GAP INDIAN JOURNAL
OF FORENSICS AND BEHAVIOURAL SCIENCES
(ISSN – 2582-8177)
Globally peer-reviewed and open access journal.

STRENGTHENING ONLINE SECURITY THROUGH A COMMUNITY-DRIVEN CYBER THREAT DATABASE: A COLLECTIVE DEFENCE APPROACH

Aditya Bhadouria[1], Shivam Patel[2], Kiranbhai R Dodiya[3*], Akash Khunt[4]

[1]M.sc Cyber Security NSIT-IFSCS, Ahmedabad, Gujarat, India.
(adityabhadouriaoff@gmail.com)

[2]M.sc Cyber Security NSIT-IFSCS, Ahmedabad, Gujarat, India.
(shivampatel9051@gmail.com)

[3*]Assistant Professor, (Cyber Security) NSIT-IFSCS, Ahmedabad, Gujarat, India.
(kirandodiya01@gmail.com)

[4]Assistant Professor, (Cyber Security) NSIT-IFSCS, Ahmedabad, Gujarat, India.
(akpatel950@gmail.com)

Abstract

As we all know, cyberspace encompasses all spheres of human activities in today's world, which has completely altered social interactions and every facet of life, making cybersecurity of utmost importance. The scope of the present investigation encompasses the problem of establishing a self-help-oriented database that should impede cyber assaulters on the web address. The proposed database shall be a common storage for hackers' IP addresses. The websites must be provided with this information to protect themselves. This action will help the websites and those using them implement quick remedial actions and improve the security of a common network of websites connected to the system. The approach presented in these recommendations' places special stress on the issue of collective safety as the basis for effective defence against the evolving nature of aggressive actions in cyberspace. By blocking access to the resources of confirmed aggressors, this collaborative effort makes each resource safer and reduces the chance of an attack being carried out in the future. This security database is vital because cybercriminals are always out to improve their performance within the restrained boundaries of the net. The study discusses the necessity of determining the organisational security measures, such as IP allowlists and block lists, and relocation of the virtual location of users. Not only a community-centred approach but also these processes create the system so that it is protective against a cyber attack, and the system changes continuously and allows healthy adaptations within it. The paper also demonstrates how fast-changing daily legal and external environments force individuals to change cyber termination security. This shared database makes proactive detection and blocking of possible attackers possible for websites of all sizes. This project intends to democratise this technique for widespread adoption, taking inspiration from industry heavyweights like Google and Microsoft, which have successfully adopted similar systems.

Keywords: *Cybersecurity, Community-driven database, Hacker IP addresses, Malicious attacks, Threat Intelligence, Centralized repository, and Authentication.*

1. INTRODUCTION

1.1 Overview of Cyber Threat Landscape

The digital threat is rapidly evolving and reaching unprecedented complexity and danger. Cyberattacks, now more sophisticated than ever, pose a significant threat to individuals and corporations. Hackers are employing advanced techniques, including ransomware, phishing, and Distributed Denial of Service (DDoS) attacks, to breach networks and steal sensitive data. Unauthorised access attempts are becoming increasingly common, even on websites with robust security measures. This urgent situation underscores the critical need for a collective defence approach[1].

GAP INDIAN JOURNAL
OF FORENSICS AND BEHAVIOURAL SCIENCES
(ISSN – 2582-8177)
Globally peer-reviewed and open access journal.

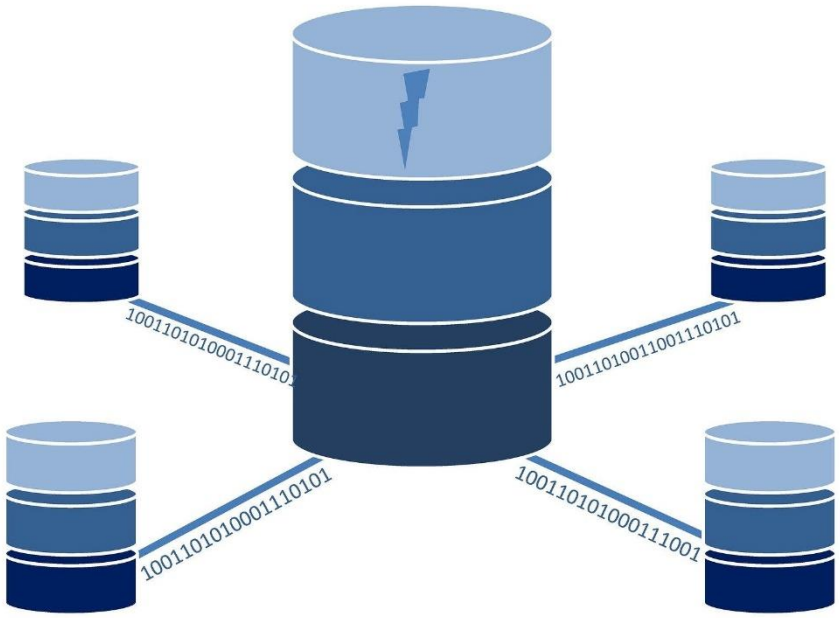

Figure 1: Partner Websites Sharing their Data-Base to the Community Data-Base.[2]
Figure 1 shows the Contribution of Databases to the Community Database.

