ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr671

All-in-One Identity Protection and Phishing Defence System

Aryan Khandelwal[1]; Sarvesh M Rao[2]; Kaavya B[3]; Dr. U. Surendar[4]

[1;2;3]B. Tech 4th Year; [4]Assistant Professor,

[1]Department of CSE, SRMIST, Chennai, India
[2]Department of CSE, SRMIST, Chennai, India
[3]Department of CSE, SRMIST, Chennai, India
[4]Department of CSE, SRMIST, Chennai, India

Publication Date: 2025/04/26

Abstract: SecureBrowse is an extension of Google Chrome designed to address the growing threats of cybersecurity such as phishing, weak passwords and identity theft. Combine three key features: Phishing detection for real time alerts on malicious websites, password administrator for safe credential storage and identity protection to safeguard the confidential user data. With an emphasis on accessibility and ease of use, Securebrowse is perfectly integrated into daily navigation while guaranteeing robust security through advanced encryption and cybersecurity practices. This project empowers users to navigate the digital world safely and confidently.

Keywords: *Secure Browse, Phishing Detection, Identity Protection.*

How to Cite: Aryan Khandelwal; Sarvesh M Rao; Kaavya B; Dr. U. Surendar (2025). All-in-One Identity Protection and Phishing Defence System. *International Journal of Innovative Science and Research Technology*, 10(4), 1462-1467. https://doi.org/10.38124/ijisrt/25apr671

I. INTRODUCTION

In the current interconnected digital world, cyber threats such as phishing attacks, identity theft and poor password management continue to evolve, raising significant risks for people, companies and organizations equally. As the most confidential data is shared and stored online, the need for a unified and robust cyber security solution has never been more critical. To address these growing concerns, we propose a **identity and defence protection system of Phishing,** a comprehensive and easy -to -use platform designed to strengthen digital security from multiple angles.

This innovative solution perfectly integrates phishing **advanced**, Safe **password management** and Identity **protection** in a single application, offering users a centralized centre to administer and safeguard their digital identities. Taking advantage of Avant -grade technologies such as **end -to -end encryption**, Automatic **learning algorithms** and **Multifactor authentication (MFA)**, the system actively detects and neutralizes threats in real time while guaranteeing that credentials and personal data of users remain private and safe.

The **phishing detection** module uses automatic learning to analyse emails, websites and other communication channels for suspicious patterns, alerting users before they can be victims of fraudulent attempts. Simultaneously, the **Password Administrator** stores safe and unique passwords for each account, automatically generates strong credentials and eliminates the need to remember multiple session, significantly reducing the risk of reuse of credentials and brute force attacks.

In addition, the identity **protection component** continuously monitors the dark website and data violations due to compromised personal information signs, allowing rapid action when suspicious activity is detected. Users receive alerts and recommendations to mitigate any potential damage, preserving their online reputation and financial welfare.

Either for people looking for tranquillity in their navigation or daily organizations that strive to comply with cybersecurity regulations and protect their interested parties, this system that covers everything offers a scalable, reliable and proactive defence against the growing landscape of cyber threats.

Ultimately, our solution allows users to tools and knowledge they need to navigate the digital world safely, with confidence and safe.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr671

II. LITERATURE SURVEY

- Luther Martin's paper, "Identity-based Encryption: From Identity and Access Management to Enterprise Privacy Management," describes how IBE could simplify key management based on user identities instead of PKIs. Implicit key authentication and built-in recovery of keys from the system also make enhanced security and privacy possible. In addition to these, HIBE is a variant of IBE, which allows delegating the generation of keys across organizational levels. However, the key escrow problem remains an open issue because the PKG may decrypt all messages.

