International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.1 (2025) pp. 935-948
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Artificial Intelligence and Advanced Cybersecurity to Mitigate Credential-Stuffing Attacks in the Banking Industry

Homam El-Taj[1]*, Danah Hamedah[2], Rawan Saeed[3]

[1]Dar Al-Hekma University, Cybersecurity Department, Jeddah-Saudi Arabia
* **Corresponding Author Email:** htaj@dah.edu.sa - **ORCID:** 0000-0001-7565-4760

[2]Dar Al-Hekma University, Cybersecurity Department, Jeddah-Saudi Arabia
Email: danahhamedah@gmail.com - **ORCID:** 0009-0005-8896-481X

[3]Dar Al-Hekma University, Cybersecurity Department, Jeddah-Saudi Arabia
Email: irrawan.1.qureshi@gmail.com- **ORCID:** 0009-0002-3829-7076

Article Info:

DOI: 10.22399/ijcesen.754
Received : 12 December 2024
Accepted : 13 January 2025

Keywords:

Credential-Stuffing,
Machine learning,
Stolen credentials,
User behaviour analytics,
Adaptive authentication,
AI.

Abstract:

Credential-stuffing attacks pose a critical threat to the banking sector, leveraging stolen login credentials to compromise user accounts and inflict substantial financial and reputational damage. Traditional security measures, including Multi-Factor Authentication (MFA) and CAPTCHA, often fall short against the sophistication of these attacks, necessitating more advanced and proactive defense strategies.
This study explores the transformative role of artificial intelligence (AI) and machine learning (ML) in cybersecurity, particularly in mitigating credential-stuffing threats. AI-driven solutions enable real-time threat detection, predictive analysis, and adaptive authentication, providing enhanced protection by analyzing large datasets to identify unusual login patterns and behaviors. Despite their promise, AI and ML adoption in cybersecurity faces challenges, including data privacy concerns, the risk of false positives and negatives, and scalability barriers. This research also examines emerging technologies, such as federated learning and blockchain-based authentication, which offer decentralized and privacy-preserving approaches to combating credential-stuffing attacks. Ultimately, AI and ML present the banking sector with powerful tools to build resilient, adaptable, and efficient defenses against evolving cyber threats. By integrating these technologies with complementary innovations, financial institutions can enhance security, protect customer trust, and address the dynamic landscape of credential-based cyberattacks.

1. Introduction

Financial institutions are increasingly targeted by cyberattacks, with credential-stuffing attacks emerging as a critical threat. Credential-stuffing attacks take advantage of credentials compromised in past data breaches, exploiting users' habitual reuse of passwords across multiple platforms [1].
Once attackers gain unauthorized access, they can inflict significant damage, compromising both data security and customer trust [1].
Banks face mounting pressure to safeguard sensitive information while contending with cybercriminals who continuously refine and automate their attack methods. Credential-stuffing techniques drive billions of login attempts annually, targeting financial institutions on a massive scale. Traditional defenses, like Multi-Factor Authentication (MFA) and CAPTCHA offer limited protection, often insufficient against the growing sophistication of attackers' methods. The rapid evolution of these threats underscores the urgent need for advanced security measures capable of keeping pace [2,3].
This paper discusses the impact of credential-stuffing attacks on the banking sector, including financial losses, reputational damage, and operational strain. It examines the limitations of traditional security measures and highlights the role of Artificial Intelligence (AI) and Machine Learning (ML) in addressing these challenges. By exploring AI/ML-based solutions such as anomaly detection, adaptive authentication, and real-time threat intelligence, the paper demonstrates how

these technologies can enhance cybersecurity defenses. Furthermore, it delves into implementation challenges and provides insights into future trends and research directions to combat credential-based cyber threats effectively.

2. Credential-Stuffing Attacks

Credential-stuffing attacks represent a sophisticated and widespread threat to cybersecurity, targeting login credentials obtained from large-scale data breaches. These attacks exploit the common practice of password reuse, where users use the same login credentials across multiple platforms. This habit significantly increases the risk of unauthorized access to sensitive accounts, particularly in industries like banking, where financial and personal data are at stake [1,2].

The dark web serves as a repository for vast troves of stolen credentials, offering cybercriminals access to millions of compromised usernames and passwords. With such resources at their disposal, attackers can scale their operations using advanced tools like rainbow tables—precomputed data sets designed to reverse cryptographic hash functions. As discussed by Patel et al. (2021) and Manankova et al. (2023), rainbow tables enable attackers to quickly convert encrypted passwords into plaintext, making credential-stuffing attacks both faster and more efficient [4,5].

