Issue X October 2023

ids and passwords for authorization and install encrypted wireless networks for the staff and students and an unencrypted network for the guests. They also suggested having a network file system (NFS) protocol to allow access of home directory from any computer (Rogers & Ashford, 2015).

The cybersecurity landscape in the banking and financial sector presents significant risks to companies, especially if their security is breached. This sector remains a primary target for many cyber attackers, consistently emerging as a potential hotspot for cyber threats. Goh (2020) notes that Singapore was particularly impacted by such cyber-attacks. For instance, in May 2017, the infamous ransomware worms, WannaCry and NotPetya, spread swiftly across numerous computers. These malicious programs encrypted computer hardware, rendering them inaccessible to users. Victims were then coerced into paying a ransom to regain access to their encrypted data (Goh, 2020). The most destructive impact happened of NotPetya which cost at least 10 billion. These attacks have affected multiple banks, ATM networks and card systems. It also impacted Singapore by breaching the confidential data that was initially held by the healthcare provider, SingHealth. One of the most effective solutions to this problem is by running a training course for their employees to always be aware and proactive in an event of a security attack by measuring the number of staff that passes the security training test. They suggested to always keep track of the number of devices that are outdated to ensure that hardware used is always patched and up to date (Goh et al., 2020).

The healthcare sector has seen an uptick in ransomware attacks in recent times. Despite enhanced efforts in cybersecurity, a growing number of hospitals are becoming targets. One of the challenges in safeguarding against these attacks is the potential lack of understanding among users and technicians about how these threats function. As highlighted by Davis (2016), in 2016, no fewer than 14 hospitals found themselves at the receiving end of ransomware attacks. It's vital for top IT professionals in healthcare institutions to place as much emphasis on cybersecurity training for their teams as they do on HIPPA compliance. Gaining insights into the attack's nature, its spread, and prevention measures is the starting point in addressing these threats. Roa (2017) suggests that proactive strategies, ensuring all staff are educated about ransomware threats, can help mitigate risks in the healthcare infrastructure.

In July 2019, despite advancements in its IT infrastructure, Capital One disclosed a security breach where sensitive customer data was accessed by an external entity. As stated in their public report from July 29, 2019, Capital One acknowledged that on July 19, 2019, an unauthorized individual gained access to various personal details of their credit card users. The compromised data encompassed information typically collected during credit card applications, such as names, addresses, phone numbers, email addresses, birth dates, and self-reported incomes. This breach impacted around 100 million individuals in the U.S. and approximately 6 million in Canada. To prevent attackers from obtaining access credentials, a range of technological controls, including PR.AC-1, PR.AC-4, PR.AC-6, PR.AC-7, PR.IP-1, and PR.PT-3, are recommended. Moreover, controls like PR.PT-1, DE.AE-3, DE.CM-6, DE.CM-7, and DE.DP-2 are suggested for monitoring and alerting any unauthorized access to administrative credentials (Neto et al., 2020).The aforementioned research has shown how the print media covered the Ashley Madison data leak, and the enormous guilt and culpability that was assigned to the individuals themselves. Many believed that the disclosure of alleged "cheaters" who subscribed to a well-known adultery website was justified. Despite the fact that their personal information was compromised in a clear violation of their privacy and security, this action meant that they were denied any victim status in the incident. Instead, they were believed to be accountable for both their own demise and any resulting consequences. According to the Ashley Madison controversy, this is "an instance that has questioned how the public and media react to gross invasions of privacy when the victims are people some have little compassion for". The study discussed in this article has adequately demonstrated the influence and strength of a victim-blaming discourse directed towards those who ostensibly subscribe to the Ashley Madison website (Cross, Parker, & Sansom, 2018).

IMPLEMENTATION

Cybersecurity and threat intelligence specialists unanimously agree that online criminal activity is on the

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume VIII Issue X October 2023

rise. We have meticulously examined the latest techniques to present a comprehensive overview of methods and markers used in detecting cybercrimes. This includes advanced machine learning, deep learning investigations, and associated threat intelligence and engineering tasks across various analysis layers, such as surface, deep, and darknets (Ahn, Hu, Lee, & Meng, 2010). Initially, to aid in the management and development of these intelligence solutions, we provide (i) a classification of the existing methods. This is further broken down into (ii) an outline of the types of criminal actions that can be identified and (iii) a compilation of the indicators and risk features pertinent to such detection (Parkinson & Khan, 2022). The subsequent step involves pinpointing the primary challenges and factors in engineering and management that require attention. We employ Topic Modelling Analysis to discover and scrutinize the most relevant threat concepts present in both the surface web and the deeper, hidden layers of the internet. Next, we establish a roadmap by highlighting existing gaps and challenges. Insights from professionals further enrich our findings. The analysis effectively illustrates the discrepancies between the theory and practical application of threat engineering and management across the surface and deep web. Our thorough literature review further elucidates the scope of current risk assessment methods for the said domains. Addressing these methods is crucial for law enforcement agencies to efficiently tackle cyber threats and crimes. If a unified data model existed for setting access control policies, one could also offer policy analysis and reasoning at a high level, without being tied to a specific platform. In actuality, given the diversity of data models, access control models, and related configuration options, such as policy propagation and conflict resolution criteria, adopted by Big Data platforms, it can be extremely challenging for security administrators to comprehend the impact of a set of access control policies on the data resources that are managed by their systems and to evaluate the quality of the specified policies (Colombo & Ferrari, 2019). Most of the research in this area has been focused on reasoning about the completeness of policy sets as well as correctness verification, redundancy detection, and inconsistency detection. To complete the investigation, a variety of strategies have been used, including formal methodologies, machine learning, and data mining techniques.

A. Methodologies & Theories

There are still some murky areas in the criminal law related to cybercrime. Digital piracy, for instance, was initially used to prohibit copyright-infringing methods and behaviors in their tangible forms. However, it has evolved to encompass the unlawful use of content that exists solely in cloud-based digital form (McGraw, 2015). Extrapolating traditional criminal law concepts to address digital piracy in its current evolved state may be off target. We contend that while practices related to digital downloading have evolved, scholarly and legal definitions have remained static. It is inefficient to stigmatize actions that are common in the cybersphere and create a gray area between lawful and illegal behavior, wasting our legal resources and attention. We find that the social harm that is desired to be avoided, discouraged from, or punished when four theoretical viewpoints on the political application of the criminal law to digital piracy are considered.