1.2 Importance of Cybersecurity in the Digital Age

We increasingly depend on digital platforms, so implementing strong cybersecurity safeguards is paramount. Maintaining the integrity of online services and safeguarding sensitive data are essential for organisations, communities, and the public. Proactive defences are, therefore, necessary to stop cyberattacks before they can do much damage. We suggest building a Community Hacker IP Database to meet this demand. Through collaborative endeavours, websites can log potential attackers' IP addresses and share information on unauthorised access attempts. Member websites can improve their security and resilience in the digital world by uniting against cyber threats by combining their information and experience. We hope that by enlisting everyone in this common defence, we will be able to keep the community safe from the ever-increasing threats posed by cyberattacks.[3]

2. RELATED WORK

Due to increasing cyberattacks targeting mainly login credentials, the growth spurs intensive use of advanced protective measures in safeguarding critical internet infrastructures. Several research works have been focused on studying various ways against unwanted access, with a general focus on the effectiveness of successful login page security.[4] Ignatius and Yusuf proved that brute-force attacks can be possible on the CUDA platform; they also highlighted that massive computation is required to support these operations. Their conclusions emphasise incorporating cutting-edge hardware defences like GPUs to avoid serious cyberattacks. The authors also tried dictionary and GPU-based brute force attacks against hashed passwords: Laatansa et al. used to underlie the role that password hashing algorithms like SHA-1 play in reducing attack risk. Such advances notwithstanding, vulnerability is still in place, as Zhendong and Peng noted when they presented their hybrid CPU-FPGA system to improve the energy efficiency of password recovery activities.[5] These advances highlight how hard it is to maintain safe authentication procedures in a changing quickly threat landscape. More sophisticated algorithms for generating passwords are being recommended alongside the concern about the weakness of user-created passwords and their susceptibility to dictionary or brute-force attacks. Multi-layered defensive techniques, including 2-FA and password-based security, have been studied to enhance login security.[6] While 2-FA is very effective, usability has become a barrier to the widespread use of this technique. The literature focuses mainly on balancing stringent security policies against a better user experience. This is especially a challenge at work, where most users are subjected to the will of the security policy. New technologies that will probably improve the detection systems of threats include ML and AI. This study shows that such tools are very effective in an environment like smart grids, where NIST underlines the significance of the CIAA concepts: confidentiality, integrity, availability, and accountability [7]. Nevertheless, the energy sector's vulnerability to cyberattacks has long been a source of great concern because attacks unleashed at smart grids compromise the confidentiality, accessibility, and dependability of infrastructure. The current study promotes the creation of a community-driven IP blocklist database to locate

and disseminate the IP addresses of hackers from various businesses, building on these previously established foundations[8]. Organisations could be able to restrict malicious IP addresses before an attack happens by receiving proactive alerts about potential dangers from such a centralized database[9]. According to earlier research on login page security, rate-limiting and IP address allowlisting/blocklisting techniques are crucial defensive measures. Integrating machine learning with data from the community may make real-time threat identification and response possible[10]. According to previous research studies, threat detection accuracy is much increased if AI and ML are used for predictive analysis of cyber threats. Cooperation around a common IP blocklist might be a feasible, scalable defence against many cyberattacks as the threats evolve and grow in sophistication, especially in complex, networked settings[11].

3. OBJECTIVE OF THIS RESEARCH

A community developed this database to raise the level of security for all the sites that participate in the databases by exchanging vital information regarding cyber threats and establishing a cooperative defence system. Such a community would necessarily strive towards developing a more proactive and resilient cybersecurity network to detect attacks quickly and neutralise them with combined efforts and intelligence. Such a group effort aims to protect both large-sized websites and to present to users an online environment that is safe and secure.

3.1 Key Purposes of the Community Database

Centralised Database for Threat Data:
Therefore, it will be a central place where all IP addresses and hackers' IDs seeking to break into the participants' websites can be collected and archived. This approach is effective for the network in terms of sharing threat intelligence.

Real-time detection and blocking of threats:
Websites in the community can share their security data with the rest of the members in real-time and alert other members to stay alerted by their IP addresses.

Collaborative Security Network:
The network utilises collective intelligence to increase each site's resilience against cyber attacks. The community-driven database creates a collaborative atmosphere that encourages websites to collaborate to improve their security systems.