- Ishaq Azhar Mohammed's paper on 'Intelligent Authentication for Identity and Access Management' is interesting. As this discusses the IAM benefits in an enterprise, especially keeping the authentication issue as the core, it points out the challenges of effective password management and IT redundancy-impacting productivity, security, and efficiency. This solution introduces an intelligent approach to IAM, consolidating user identities into one identity with unified roles and rules, easing administration but at the same time enhancing security. It tries to probe into how methods like multifactor authentication can help streamline processes.

- This paper by Ishaq Azhar Mohammed 'Identity and Access Management as Security-as-a-Service from Clouds,' discusses IAM solutions offered as a SECaaS from cloud platforms. The paper examines how IAM from the cloud benefits from high-security advantages. The paper likely covers the benefits, challenges, and associated implementation aspects of the IAM service delivered over the cloud.

- Abikoye et al. (2019) offer a paper, 'Modified Advanced Encryption Standard Algorithm for Information Security' published in Symmetry. The paper is likely a means through which improvements are offered to the AES algorithm to enhance information security. The paper would probably discuss the type of modifications done to the AES to solve particular security issues or performance enhancement. It is probably working on the approach of offering a more robust type of encryption algorithm for secure data transmission and storage.

- A Survey of Access Control and Data Encryption for Database Security' is a paper written by Khalaf and Kadi, and published in the Journal of King Abdulaziz University. This paper would have given mechanisms for access controls and data encryption techniques that enhance security in a database. It may include many models of access and ways of data encryption in the databases. Probably the focus is on surveying existing approaches and their effectiveness in ensuring database security.

- Bhajantri and Mujawar published their paper, 'A comprehensive review of access control mechanism based on attribute-based encryption scheme for cloud computing', in the International Journal of Advanced Pervasive and Ubiquitous Computing (IJAPUC). The paper would most probably give an in-depth review of the access control mechanisms employed by attribute-based encryption in cloud computing environments. The paper may describe various ABE schemes with their application in controlling access to cloud resources with attributes. It is more likely to focus on the notion of assessing the success and suitability of the application of ABE-based access control over security in cloud environments.

- Kapil et al. (2020) have presented an attribute-based score encryption (HE) algorithm to secure big data in the Hadoop distributed file system (HDFS). This algorithm combines ABE with key encryption to protect the data and thwart brutal force attacks. Instead of merely encrypting the data, it also generates "scores" that are deceptive but attractive appearing. A few of the issues identified are handling the complexities of an amalgamation of ABE and HE, performance with large amounts hosted in HDFS, and efficient key distribution and management. The current paper addresses the problem that big data systems such as Hadoop, besides the large scale of data, have to deal with and lead to the necessity of balancing between security and computing overhead.

- Heading, Katsikeas, and Lagerström conducted an extensive literature review in 2023 of related research communities in the context of cybersecurity vulnerability assessment. They map the landscape of research activities, identify key topics, methodologies, and collaboration networks within that field and outline a wide variety of approaches used to assess vulnerability, from technical analysis of policy and management perspectives. The issues noted here involve issues concerning fragmentation of research activities, which may affect comprehensive strides toward overall understanding as well as the accelerating rate of threats, which are indeed outpacing the assessment methodologies used. Other concerns in this regard include not standardizing methodologies across the distinct domains or disciplines and a stronger need for more extensive interdisciplinary involvement to adequately tackle involved cybersecurity issues.

- Varsha and Suryateja (2014) also discussed the utility of using attribute-based encryption along with Advanced Encryption Standard to enable and promote wide-scale sharing of PHR in a cloud environment. Their approach is based on ABE for access according to attributes of the users, so that the encrypted data can be maintained within the reach of an attacker, along with the AES-based secure mechanism for encryption of the actual data. This double layer of encryption approach aims at improving the security and accessibility in managing PHR. Their work highlighted some of the issues concerning core and distribution management, scalability when growing with the users and attributes, as well as the trade-off towards security and system performance. It also involved legitimate access that was to protect health information in a dynamic cloud environment.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr671

- A new cryptographic approach to the access control of encrypted data has been introduced, as presented in Goyal, Pandey, Sahai, and Waters's "Characteristic Encryption for Access Control of Encrypted Data" in 2006. The authors introduce the concept of Attribute-Based Encryption (ABE), through which access policies can be defined based on user attributes rather than identities. It allows fine access control wherein data will be accessed only by users with a given set of credentials. An efficient scheme of ABE construction is presented, and its practical application in different scenarios that require flexible and reliable data sharing is demonstrated. The proposed scheme improves the ability to handle and protect sensitive data in a decentralized environment.