Once equipped with stolen credentials, attackers deploy automated systems to conduct large-scale login attempts. Botnets and custom scripts systematically test combinations of usernames and passwords across numerous platforms, often executing thousands of attempts within seconds. These automated tools leverage the fact that many users reuse passwords, enabling attackers to gain access to multiple accounts with minimal effort [6,7].

Credential-stuffing attacks differ from brute-force attacks in that they rely on pre-existing credentials rather than guessing passwords. This precision increases their effectiveness, particularly against systems that rely on conventional defenses [6]. To further evade detection, attackers frequently use proxy networks to mask their IP addresses, making login attempts appear as though they originate from diverse locations. This tactic circumvents IP-based security measures, allowing attackers to remain undetected for extended periods [8-17].

The growing sophistication of credential-stuffing attacks underscores the urgent need for advanced cybersecurity defenses. As attackers continue to refine their tools and techniques, traditional measures are proving increasingly inadequate, calling for innovative solutions to combat this persistent threat [3,5].

2.1 Compromised Credential Scenarios

To understand the impact of credential-stuffing attacks, it is crucial to examine real-world scenarios where compromised credentials have caused significant data breaches among leading organizations.

The figure 1 illustrates a scenario where compromised credentials impact user accounts with major organizations such as Meta, Google, and Microsoft. These companies are frequent targets of credential-stuffing attacks, which have led to substantial data breaches. The figure highlights how a single set of stolen credentials can provide attackers with unauthorized access to sensitive services hosted by these organizations, demonstrating the far-reaching consequences of such attacks.

Large-scale breaches often expose users' login details, which are subsequently exploited in credential-stuffing attacks on other platforms where users have reused their credentials. For example, after breaches that revealed login information, attackers took advantage of this compromised data to gain unauthorized access to multiple accounts across various services [8-10]. This sequent effect confirms the critical need for robust authentication practices, such as multi-factor authentication, and greater user education to mitigate the risks posed by credential-stuffing attacks.

2.2 Credential-Stuffing Process

Building on the understanding of the impact of compromised credentials, it is important to break into the technical process behind credential-stuffing attacks and how attackers exploit stolen data.

The figure 2 illustrates the process of a credential-stuffing attack initiated by a hacker using a database of compromised usernames and passwords. These credentials, obtained from prior data breaches, are fed into automated tools designed to test login attempts across multiple platforms. The figure visually demonstrates how attackers exploit these stolen credentials to gain unauthorized access to a variety of online services.

In the illustration, the hacker is positioned at the center, representing the orchestrator of the attack. On the right, the figure represents the target platforms—such as storage systems, email services, and social media accounts—highlighting the widespread scope of credential-stuffing. This visualization explains how attackers rely on the repetition of credentials across different services to

increase the chances of success. By testing the same credentials across multiple platforms, attackers consente on user habits to achieve large-scale unauthorized access [11].

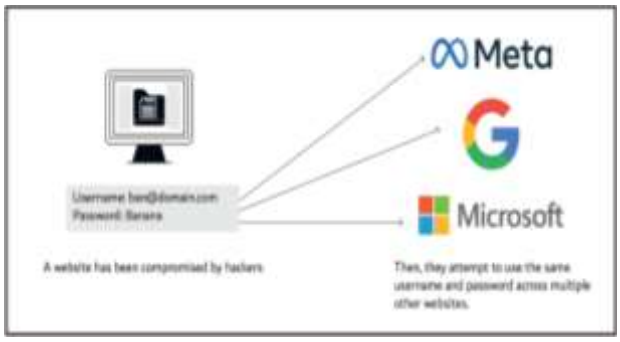

Figure 1. *Credential-Stuffing Attack [12]*

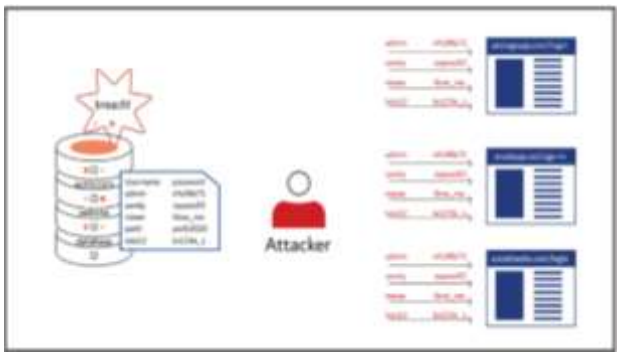

Figure 2. *Reusing Compromised Credentials for Unauthorized Access [13].*

3. Tools and Methods Used by Attackers

Credential-stuffing Cybercriminals performing credential-stuffing attacks rely on sophisticated automation tools designed to increase their chances of success. This toolkit includes automated bots, rainbow tables, account-checking tools, and proxy services, each of which plays a critical role in executing large-scale attacks against vulnerable systems.