Despite rapid advancements in authorization and access control technology, the general public's perception of it lags behind the solutions available today. This widespread belief, or misperception, compares modern technologies with innovation, digital transformation, and customer-centricity, which prevents organisations from implementing contemporary solutions in the first place (Duchamps, 2022). Role-based access control solutions still predominate, where your level of access is determined by your position within the organization. However, the issue arises when applied to customers, as they don't assume multiple roles.

They merely play the part of the customer. Therefore, as a customer, you either have access to things like your Amazon Echo, health records, online banking, etc. or you don't. By granting both employees and customers fine-grained access, modern access management addresses this issue. Customers are no longer treated uniformly; they can be categorized as minors, elite members, or subject matter specialists. Organizations can establish rules for who has access to what by considering the characteristics of the customer, the digital asset, and the context, using modern policy-based access control.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume VIII Issue X October 2023

The underlying idea is straightforward: without centralized access control, an abundance of rules may emerge with no clear entity to be held responsible. Centralized access management does have some restrictions, though. How do you manage access for users who are familiar with your ecosystem or who work for its members but are not personally acquainted with you? Users are authorised to grant access to others as well as themselves through the administration of delegated access. Subscribers can manage family accounts, partner organisations can control access for their employees, and users can invite friends or co-workers to share or cooperate. And no, by doing so, you are not going to unleash Pandora's box. All new users are required to register before any authorizations are given. Organizations exercise control by establishing rules that outline who is allowed to invite types of relationships, and they are given visibility. Data from event logs can be accessed by organisations to monitor user engagement, relationships, and growth.

PROPOSED SYSTEM

During the pandemic, the global community faced multifaceted tech-related security challenges. Among these were digital inequality, heightened concerns over privacy, the rapid rise of automation, and the rampant spread of misinformation. Digital inequality refers to disparities in access to, use of, or the impact of information and communication technologies. As the world swiftly transitioned to online platforms for work, education, and social interaction due to pandemic restrictions, those without adequate access to technology or the internet found themselves further marginalized. This digital divide became more pronounced, emphasizing the gaps between various socio-economic groups, regions, and demographics.

In this context, Griffiths highlighted a significant increase in cyber threats. Cyberattacks surged by 358% in 2020 compared to the previous year and grew by another 125% in 2021, with a continued upward trend anticipated for 2022 (Griffiths, 2022). This surge underscores the heightened cyber vulnerabilities during the pandemic era. The escalation in cyberattacks can be attributed to the broader adoption of remote work and increased dependence on technology. Systems that lacked robust security measures became prime targets, revealing vulnerabilities often underestimated by individuals and organizations.

A comprehensive solution is required to mitigate these risks associated with information security and to prevent cyberattacks. Cyberattacks presents itself in many forms such as malware, data theft, privacy breach and others, and it is crucial that systems have adequate security measures in place to prevent these from happening. The foremost method of preventing cyberattacks is to eliminate any possible vulnerabilities in systems that attackers may exploit. This can be achieved through various controls such as patch management, secure configuration, and network monitoring to mitigate the 'breach' stage of cyberattacks (Reducing your exposure to cyber attack, 2015). A prominent and most definitive control that can be utilised as a solution to mitigate risks and cyberattacks is access control.

Access control can be considered one of the best solutions for detecting attempted cyberattacks and preventing them. Access control enables the recognition, authentication, and authorization of users before granting access or privileges to applications, data, systems, or resources. By ensuring that only authorized users have privileges to access critical and confidential systems, it becomes possible to protect applications, data, systems, and resources, thus minimizing the risk of cyberattacks and associated security risks. Access control systems enhance security by reducing vulnerabilities, providing system visibility, and logging access activities. These systems are vital for auditing and detecting potential misuse or unauthorized attempts. Nevertheless, their success relies on proper implementation and regular updates. Organizations can also improve their compliance with policies and laws related to access control and data privacy by implementing an access control system, thereby enhancing their protection against cyberattacks, data theft, and privacy breaches.

An access control system allows an organization to regulate employees' or users' access to its applications, data, systems, and resources by assigning privileges based on their roles. These privileges would allow them to only access organisation's applications, data, systems and resources that they are permitted to. Using this method of control that allows only certain users to access specific resources would minimize the risk of internal threats such as sabotage, accidental data loss, theft of data and unsafe cyber security practices, as

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume VIII Issue X October 2023

well as external threats such as cyberattacks and system exploits. This is because while employees are trusted by the organisation when granting access privileges, these privileges may be easily abused or misused, whether intentionally or accidentally. On the other hand, an access control system also detects, alerts and remediates unknown access to systems that are not authorised. This is particularly useful for outsider access or potential attackers with the intention of gaining control over applications, data, systems, or resources of an organisation for their own personal gain.

An access control system is integral for organizations, serving not just as a gatekeeper to their applications, data, systems, and resources, but also as a tool to address and diminish security risks, including inequality, privacy, automation, and misinformation. By adhering to the principles of the CIA triad – Confidentiality, Integrity, and Availability – the system ensures fairness by granting users the privileges they rightfully deserve, thereby neutralizing potential power disparities.

Confidentiality is maintained as the system ensures that only authorized individuals can access specific data, safeguarding both user and organizational privacy. This reduces the risk of unauthorized data exposure or breaches. Integrity is preserved by ensuring that data remains unaltered and authentic, and that actions are performed with the correct permissions. As for Availability, in an era where automation is prevalent, human oversight remains crucial in managing access control systems. While automation can streamline certain processes, it's not infallible and can occasionally grant or deny access erroneously.

Furthermore, by controlling access, the system plays a pivotal role in mitigating the spread of misinformation. Restricting unauthorized access can significantly reduce the chances of digital propaganda dissemination and the unethical use of technology.