3.2 Preventive Defence and Constant Adjustment:
A vulnerability of one website alerts other community members' websites to stay updated and on top of the attacker's methodology or tip.

3.2.1 Democratisation of Resources for Advanced Cybersecurity:
The database offers cutting-edge cybersecurity information to any website, from small to large. In this sense, it accumulates resources and intelligence banks, allowing a small website to receive the same security that larger, established platforms receive. Thus, together, these goals build a robust and adaptive defence system to endure constantly changing cyber threat environments[12].

Better protection against internet attacks:
Participating sites can share a database of known hackers to curb the threats before they exploit weaknesses. Real-time detection of threats and response With a community-driven database that delivers real-time information, sites can immediately respond to newly discovered threats, reducing the chance of a successful attack. Enhanced Safety Through CooperationAll that the network does to improve each website's security posture, offering a stronger defence against cyber assaults than the site alone could provide, serves that same end. Constantly Evolving Security:The sites also benefit, as the database holds new information, thus providing a strong defence against the latest hacking tactics.Getting Advanced Resources in Cybersecurity This provides similar high-performance security intelligence to smaller, less wealthy websites, helping to democratise cybersecurity and balance the playing field[13].

Be benevolent toward the safety of the internet:
Suppose they can include it in the community-run database. In that case, websites can contribute to a safer space for everybody by joining the larger effort to make the Internet a safer resource. Such benefits enable sites to stand up in defence better, making the Internet safer and more trustworthy[14].

GAP INDIAN JOURNAL
OF FORENSICS AND BEHAVIOURAL SCIENCES
(ISSN – 2582-8177)
Globally peer-reviewed and open access journal.