- In the paper by Bethencourt, Sahai, and Waters in 2007, there is a new type of Attribute-Based Encryption called Ciphertext-Policy ABE abbreviated as CP-ABE. In this process, a ciphertext access policy is defined for the encryption process. This is made such that it allows the data owner to make a decision on which one has the privilege of decrypting the data according to its attributes. This technique allows flexibility and security in managing access without relying on underlying cryptographic primitives, making it quite suitable for application scenarios requiring access control with sharing data and protecting them. The authors give a constructive complete implementation of CP-ABE to illustrate the efficiency and effectiveness that such a structure brings about in terms of sensitive information access within distributed systems and also discuss how the scheme offers resistance against fusion attacks, thereby making this structure tougher in practical application.

- The paper proposed by Attrapadung and Imai entitled "Dual-policy attribute-based encryption" is a paper that proposes an extended notion in Attribute-Based Encryption (ABE), where key-policy ABE and ciphertext-policy ABE are merged into the same framework. Dual-policy ABE consequently enables policies that have been defined within a user's keys to be compatible with policies existing in the ciphertext, thus creating a higher expressiveness level in any access control framework. The presented construction and security analysis by the authors in their scheme will demonstrate the applicability of their scheme in handling more complex access control scenarios. Thus, this approach will extend the applicability of ABEs within diverse environments where increasingly sophisticated fine-grained access management is required.

- Take a look at by using Bendoly and Swink (2007) explores the impact of information entry on mission control conduct, performance, and perceptions. It highlights how getting right of entry to applicable and timely facts can have an effect on selection-making, venture execution, and the overall efficiency of control practices. The authors found that accelerated records get right of entry to enhance challenge overall performance by facilitating higher coordination and verbal exchange. Moreover, it moderates the connection between managerial conduct and outcomes, improving each the perceptions of fulfilment and actual mission results. The study emphasises the significance of obvious and available facts structures in powerful project control.

- Jarvenpaa and Ives (1994) look at the concept of the global network agency, focusing on the possibilities and challenges presented by records management in an increasingly interconnected international network. They argue that rising technologies and global networks allow businesses to function extra flexibly and effectively across geographic boundaries. However, this shift additionally brings challenges, together with handling various statistics structures, ensuring data consistency, and overcoming cultural and organizational variations. The authors emphasize the want for powerful statistics management techniques to harness the capacity of world networks whilst addressing the complexities of coordination, verbal exchange, and managing in a decentralized organizational shape.

- Mohammed, Hassan, and Yusuf Mohammed (2018) talk about the improvement and implementation of an internet-based totally Identity and Access Management (IAM) system for corporations. The paper highlights the crucial position of IAM in making sure stable access to organizational sources by using coping with user identities and controlling get entry to rights. The authors advise a web-based totally answer that complements safety and simplifies the method of managing person authentication, authorization, and role-based totally get admission to across numerous corporation structures. Their technique specializes in scalability, ease of use, and flexibility to deal with the developing complexity of corporation environments whilst maintaining high standards of security and person control.

III. IMPLEMENTATION

➢ *Download & Install*

The user downloads and installs the Chrome extension from the official store.

➢ *Log in*

User log in using their credentials to access the features.