The recent pandemic has heightened threats across various sectors, particularly in technology. As an increasing number of individuals transitioned to remote work, they became more vulnerable to security breaches, often due to insufficient security protocols in their home setups. An access control system serves as a safeguard against these vulnerabilities. It vigilantly monitors user activities, regulates access to company applications, data, and resources, and promptly flags any suspicious or unauthorized actions.

PROTOTYPE SYSTEM

We've crafted a prototype interface that includes features like a user menu, audit log, and notification alerts. This application is tailored for management and security engineers to oversee employee activities within the company, ensuring data isn't accessed without the right permissions. Managers or the security team can access the application on their computers, where they'll find the audit log for both security engineers and managers, and an access history exclusive to managers. Additionally, if a regular employee attempts to access a restricted website, a notification alert will appear, prompting upper management to intervene and potentially grant access. The design mockups of the prototype can be viewed in Figure 1.

A. Upper Management/Security Team

The audit log is the screen that security engineers use to view the actions taken by each employee, including their IP address and location. There is also a 'See more actions' button that displays additional actions taken by that specific employee. The actions shown within the black box in the picture represent only the employee's most recent actions.

The 'Manage access' button provides options for a security manager to grant access to specific files or software for an employee. The 'block' button is used to prohibit the employee from accessing any files or software.

Lastly, if the application recognizes the user, the employee's name will be displayed. If the user is accessing the system from outside the network or from an unrecognized device, it will show 'Unknown User(?)' highlighted in red, indicating that an external source is accessing the database. This display includes the action taken, IP address, and location if available.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume VIII Issue X October 2023

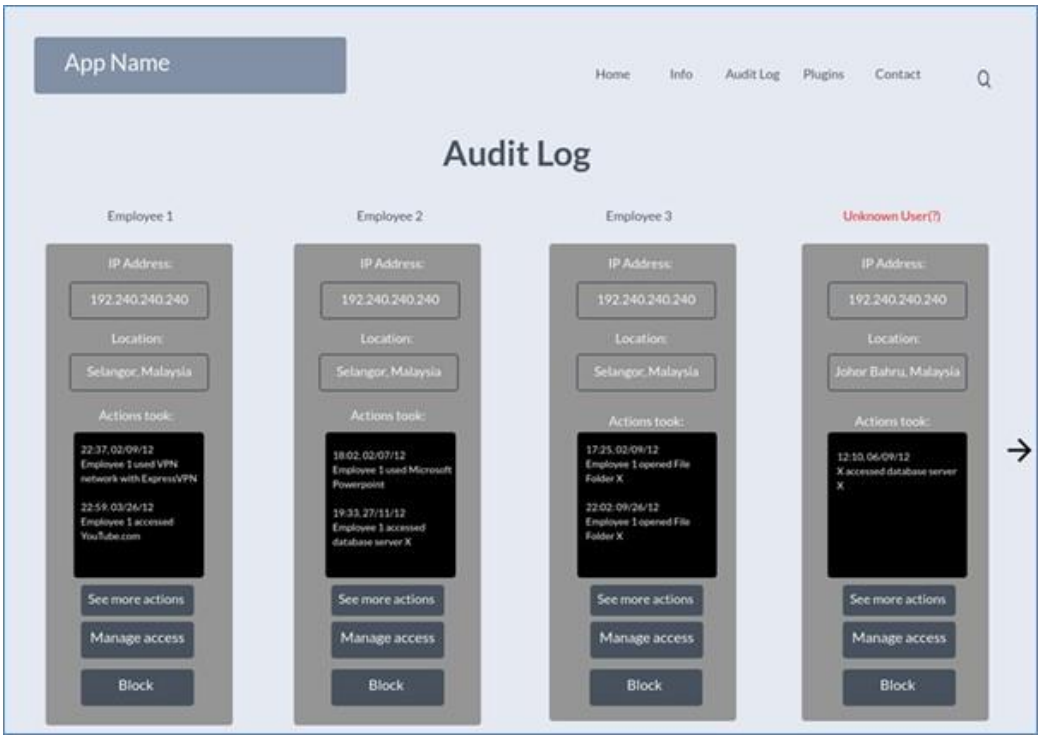

Figure 1 shows Audit Log for Security Engineers

The access history page is a menu accessible to upper management within the company. Here, they can view the actions taken by employees within the company, including options to display the most recent actions, sort them alphabetically, or sort by the number of actions taken.

The default page displayed is set to 'most recent,' as shown in Figure 2. It will then list the name of the employee, the time and date of access, along with the action taken. An additional feature is the 'block' button, which allows for the instant blocking of specific actions taken by employees.