4. METHODOLOGY

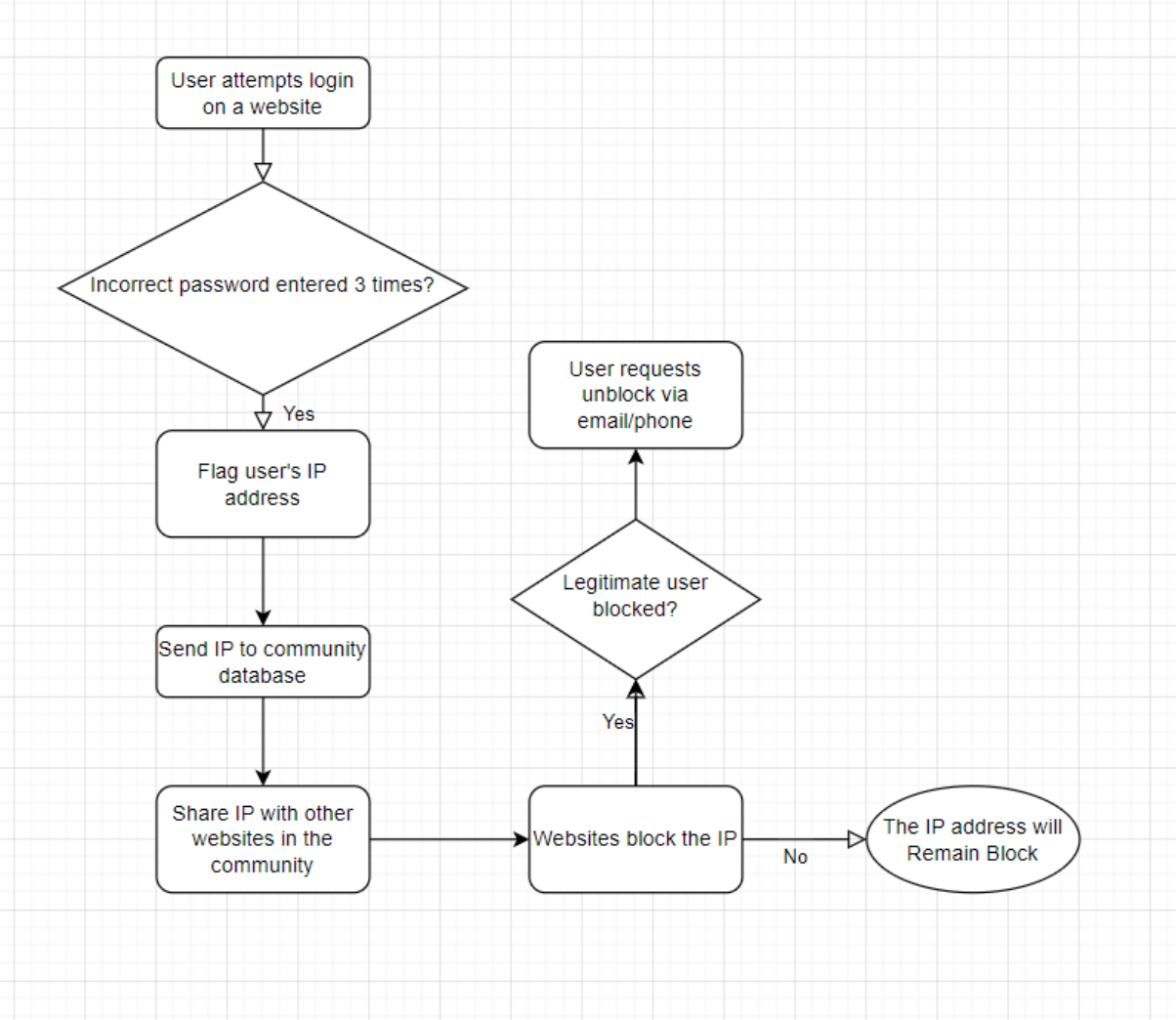

Figure 2: Flow Chart of Community Database

Figure 2 shows a login security system that uses a public database to thwart attempts at unwanted access. It shows two people trying to log into a system. If the user inputs the incorrect password more than three times, an automated code is generated and sent to the user's approved email address or phone number for verification. The graphic also demonstrates the incorporation of a community-driven IP blocklist, which flags and disseminates IP addresses associated with unsuccessful login attempts to the wider community. If a suspect IP address is found, it is added to the database, protecting other linked systems against compromise. If needed, users have the option to unblock certain IPs. By exchanging known harmful IPs, the community database protects several organisations.

4.1 Design of the Central Repository

The foundation of the community-driven database is the central repository. All threat data is gathered, stored, and dispersed from this safe, central location. The design must prioritise high availability to guarantee that participating websites can always access the repository. Additionally, as new websites join the network, they should be able to scale up to handle the growing community data. It should explain the previous updates to the new customers; it's the community blocks and the importance of integrating backup and redundancy data systems to avoid data loss. It should support real-time data sharing, enabling websites to receive and overcome threat intelligence instantly. To ensure the integrity and confidentiality of the data, advanced security mechanisms like encryption and access controls must be implemented.

4.2 Data Collection and Storage Techniques

Data collected comprises information on failed logins, IP addresses, and suspicious activities sourced from websites that form part of the network. To avoid any integration issues, the data has to be standardised. The data is at risk of being hacked anytime when downloaded from the websites to the central repository. Hence,

the downloaded data should be encrypted. Once received, it also has to be encrypted to retain it for safe storage. For example, hashed data can protect the anonymity of potentially sensitive user information. Besides the two considered above, there are two other highly important functionalities of the data storage solutions: handling large volumes of data and real-time quick retrieval and analysis in the threat detection process.

4.3 IP Address Allowlisting and Blocklisting

A list of IP addresses that are banned and allowed will be updated periodically by the repository. Allowlisting is locating and approving trusted IP addresses to provide uninterrupted service for authorised users and systems. On the other hand, blocklisting focuses on malicious IP addresses that have been linked to questionable behaviour patterns, including a pattern of unsuccessful login attempts or known hacking activity. All participating websites have access to these blocked IP addresses, enabling them to proactively stop attacks from these sources. Due to the system's flexibility, websites should be able to tailor allowlisting and blocklisting rules to meet their unique requirements while utilising the network's collective intelligence.

4.4 Authentication and Access Control Measures

Processes of access control and tight measures ought to follow the fact that only authorised people should access and manage the repository. The central repository has to be protected from unauthorised access. A high authentication technique can be developed by the use of a multi-factor authentication technique where validation of the identities of the users is required using various sources. It will reduce the threats caused by insiders because there could be different levels of access depending on what role a user is performing. Such audits and security updates are required to validate the existing measures to combat emerging threats and ensure continued security for the repository.

4.5 Implementation Strategy

4.5.1 Integration with Participating Websites

It must make a seamless link between each site and the community-driven core database. First, secured communication mechanisms, or APIs, are offered to the websites to send data into and receive data from the repository. Changes in authentication and security systems should also be undertaken when integrating the website with the ability to interact with the central database. For example, if the system detects some suspicious login patterns or if it concludes that any IP address was denied access to a particular website, then it must search the central database and automatically take all the necessary steps for the detection of the probable match, like deny access or may activate other security mechanisms, such as MFA or CAPTCHA. The sites need to go into operation without a hitch because more security will be added to the integration in every possible way without disrupting the current infrastructure.

4.5.2 Update Mechanisms for Threat Information

Current threat information is critical in effective defence against emerging online threats. Institute an automatic refreshing system wherein every site will periodically refresh with updated threat data from the central source. These include new patterns identified in attacks, in addition to the blocklist of malicious IP addresses, amongst other security information findings that may be relevant. Depending on the robustness of systems and the extent of security needs, changes in the forms should be able to reach the sites in real-time or at regular intervals. Also, websites must be able to introduce new threat intelligence into the repository, which in turn experiences the benefits of this knowledge. Anyway, both ways of communication allow the defence system to respond flexibly.