3.1 Automated Bots

Automated bots form the core of credential-stuffing operations. These malicious programs are designed to flood login portals with stolen credentials at speeds far beyond human capabilities. By mimicking normal user behaviors, such as inputting usernames and passwords, bots can avoid basic security measures, including rate-limiting protocols intended to flag unusual access patterns. Once deployed, bots can persistently attack a target until they either gain access successfully or exhaust the allowed login attempts.

Advanced bots have been developed to bypass CAPTCHA challenges, which are often implemented as an additional security layer to differentiate between human users and bots. This capability significantly enhances the effectiveness of credential-stuffing attacks, allowing attackers to operate with greater stealth and efficiency [14].

3.2 Rainbow Table Tools

Rainbow table tools represent a sophisticated method for exploiting weak password security on a large scale. These tools rely on precomputed tables of hash values corresponding to common passwords, enabling attackers to quickly reverse cryptographic hashes and identify valid passwords without exhaustive guessing. Compared to traditional brute-force methods, rainbow tables significantly reduce the time required to crack passwords.

In the context of credential-stuffing, rainbow tables are especially effective because many users reuse passwords across multiple accounts. When attackers gain access to one set of credentials, they can use rainbow tables to identify matches in other systems where the same passwords might be used. This process accelerates the attack and increases the probability of succesfully breaching multiple accounts with minimal effort [15].

3.3 Account Checking Tools

Account-checking tools play a crucial role in refining credential-stuffing operations by verifying the validity of stolen credentials. These tools systematically test credentials against various online services, such as banking platforms, to identify active username-password combinations. By filtering out invalid credentials, account checkers enable attackers to focus their resources on viable targets, significantly improving the success rate of breaches.

Many account-checking tools also feature notification systems that alert attackers when a successful login occurs. This allows attackers to quickly exploit compromised accounts before users or institutions can respond. The efficiency of these tools confirms the critical need for swift detection and response strategies, particularly for financial institutions facing credential-stuffing threats [16].

3.4 Proxy Services

Proxy services are an essential component of an attacker's toolkit, enabling them to distribute login attempts across numerous IP addresses. This technique helps attackers avoid detection and bypass security mechanisms designed to monitor unusual activity patterns. By masking their identity and making login attempts appear to originate from

diverse geographic locations and devices, attackers can bypass traditional security measures.
Residential proxies are particularly effective because they simulate legitimate internet traffic, making it even more difficult for security systems to distinguish between genuine users and attackers. This distribution strategy not only minimizes the risk of being blocked by the targeted system but also allows attackers to conduct prolonged operations without triggering security alarms [17].

4. Impacts of Credential-Stuffing Attacks on the Banking Sector

To effectively understand the full scope of credential-stuffing attacks, it is essential to examine their various impacts on the banking sector. These attacks not only pose significant financial and operational challenges but also destroy customer trust and strain regulatory compliance efforts. For instance, financial institutions face billions in losses annually due to unauthorized transactions and recovery efforts, while regulatory fines under laws like the General Data Protection Regulation (GDPR) add to the burden [1,18]. Furthermore, the reputational damage caused by data breaches often leads to customer turnover, compounding the financial and operational strain [19]. The following sections investigate these critical consequences, highlighting how credential-stuffing incidents disrupt banking institutions and their clients.

4.1 Financial Losses and Regulatory Fines

Credential-stuffing attacks impose significant financial burdens on banks, including unauthorized transactions, identity theft, and fraudulent account activity. Beyond these immediate losses, banks face high recovery costs for reversing fraudulent transactions, issuing new credentials, and restoring compromised accounts. Additionally, banks are subject to strict regulatory frameworks, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), which impose heavy fines for data breaches involving personal information. These regulations enforce severe penalties for non-compliance, intensifying the financial strain on banks dealing with credential-stuffing incidents [18].

4.2 Damaged Trust and Customer Loyalty

Customer trust is paramount in the banking sector, as clients expect robust security for their financial data and transactions. Credential-stuffing attacks can demolish this trust rapidly. When unauthorized access leads to account compromise, customers may feel their bank has failed to protect their data, prompting account closures and customer turnover. Even unaffected customers may lose confidence, deciding to switch to competitors known for stronger security protocols. Such incidents not only destroy trust but also lead to long-term financial challenges for affected institutions [19].

4.3 Account Takeover

Cybercriminals often use stolen credentials to perform full account takeovers, gaining complete control over bank accounts. With unauthorized access, attackers can initiate high-value transfers, make unauthorized purchases, and even apply for financial products such as loans and credit cards. In many cases, these fraudulent actions go unnoticed until the account holder detects unauthorized transactions, by which time significant financial damage may have already occurred. Banks are often required to compensate affected customers, further increasing financial liabilities and straining customer support resources [20].