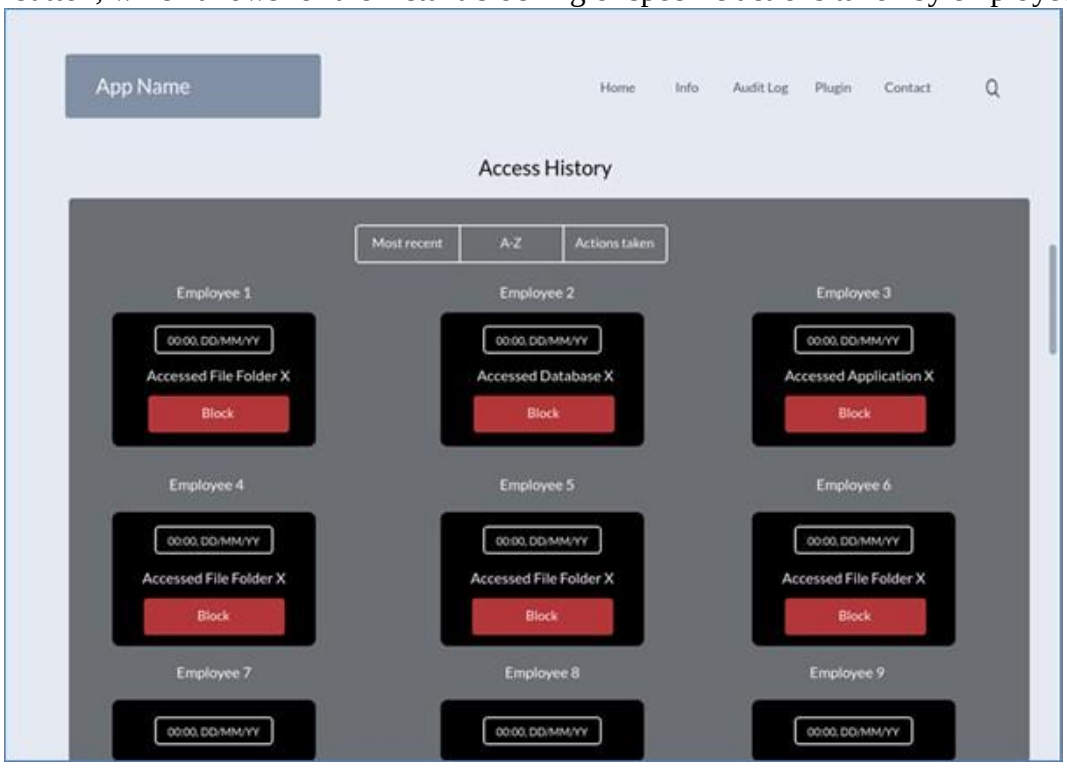

Figure 2 shows the access history.

The 'Request access' option will only be visible to security engineers when a specific employee requests

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume VIII Issue X October 2023

access to a particular page. A popup window will appear on their screen, displaying the name of the employee, their employee ID, privileges, the IP address of the requested page, its location, and its domain name.

The security engineer can then decide whether to grant or deny the requested access by the employee.

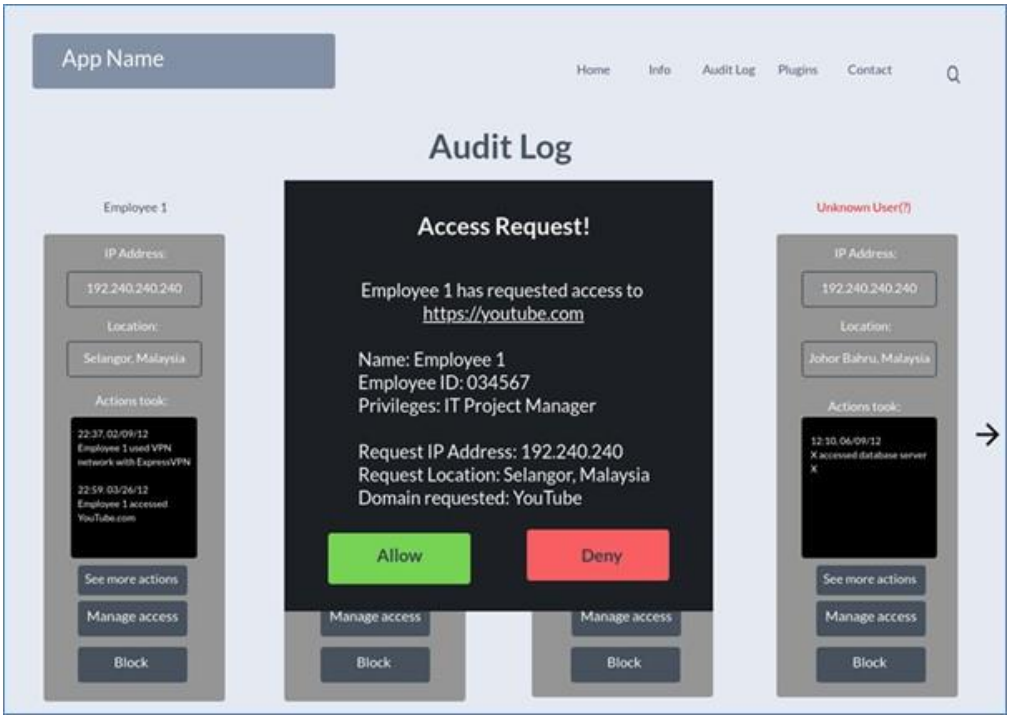

Figure 3 shows requesting access.

This page displays the duration of access granted, which is determined when the security engineer presses the 'allow access' button. The security team can specify the duration of access for the employee requesting access by using a dropdown menu.

The options include 15 minutes, 30 minutes, 1 hour, or 24 hours. After the chosen time elapses, the security engineer can press 'allow,' and access will be restricted once again.

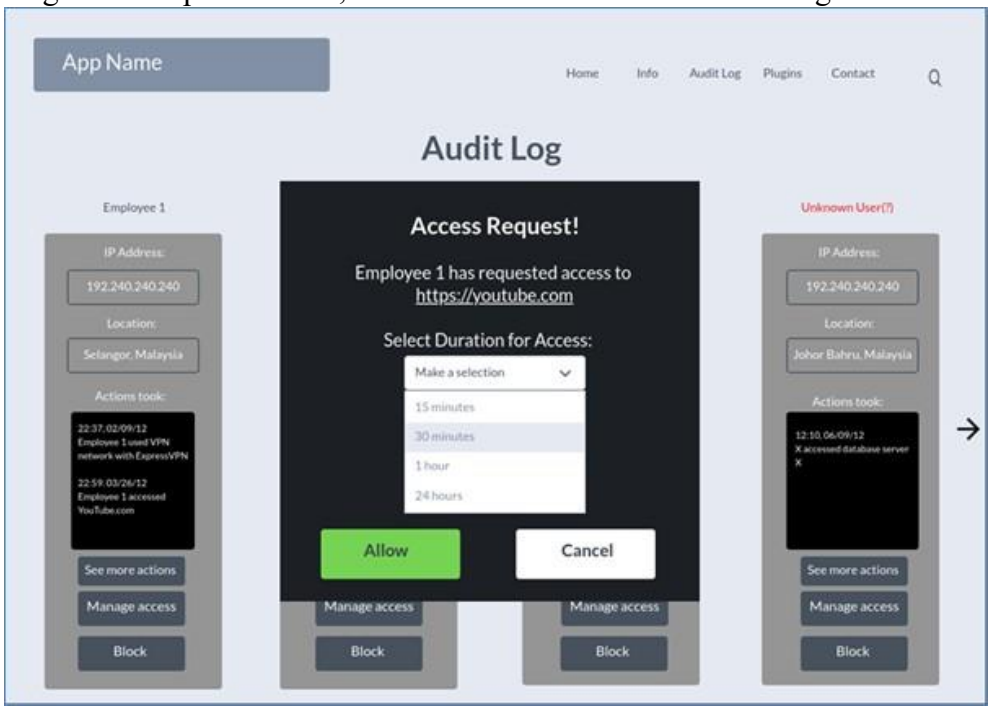

Figure 4 shows the time given for access granted.