4.5.3 Protocols for Reporting and Handling Cyber Threats

Procedures for reporting and handling cyber threats should be standardised and accurate. A website must log and report suspicious activity to a central repository through a procedure in place when necessary. That could include offering full information regarding the IP address, what sort of attack, and what the website does. Based on threat data analysis, the central repository will supply the other participating sites with relevant threat information if that's determined to be the case. This should, therefore, provide processes for the treatment and reporting of various forms of threats. In this respect, multi-step verification should be incorporated for probable breaches, instant IP blocking for high-threat attacks, and alerts for suspicious yet inconsequential activity. Therefore, these measures should be exposed to regular training and updates harmonised with the approach towards cybersecurity within participating websites.

4.6 Stepwise Working of Single Website for Sharing Data (Flow chart)

Step 1: The system verifies the password entered by the user when they try to log in. The user can enter the right password for up to three tries. If the login is successful after these tries, the user can access their dashboard or any other following pages.

Step 2: If all three attempts are unsuccessful, the system detects possibly harmful behaviour and triggers extra security measures. As part of this, an automated verification code will be sent to the user's registered email

GAP INDIAN JOURNAL
OF FORENSICS AND BEHAVIOURAL SCIENCES
(ISSN – 2582-8177)
Globally peer-reviewed and open access journal.

address. This code provides additional security by assuring a hacker cannot proceed without access to the user's email.

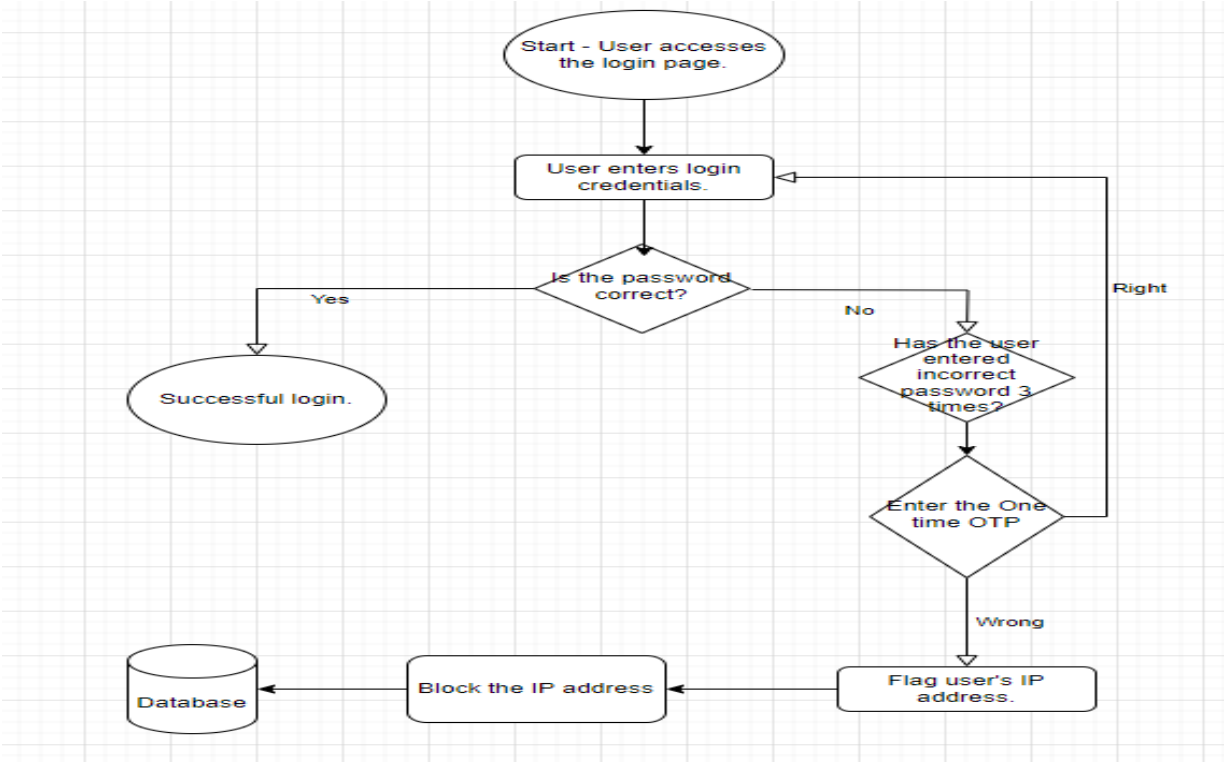

Figure 3: Flow Chart of one Website to Save their Database

Step 3: If an unauthorised person tries to enter the incorrect code, the system blocks the IP address linked to the attempted breach. The account is secured, and additional hacking attempts from the same source are prevented.
Step 4: If an authentic user discovers their IP address has been blocked because of a mistake, they can unblock it by going to their account settings or clicking on a link in the email notification. This allows for flexibility for authorised users without compromising security.