➢ *Enable Features*

The user selects and enables one or more of the following features:

- Identity Protection
- Password Manager
- Phishing Protection

➢ *Identity Protection (If Enabled)*

- Scans for tracking cookies and removing them.
- Blocks ads to enhance privacy.
- Applies additional security measures to prevent data leaks.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr671

➢ *Password Manager (If Enabled)*

- Auto-fill login credentials on saved websites.
- Securely stores and encrypts user passwords.
- Provides quick and seamless access to accounts.

➢ *Phishing Protection (If Enabled)*

- Detects and blocks phishing websites in real time.
- It prevents users from entering sensitive information on malicious sites.
- Provides alerts and warnings against online threats.

➢ *Continuous Protection*

- The extension runs in the background, ensuring ongoing security.
- Updates automatically to protect against new threats.

IV. RESULT

Fig 1 Secure Browse Extension Popup Home Page showing all the available Options.

Fig 2 A Page with an AD Placement when the Identity Protection Feature is Disabled

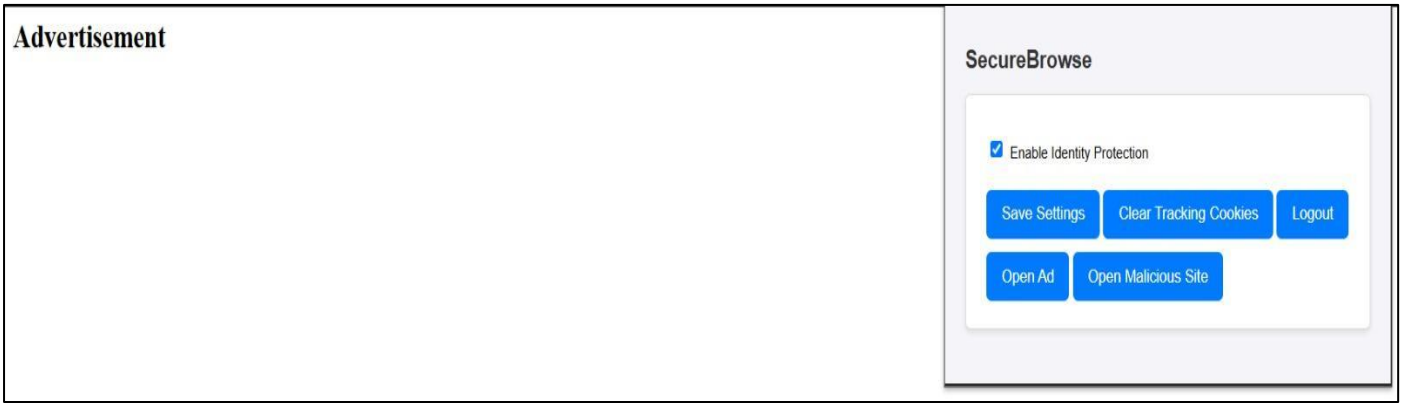

Fig 3 A Page with AD Placement when the Identity Protection Feature is Enabled.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr671