This is the unidentified access page, which will only be visible to security engineers when an unknown,

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume VIII Issue X October 2023

unrecognizable device attempts to access a specific file from the network or database. In this case, an alert will appear on their screen, providing information about the unknown device, including its IP address, location, time of the action, and domain name.

The application will also inform the user that the device is not recognized and offer two options to the security engineer: allow the access or deny it.

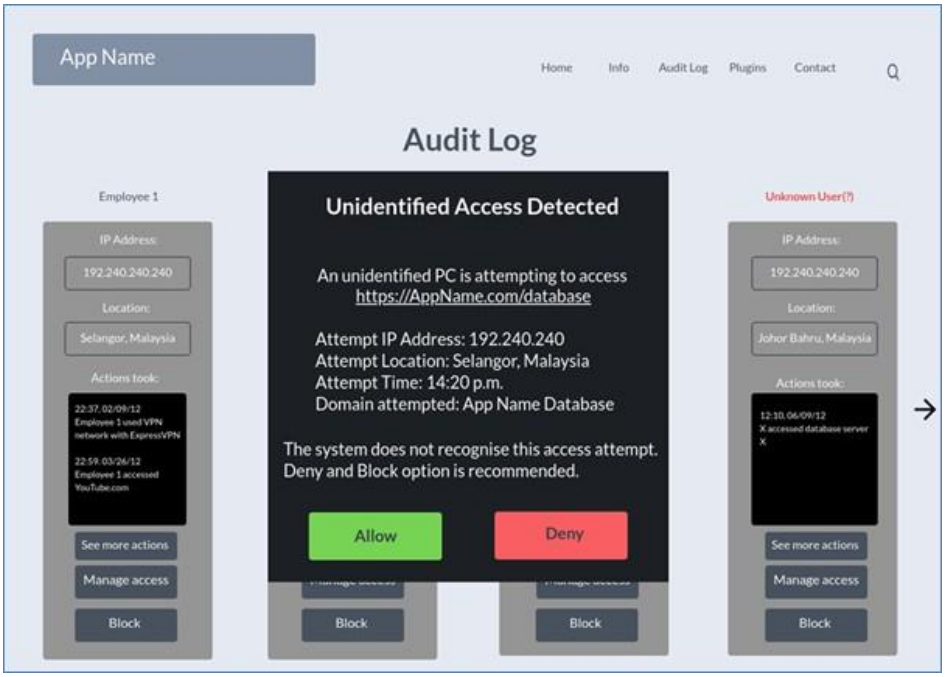

Figure 5 shows unidentified access.

This is the action undo page that the security engineer team sees after allowing or denying user access. The screen below confirms the action taken by the user, indicating that access from the displayed IP address has been blocked. It also provides details such as location, time of the action, domain attempted, and website details. At the bottom of the alert, it states,

'This user will not be able to access the attempted website.' This confirmation reassures the user that the IP address has been blocked and allows them to undo the action if necessary.

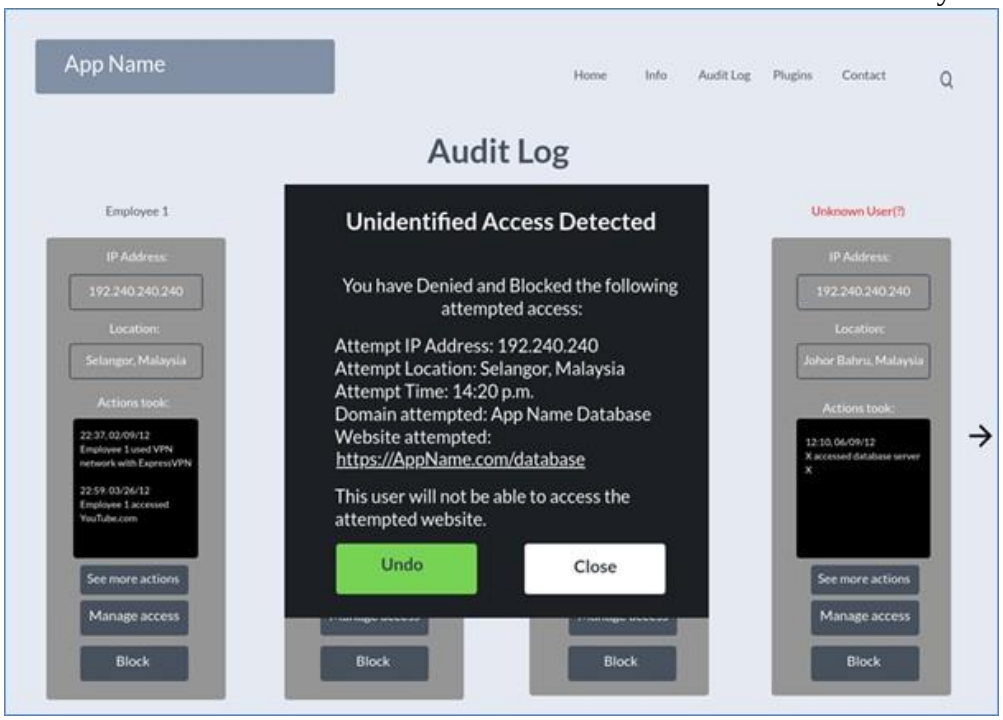

Figure 6 shows undo an action

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume VIII Issue X October 2023

B. Employees/Users

This page shows if an employee is accessing a database without authorisation and the data will be registered in the audit log of a security engineer, thus an automated notification alert marked in red stating 'Access Restricted' will be displayed on the employee's screen restricting their access and remain blocked from that particular page as they are not given the authority to access the specific database, file, website or software. Giving the user only the chance to exit the page or access a different page.