5. SECURITY MEASURES AND PROTOCOLS

Overview of Security Protocols:Data Encryption: All the data in motion and at rest at transmission between the central repository and participating websites with highly secure encryption techniques AES-256 that will protect private information, such as IP addresses or threat intelligence, from falling into any wrong hands.
Centralised repository: Only authorised users can view the data, and minor alterations can be made based on adopting multi-factor authentication and role-based access control. Access level definition based on user role reduces insider threats.
Cyber incident reporting and response: Standard reporting and handling of cyber threats ensure standardised, reliable site communication. While the method for handling non-critical situations is manual review, critical situations like IP blocking will be managed through automated systems.
Monitoring and Auditing: Regular auditing must ensure security procedures are followed and that any vulnerabilities, if found, looking for unusual activities in websites and repositories are constantly being monitored.

5.1 Flexible Authentication Methods

It would add multi-factor authentication to secure the user's login to a central repository or participating website. MFA ensures that another layer of authentication, such as OTP and biometric authentication, occurs before one can access the account in case a password is compromised.
The CAPTCHA challenges, and the verification codes applied a check against automated brute force attacks. In this case, if the username or the password of the account is wrong several times, then the code will be forwarded to the actual mail address of the user.
User Initiating IP Unblocking—This method preserves flexibility while retaining security in case the Legitimate user's IP is mistakenly blocked. Users can unblock their IP from account settings or click the email-supplied link.

5.2 Dynamic Adaptation to Emerging Threats

This maintains a central repository that refreshes the associated websites about the involvement of new threats, also termed new blocked IP addresses and distinctive attack patterns. The central repository ensures constant protection through real-time warnings of the latest threats that surface.

Adaptive Security Measurers: The adaptive mechanisms system adapts security using some protocols to fit the state of threats, such as raising the account lock-out period if marked activity is noted along this attack route.

The participating website and repository are updated with patches and information about recent developments. Therefore, security measures are kept abreast of current developments in cybersecurity through an active approach to exploiting vulnerabilities.

6. CASE STUDIES AND INSPIRATION

This ever-changing, complex area of cyber security harms and threatens every living being on earth daily. Organisations are, therefore, embracing crowd-sourced systems for threat intelligence that collect, analyse, and share malicious IP addresses and other IoCs. This case study illustrates how huge organisations such as Malwarebytes, AbuseIPDB, and Project Honeypot use crowdsourcing to help customers avoid online attacks. Lessons gained from Google and Microsoft, etc.

6.1 Malwarebytes Threat Intelligence

Client Data-Scraping: Malwarebytes is one way an organisation can generate new intel on malware and malicious IPs from its vast client base. It identifies new threats in real-time by using telemetry data emanating from millions of endpoints.

Partnership: It would enable Malwarebytes to update and improve its threat intelligence database by partnering with other companies and organisations involved in cybersecurity activities.

Community Involvements: Malwarebytes boasts of its proactive defence approach. Using threat intelligence, it neutralises threats to predict and check them.

6.2 Abuse IPDB

Community success: AbuseIPDB is a good example of true community-driven success. It allows consumers, network administrators, and security experts to report malicious IPs, creating an extensive and responsive crowdsourced database.

API Integrations: The application enables companies to incorporate threat intelligence into their tooling easily. By opening up access to its API, programs created by Abusers can automatically be located and blocked. With a transparent reporting system that helps users understand all the detailed information about why an IP address is reported, AbuseIPDB is accountable. Therefore, this database employs this methodology to encourage trust and accountability.

6.3 Project Honeypot

1. Project Honeypot: It is a proof-of-concept that such systems as honeypots attract potential attackers, allowing them to be tracked. It aids in understanding the TTPs of cybercriminals and gathering significant data.
2. Community Collaboration: Project Honeypot, like AbuseIPDB, relies on a volunteer community to set up honeypots. The platform's cumulative ability to identify and report malicious activity is strengthened through individual contributions.
3. Geographical Reach: Project Honeypot promises to paint an international picture of threats by deploying honeypots around the globe, thus making their data useful to users from different geographical locations.

6.4 Examples of Successful Implementations

Medium-Sized Business Taking on the Malwarebytes

Problem: The mid-size IT company was under relentless malware and phishing attacks beyond the capabilities of antivirus software.

Solution: The firm would use information about all the threats from Malwarebytes to identify and block any fresh malware or even malicious IP addresses on every endpoint with the rapid installation of the Malwarebytes app.

Conclusion: The company suffers from a shocking incidence of malware that dwindles to 75% with a successful phishing attack.