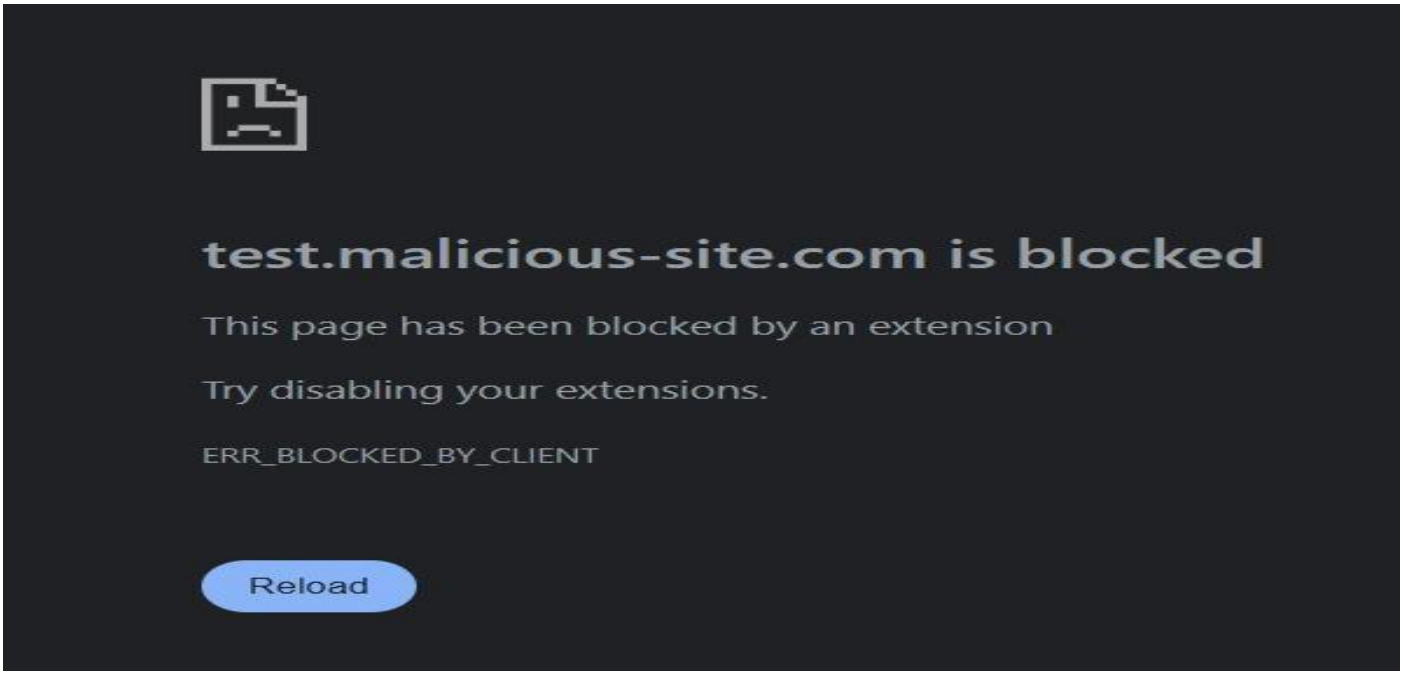

Fig 4 Site Getting Blocked by the Extension when Visiting a Malicious Site to Prevent Phishing Threats

V. DISCUSSION

To effectively address cybersecurity threats, the **All-in-One Identity Protection and Phishing Defense System** is structured into the following key modules:

➢ *Phishing Detection Module*

- Identifies and blocks phishing websites using **machine learning** and **real-time threat intelligence** from databases like PhishTank.
- Analyzes website URLs and content to detect suspicious behavior.
- Provides alerts and warnings to users about potential phishing threats.

➢ *Password Manager Module*

- Securely stores and manages user credentials using **encryption algorithms** like AES-256.
- Generates strong passwords and auto-fills login credentials to prevent weak password usage.
- Implements **multi-device synchronization** for seamless access.

➢ *Identity Protection Module*

- Enhances security using **Two-Factor**
- **Authentication (2FA)** via SMS or authenticator apps.
- Detects unauthorized login attempts and notifies users of suspicious activity.
- Implements **OAuth-based secure authentication** for third-party login protection.

➢ *User Authentication & Authorization Module*

- Uses **JWT (JSON Web Tokens)** for secure user sessions.
- Implements **role-based access control (RBAC)** to restrict unauthorized access.
- Supports **biometric authentication (optional)** for an added layer of security.

➢ *Security Monitoring & Reporting Module*

- Tracks and logs security events, including phishing attempts and login activities.
- Generates detailed reports on **user activity and security threats**.
- Provides real-time notifications for detected security breaches.

➢ *Admin Dashboard & User Interface Module*

- A user-friendly dashboard for managing stored passwords, security settings, and phishing reports.
- Allows users to customize security preferences.
- Provides a visual representation of detected threats and security status.