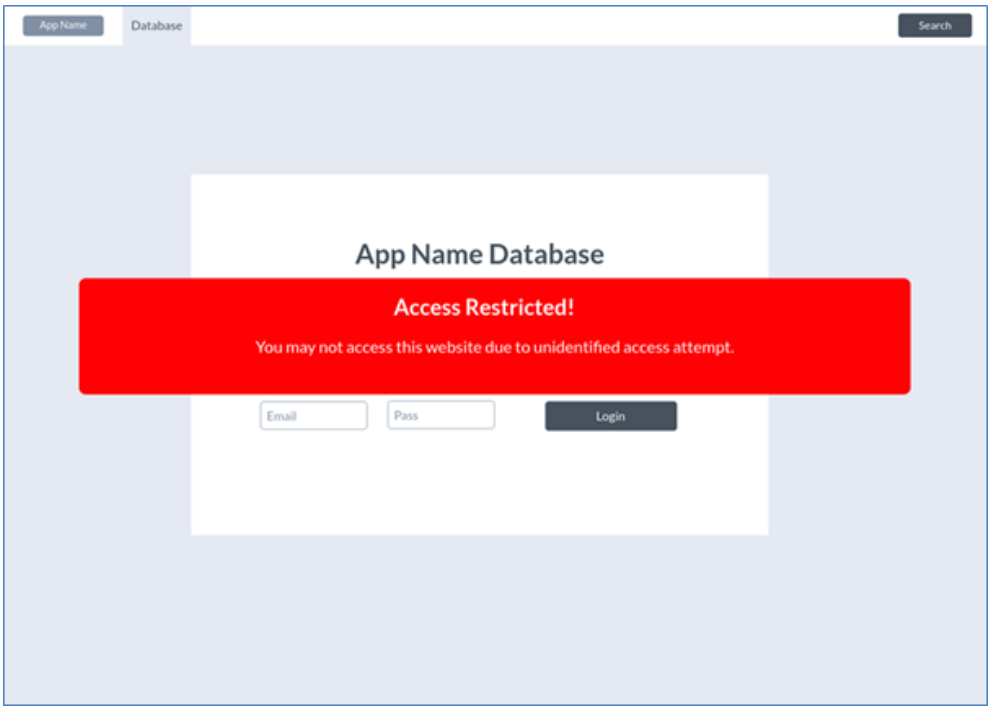

Figure 7. shows the access restricted.

The blocked page is where an employee attempts to access a page and can be blocked at any time. The employee's action will be logged in the audit log by a security engineer. Upper management can review this log from their end and has the capability to block the action instantly.

This action triggers a notification alert on the user's screen, displaying 'You have been blocked from accessing this page.' The user is then presented with the option to either request access or exit the page.

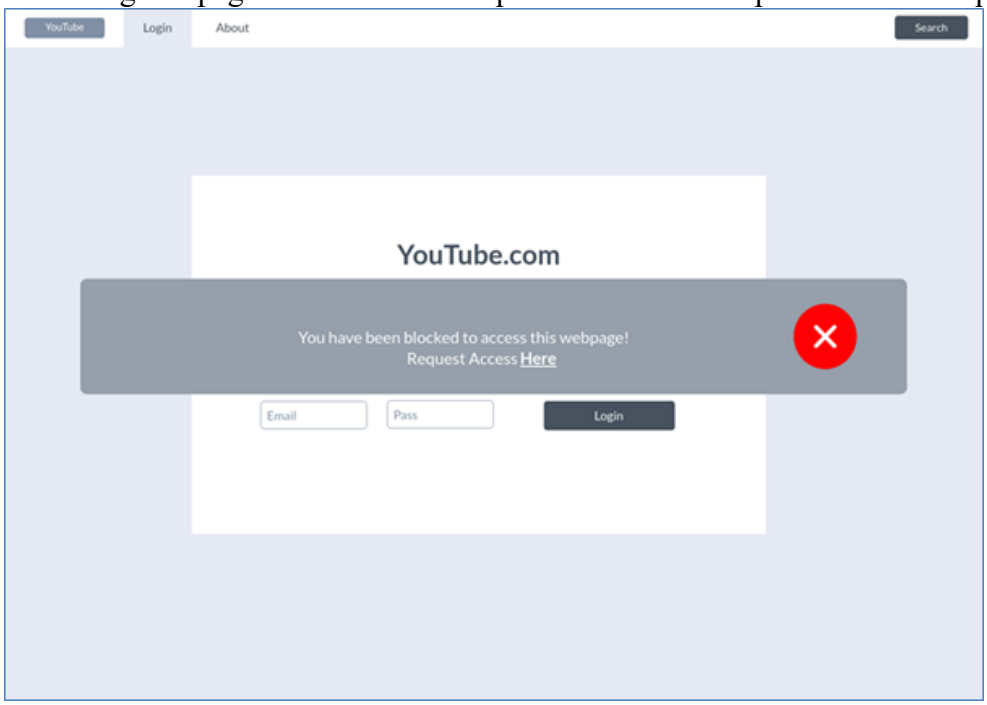

Figure 8 shows blocked access.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume VIII Issue X October 2023

This page is the 'request denied' page, which is shown to employees if their request to access a certain page is denied by upper management.

Consequently, an alert stating 'You have been blocked from accessing this webpage! Your request has been denied' will be displayed to the user, leaving them with no option but to exit or access a different page.