Implementing AbuseIPDB in a Financial Institution:

Problem: It was discovered that a financial organisation has some DDoS attacks and login attempts on some suspicious IP addresses.

Solution: The AbuseIPDB API, combined with the institution's firewall and SIEM platform, provided a solution for automatically blocking IPs related to abusive activity.

Result: The security team's efficiency increased since there were fewer interventions through automation. The occurrence and impact of DDoS attacks were reduced by 60%.

6.5 Project Honeypot in an Educational Network

Problem: This problem was caused by the continuous spewing of spam by the infected machines connected to the campus network and the existence of botnets.

Solution: Project Honeypot was deployed institution-wide for traffic monitoring, statistics gathering, and malicious traffic identification. Based on the data it collected, it could mark blocks of IP addresses as malicious and thus identify compromised devices.

Result: The university has considerably reduced spam and bots, improving security and performance inside the network.

Projects Honeypot, AbuseIPDB, and Malwarebytes Threat Intelligence underscore some of these community-based approaches to cybersecurity. These platforms harness threat information from partners, customers, and community contributors to provide total threat information that helps protect businesses from constantly evolving cyber threats. Valuable lessons may be drawn from firms that wish to collaborate and uphold proactive defence efforts for enhanced security controls.

6.6 Benefits and Impact

6.6.1 Enhanced Security for Connected Websites

1. United Threat Response: Participating sites have a common defence mechanism through their linking to the community-driven database. Once a threat has been identified on one of the sites, it would be flashed across the network so that all the connected sites can take immediate preventive measures. Thus, this forms a defence mechanism where popular attacks such as dictionary and brute force attacks would not occur.
2. Dynamic IP Blocking: Once the system identifies a dubious activity, it automatically blocks malicious IP addresses. The centralised method blocks networkwide vulnerabilities because other websites can proactively act against a threat identified on one site.
3. Flexible Recovery Mechanisms: True users who have their IP address blocked accidentally have a simple way of this happening through a user-friendly interface; therefore, the security mechanism must be strong yet flexible.

6.7 Proactive Threat Detection and Prevention

1. Real-time threat intelligence: The system's constant collection and sharing of threat data allows participating websites to upgrade their defences in real time. With this proactive strategy, new dangers are promptly detected and eliminated before they can do much harm.
2. Automated Security Measures: Many of the system's fundamental security operations, such as locking off illegal users and providing verification codes, are automated. This decreases the possibility of successful attacks and lessens the workload for website administrators, freeing them up to concentrate on other important duties.
3. Constant Monitoring and upgrades: To guarantee that websites are kept safe from the newest online threats, regular audits, security patches, and upgrades are performed. The adaptive security mechanisms further improve this by modifying the defensive plan in reaction to new threats.

6.7.1 Contribution to the Broader Cybersecurity Community

1. Collaborative Defence Network: This is a community-led system where the sites can feed their threat intelligence into the common pool. Altogether, aggregated efforts make the cyber ecosystem harder as it becomes much more difficult to hit certain websites in aggregate efforts.
2. Industry Standards are Set: This would raise the digital landscape's security posture. The effort prompts using best cybersecurity practices, including encryption, authentication, and dynamic threat response.
3. Information sharing: Participating sites provide practical threat intelligence, new threats, and missing sophisticated knowledge. The information gathered by the cybersecurity community fuels innovation and cooperation, and in the long term, such communities will develop stronger and more potent defences.

7. CHALLENGES AND CONSIDERATIONS

7.1 Potential Obstacles to Implementation

Integration Complexity: When creating one central repository, integrating multiple websites under different structures and security protocols is complex. Depending on the application, the process may take time and money.

Onsite site growth increases the pressure to handle the increased flow and storage of data. The challenge is that the infrastructure should be able to accept all this without compromising on performance.

It is also challenging to make the websites interact with the grassroots project by engaging in an active data exchange to make the Internet safer than ever, especially when it is also scaring the guts out of them to make them want even to lower the current systems' level of interference.

7.2 Privacy and Data Protection Concerns

Any data that concerns sensitivity, such as the distribution of IP addresses and Threat Intelligence data, will have to consider GDPR along with other requirements in privacy regulations and rules for managing sensitive data with proper anonymisation or management, thus avoiding legal hazards.

Data Breach Risks: While this central repository promises much security, attackers see it only as a goldmine. The safety of the intruders must be ensured to keep the participatory websites trusting the system.

User Privacy: The balance between security and user privacy. The system cannot be a harsh security measure that reveals personal details about and prosecutes honest users.

7.3 Maintenance and Continuous Improvement

1. Regular Updates and Fixes: It won't be a simple task to update the mother repository with the latest security and new threats about all its websites. This would be pretty testing since new threats would be discovered in the system.
2. Auditing and Monitoring: Surely, there would be a requirement for an operational framework in terms of scheduled audits and system monitoring to strictly show that the security controls implemented are uniform and operational in performing what they have been expected to do. Such an effort, however, would take time and resources in terms of skill.
3. Adaptive Security Strategies: Changes in security controls over the relevant system should include cyber security measures. These changes mean improving norms and standards and adopting new technologies to keep up with threats' changes and challenges.