VI. CONCLUSION

The All-in-One Identity Protection and Phishing Defense System is a comprehensive cybersecurity solution that addresses the growing threats of phishing attacks, weak password management, and identity theft. By integrating phishing detection, secure password storage, and identity protection, this system enhances online security and provides users with a safer digital experience. The implementation of machine learning, encryption, and multi-factor authentication ensures robust protection against evolving cyber threats. This project not only helps individuals and organizations safeguard their sensitive data but also promotes better security practices by encouraging the use of strong passwords and real-time phishing detection. By providing a user-

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr671

friendly and efficient security solution, this system contributes to the larger goal of cyber threat mitigation and a more secure digital environment .With its scalable and adaptable design, the proposed system can be further enhanced with additional security features, making it a valuable tool for protecting users against emerging cyber risks in the ever-evolving digital landscape.

REFERENCES

[1]. Martin, L. (2007). Identity-based Encryption: From Identity and Access Management to Enterprise Privacy Management. Information Systems Security, 16(1).

[2]. Mohammed, I. A. (2017). Systematic review of identity access management in information security. International Journal of Innovations in Engineering Research and Technology, 4(7), 1-7.

[3]. Azhar, I. (2017). Identity and Access Management as Security as a Service from Clouds. International Journal of Creative Research Thoughts (IJCRT), ISSN 2320-2882.

[4]. Abikoye, O. C., Haruna, A. D., Abubakar, A., Akande, N. O., & Asani, E. O. (2019). Modified advanced encryption standard algorithm for information security. Symmetry, 11(12), 1484.

[5]. Khalaf, E. F., & Kadi, M. M. (2017). A survey of access control and data encryption for database security. Journal of King Abdulaziz University, 28(1), 19-30.

[6]. Bhajantri, L. B., & Mujawar, T. N. (2019). A comprehensive review of access control mechanism based on attribute based encryption scheme for cloud computing. International Journal of Advanced Pervasive and Ubiquitous Computing (IJAPUC), 11(3), 33-52

[7]. Kapil, G., Agrawal, A., Attaallah, A., Algarni, A., Kumar, R., & Khan, R. A. (2020). Attribute-based honey encryption algorithm for securing big data: A Hadoop distributed file system perspective. PeerJ Computer Science, 6, e259.

[8]. Heiding, F., Katsikeas, S., & Lagerström, R. (2023). Research communities in cyber security vulnerability assessments: A comprehensive literature review. Computer Science Review, 48, 100551.

[9]. Varsha, B. S., & Suryateja, P. S. (2014). Using attribute-based encryption with advanced encryption standard for secure and scalable sharing of personal health records in the cloud. *International Journal of Computer Science and Information Technologies*, 5(5), 6395-6399. Proceedings 7* (pp. 168-185). Springer Berlin Heidelberg

[10]. Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006, October). Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM Conference on Computer and Communications Security* (pp. 89-98).

[11]. Bethencourt, J., Sahai, A., & Waters, B. (2007, May). Ciphertext-policy attribute-based encryption. In *2007 IEEE Symposium on Security and Privacy (SP'07)* (pp. 321-334). IEEE.

[12]. Attrapadung, N., & Imai, H. (2009). Dual-policy attribute-based encryption. In *Applied Cryptography and Network Security: 7th International Conference, ACNS 2009, Paris-Rocquencourt, France, June 2-5, 2009.

[13]. Bendoly, E. and Swink, M., 2007. Moderating effects of information access on project management behavior, performance and perceptions. *Journal of Operations Management*, *25*(3), pp.604-622.

[14]. Jarvenpaa, S.L. and Ives, B., 1994. The global network organization of the future: Information management opportunities and challenges. *Journal of management information systems*, *10*(4), pp.25-57.

[15]. Mohammed, K.H., Hassan, A. and Yusuf Mohammed, D., 2018. Identity and access management system: a web-based approach for an enterprise.