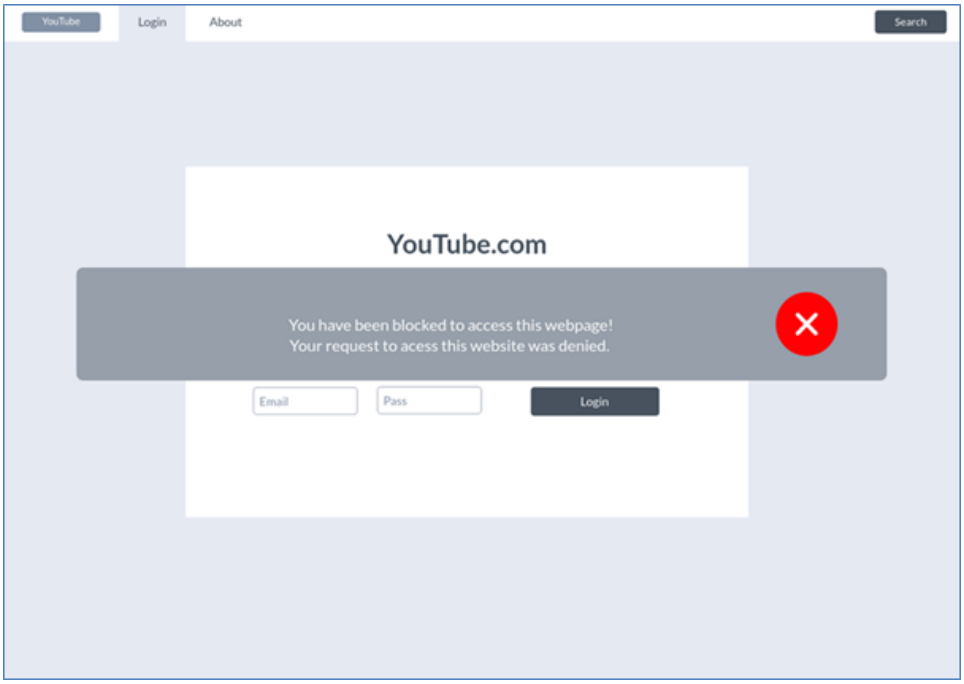

Figure 9 shows the request denied.

This is a blocked page that will only appear to users who have been denied access to everything, essentially being blocked from accessing any file, software, database, or website. This can occur when upper management blocks their access or when they successfully attempt to access a restricted file for which they do not have authorization. Consequently, a red alert will state, 'Your account has been blocked. You have attempted to access this website illegally.

Please contact the IT department for further action,' leaving the user with no other option than to contact the IT department.

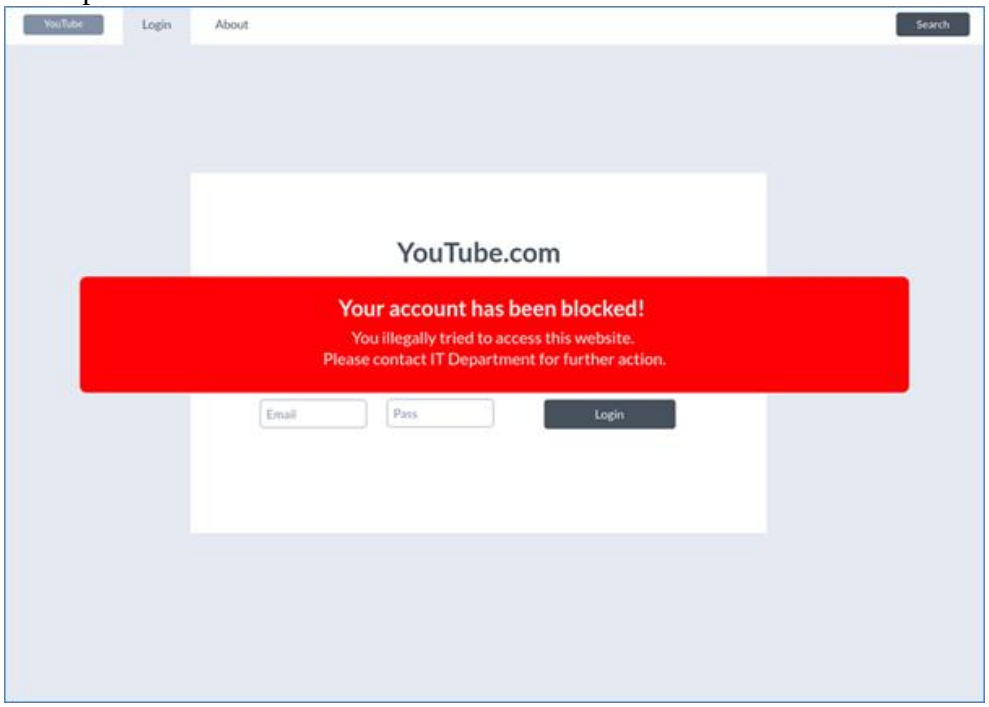

Figure 10 shows the account blocked.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume VIII Issue X October 2023

CONCLUSION

In the dynamic realm of cyber threats, ensuring the security of digital assets is of paramount importance for organizations globally. This paper underscores the critical role of access control applications in fortifying defenses against cyber intrusions. Through an in-depth exploration of modern access control mechanisms, we emphasize their significance in preventing unauthorized access and upholding data integrity. Real-world scenarios further illustrate the effectiveness of stringent access control measures in countering cyber threats and lessening their potential repercussions. However, the implementation of these systems is not without challenges, such as scalability, privilege management, and system resilience. Our research accentuates the vital nature of access control in the digital era, offering practical insights to bolster organizational defenses against the omnipresent cyber threat landscape. Periodic updates to automation processes are crucial to ensure data security, preserving its authenticity, confidentiality, and preventing potential misinformation. Integrating access control into security strategies can address these concerns, but there's a caveat: unintended permissions could be granted. To counteract this, we advocate for solutions like multifactor authentication as a promising future measure.

In summation, the sanctity of information security is pivotal in safeguarding an organization's data and intellectual assets from unauthorized breaches, modifications, or disclosures that could jeopardize its reputation or assets. Building a robust security framework is an ongoing endeavor, necessitating continuous learning, enhancement, and adaptation to each organization's unique challenges and solutions. While the specifics may vary, the overarching goal remains consistent: data protection. As technology advances, so do cyber threats, making data breaches and security lapses almost inevitable. Proactively establishing a robust security posture, rather than reacting post-breach, is essential. The ultimate aim is to shield data while minimizing the impact of attacks to an acceptable threshold. While threats are inevitable, a well-structured security strategy can mitigate risks, fortifying the organization's defenses and safeguarding its invaluable data.