8. CONCLUSION

This paper proposes a systematic method of upgrading website security modules using a group-owned database monitoring and allocating IP addresses of refused log-ins. The methodology thus proposed gives strong protection against dictionary attacks and brute force attacks based on real-time IP blocking as a mode of defence, thereby strengthening proven techniques such as hashing-based authentication. Added security can be attained by automatically creating verification codes and dynamic IP filtering, where threats are immediately struck.

9. FUTURE DIRECTIONS

1.Scalability in databases: With increased websites and data, a scalable structure with a distributed architecture and automated management will certainly be performance—and security-assured, fault-tolerant, and efficient.

2.Evolution of Security Risks and Reactions: Proactively thwarting complex assaults requires adapting to changing risks using AI-driven detection and improved authentication techniques like biometrics.

10. REFERENCE

[1] M. Alawida, A. E. Omolara, O. I. Abiodun, and M. Al-Rajab, "A deeper look into cybersecurity issues in the wake of Covid-19: A survey," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 8176–8206, Nov. 2022, doi: 10.1016/J.JKSUCI.2022.08.003.

[2] "Foundation Of Data Management In Asset Management Firms | UBTI." Accessed: Sep. 21, 2024. [Online]. Available: https://ubtiinc.com/foundation-of-data-management-in-asset-management-firms/

[3] B. Preksha, R. Harish, B. Sreenivas, and M. Vasanthalakshmi, "Image Steganography using RSA Algorithm for Secure Communication," *2021 IEEE International Conference on Mobile Networks and Wireless Communications, ICMNWC 2021*, 2021, doi: 10.1109/ICMNWC52512.2021.9688352.

[4] P. Akey, S. Lewellen, I. Liskovich, and C. M. Schiller, "Hacking Corporate Reputations", Accessed: Sep. 21, 2024. [Online]. Available: http://ssrn.com/abstract_id=3143740www.ecgi.global/content/working-papers

[5] M. K. Hamza, H. Abubakar, and Y. M. Danlami, "Identity and Access Management System: a Web-Based Approach for an Enterprise," *Path of Science*, vol. 4, no. 11, pp. 2001–2011, Nov. 2018, doi: 10.22178/POS.40-1.

[6] T. Suleski, M. Ahmed, W. Yang, and E. Wang, "A review of multi-factor authentication in the Internet of Healthcare Things," *Digit Health*, vol. 9, Jan. 2023, doi: 10.1177/20552076231177144.

[7] J. R. Lewis and J. Sauro, "Usability and User Experience: Design and Evaluation," *Handbook of Human Factors and Ergonomics*, pp. 972–1015, Aug. 2021, doi: 10.1002/9781119636113.CH38.

[8] A. A. Bouramdane, "Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options, Including Ones That Incorporate Artificial Intelligence, Using an Analytical Hierarchy Process," *Journal of Cybersecurity and Privacy 2023, Vol. 3, Pages 662-705*, vol. 3, no. 4, pp. 662–705, Sep. 2023, doi: 10.3390/JCP3040031.

[9] "What is Intrusion Detection Systems (IDS)? How does it Work? | Fortinet." Accessed: Sep. 21, 2024. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system

[10] D. Jeon and B. Tak, "BlackEye: automatic IP blacklisting using machine learning from security logs," *Wireless Networks*, vol. 28, no. 2, pp. 937–948, Feb. 2022, doi: 10.1007/S11276-019-02201-5.
[11] "(10) (PDF) Cyber Security Threat And Its Prevention Through Artificial Intelligence Technology." Accessed: Sep. 21, 2024. [Online]. Available: https://www.researchgate.net/publication/376717717_Cyber_Security_Threat_And_Its_Prevention_Through_Artificial_Intelligence_Technology
[12] C. Johnson, L. Badger, D. Waltermire, J. Snyder, and C. Skorupka, "NIST Special Publication 800-150 Guide to Cyber Threat Information Sharing", doi: 10.6028/NIST.SP.800-150.
[13] "16 Types of Cyberattacks and How to Prevent Them." Accessed: Sep. 21, 2024. [Online]. Available: https://www.techtarget.com/searchsecurity/tip/6-common-types-of-cyber-attacks-and-how-to-prevent-them
[14] "15 Internet Safety Tips and Internet Safety Rules | Kaspersky." Accessed: Sep. 21, 2024. [Online]. Available: https://www.kaspersky.com/resource-center/preemptive-safety/top-10-preemptive-safety-rules-and-what-not-to-do-online