Our top recommendation for addressing security concerns within an organization is the integration of access control technology. But why is it deemed so vital? The primary advantage is its ability to restrict access to sensitive data exclusively to authorized personnel, thereby minimizing potential misuse, and reducing the likelihood of data breaches. By incorporating this feature into an application, it enhances the company management's ability to monitor data interactions, including who accesses it, when, and for what purpose. Access control is paramount in security measures, particularly in monitoring employee actions (Martin, 2019). Notably, in the absence of security engineers, access control steps in. It also offers the added benefit of reducing the need for on-site security staff, making it a cost-effective and efficient solution. One of the standout features of access control is its capability for automated management, ensuring data protection based on user access. Therefore, a security application equipped with robust access control, which can autonomously detect and log unusual activities, is instrumental in warding off potential cyber threats.

REFERENCES

1. Ahn, G., Hu, H., Lee, J., & Meng, Y. (2010). Representing and reasoning about web access control policies. IEEE. https://ieeexplore.ieee.org/document/5676253
2. Alshawi, A., Al-Razgan, M., AlKallas, F. H., Bin Suhaim, R. A., Al-Tamimi, R., Alharbi, N., & AlSaif, S. O. (2022). Data Privacy during pandemics: A systematic literature review of covid-19 smartphone applications. PeerJ Computer Science, 7. https://doi.org/10.7717/peerj-cs.826
3. Clancy, R. (2022, October 12). What is broken access control vulnerability? EC-Council. https://www.eccouncil.org/cybersecurity-exchange/web-application-hacking/broken-access-control-vulnerability/
4. Colombo, P., & Ferrari, E. (2019, January 24). Access Control Technologies for Big Data Management Systems: Literature review and future trends. Cybersecurity. https://cybersecurity.springeropen.com/articles/10.1186/s42400-018-0020-9

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume VIII Issue X October 2023

5. Cross, C., Parker, M., & Sansom, D. (2018). Media discourses surrounding 'non-ideal' victims: The case of the Ashley Madison data breach. Media, Culture & Society, 25(1). https://doi.org/10.1177/0269758017752410
6. Cybercrime module 10 key issues: Cybercrime that Compromises Privacy. (2019). UNODC. https://www.unodc.org/e4j/en/cybercrime/module-10/key-issues/cybercrime-that-compromises-privacy.html
7. Cybersecurity remains one of Malaysia's top concerns, says Hamzah. (2022, March 28). Free Malaysia Today. https://www.freemalaysiatoday.com/category/nation/2022/03/28/cyber security-remains-one-of-malaysias-top-concerns-says-hamzah/
8. Dr. S., Mohanavel. (2021). Prevention from cyber security vulnerabilities in COVID-19 pandemic situation.
9. Duchamps, W. (2022, July 22). 9 common access management myths debunked. LinkedIn. https://www.linkedin.com/pulse/9-common-access-management-myths-debunked-ward-duchamps/
10. Eian, I. C., Yong, L. K., Li, M., Qi, Y. H., & Z, F. (2020). Cyber attacks in the era of COVID-19 and possible solution domains. Preprints. https://doi.org/10.20944/preprints202009.0630.v1
11. Georgescu, T. (2021, May 14). A study on how the pandemic changed the Cyber security Landscape. Research Gate. https://www.researchgate.net/profile/Tiberiu-Georgescu/publication/350833004 A Study on How the Pandemic Changed the Cyber security Landscape/links/609e5ee2458515c2658d6ec1/A-Study-on-How-the-Pandemic-Changed-the-Cyber security-Land scape.pdf
12. Global Fraud Report 2021. (2022). Cyber source. https://www.cybersource.com/content/dam/documents/campaign/fraud-report/global-fraud-report-2021.pdf
13. Goh, J., Kang, H., Koh, Z. X., Lim, J. W., Ng, C. W., Sher, G., & Yao, C. (2020, February). CyberRisk Surveillance: A Case Study of Singapore. International Monetary Fund. https://www.imf.org/-/media/Files/Publications/WP/2020/English/wpiea2020028-print-pdf.ashx
14. Griffiths, C. (2022, November 21). The latest 2022 cyber crime statistics. AAG IT. https://aag-it.com/the-latest-2022-cyber-crime-statistics/
15. He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health Care Cyber security Challenges and Solutions Under the Climate of COVID-19: Scoping Review. JMIR. https://doi.org/10.2196/21747
16. Martin, J. A. (2019, August 21). What is access control? A key component of data security. CSO Online. https://www.csoonline.com/article/3251714/what-is-access-control-a-key-component-of-data-security.html
17. McGraw, G. (2015, October 01). McGraw: Seven myths of software security best practices. Tech Target. https://www.techtarget.com/search security/opinion/McGraw-Seven-myths-of-software-security-best-practices
18. Moore, M. (2022, August 1). Top Cyber security Threats in 2022. University of San Diego. https://onlinedegrees.sandiego.edu/top-cyber-security-threats/
19. Neto, N. N., Madnick, S., Paula, A. M., & Borges, N. M. (2020, March 17). A Case Study of the Capital One Data Breach. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3542567
20. Parkinson, S., & Khan, S. (2022, April 27). A survey on empirical security analysis of access control systems: A real-world perspective. ACM Digital Library. https://dl.acm.org/doi/10.1145/3533703
21. Pranggono, B., & Arabo, A. (2020, October 3). Covid-19 pandemic cyber security issues. Wiley Online Library. https://onlinelibrary.wiley.com/doi/10.1002/itl2.247
22. National Cyber Security Centre. (2015, October 13). Reducing your exposure to cyber attack. https://www.ncsc.gov.uk/information/reducing-your-exposure-to-cyber-attack
23. Roa, R. E. (2017, June). RANSOMWARE ATTACKS ON THE HEALTHCARE INDUSTRY. ProQuest. https://www.proquest.com/openview/53149e53ad84f1cfeeba87b0a8c9d414/1?pq-origsite=gscholar&cbl=18750
24. Rogers, G., & Ashford, T. (2015). Mitigating Higher Ed Cyber Attacks. ERIC. https://files.eric.ed.gov/fulltext/ED571277.pdf