4.4 Operational Strain and Recovery Costs

Credential-stuffing attacks place considerable pressure on a bank's operational and IT resources. Beyond direct financial impacts, banks endure costs related to strengthening security measures, investigating breaches, and supporting affected users. Significant investments in advanced defenses, such as AI and machine learning systems, are necessary to detect and mitigate escalating threats. These costs underline the necessity of proactive cybersecurity investments to minimize the long-term impacts of credential-stuffing attacks. Additionally, swift responses to credential-stuffing breaches often require overtime and additional labor costs, as security teams work to prevent future intrusions. These combined costs assures the necessity of robust cybersecurity measures to ensure financial stability in today's banking landscape [21].

5. Challenges in Traditional Mitigation Techniques

Traditional mitigation techniques, such as Multi-Factor Authentication (MFA) and CAPTCHA systems, provide some level of protection against credential-stuffing attacks. However, these methods face significant challenges that limit their effectiveness in today's rapidly evolving cyber threat landscape. Attackers continually develop advanced techniques to bypass these defenses,

rendering them insufficient as standalone security measures.

For instance, sophisticated phishing attacks and SIM-swapping tactics allow attackers to deceive MFA, while advanced bots equipped with Optical Character Recognition (OCR) can easily bypass CAPTCHA systems. These evolving tactics highlight the inadequacy of static security measures in addressing dynamic and increasingly sophisticated credential-stuffing operations.

To counter these challenges, there is an urgent need for adaptive and robust solutions that leverage real-time threat intelligence and behavioral analysis. These advanced measures can provide a more proactive defense against the growing sophistication of credential-stuffing attacks.

5.1 Multi-Factor Authentication

Multi-Factor Authentication (MFA) is designed to enhance security by requiring users to verify their identity through multiple methods. While this additional layer of protection improves defenses against credential-stuffing attacks, many users find the process inconvenient or frustrating. This often results in skipped or disabled MFA settings, diminishing its overall effectiveness.

Additionally, cybercriminals have developed sophisticated methods to bypass MFA protections. Techniques such as phishing attacks and SIM swapping exploit system vulnerabilities, making MFA less reliable as a standalone defense against credential-stuffing attacks. For example, high-profile cryptocurrency breaches have demonstrated the risks of MFA circumvention. These challenges underscore the need for complementary security measures to address evolving threats [22].

5.2 CAPTCHA Systems

CAPTCHA systems are designed to differentiate human users from bots by presenting challenges that are simple for humans but difficult for automated systems. However, attackers have increasingly exploited vulnerabilities in these systems using techniques such as Optical Character Recognition (OCR) and advanced scripts, effectively bypassing CAPTCHA protections.

In addition to these technical limitations, CAPTCHA systems often create a negative user experience. Many users find them inconvenient and disruptive to their workflow, leading to frustration and reluctance to engage with security protocols that rely on this technology. This poor user perception undermines the effectiveness of CAPTCHA systems as a defense against credential-stuffing attacks, highlighting the need for more user-friendly and robust alternatives [23].

5.3 Password Hygiene

Maintaining secure passwords is a cornerstone of cybersecurity. Despite growing awareness of the importance of unique and complex passwords, many users continue to rely on weak or reused passwords for convenience. This practice leaves individuals highly vulnerable to credential-stuffing attacks, as compromised credentials can grant unauthorized access to multiple accounts.

Password managers simplify the creation and storage of secure passwords, offering a practical solution to improve password hygiene. However, their adoption remains inconsistent. Many users distrust these tools, fearing potential vulnerabilities, or fail to integrate them into their daily routines. This reluctance perpetuates the risks of security breaches, underscoring the ongoing challenge of fostering strong password practices [24].

6. Limitations of Traditional Approaches

Traditional cybersecurity measures, such as Multi-Factor Authentication (MFA) and CAPTCHA systems, play an important role in defending against credential-stuffing attacks. However, these tools are largely reactive, activating only after an attack has begun. For instance, MFA is triggered during login attempts, creating a window of opportunity for attackers to exploit. Similarly, CAPTCHA systems operate only after an attack is underway, leaving systems vulnerable during critical early stages [25,26].

The effectiveness of these traditional defenses is further compromised as attackers adopt advanced techniques, such as machine learning algorithms, to bypass CAPTCHA and intercept MFA credentials. These limitations expose financial institutions to significant risks [27]. Moreover, the complexity of MFA and CAPTCHA systems often frustrates users, discouraging their adoption. Many users prefer less secure platforms that prioritize convenience, undermining the effectiveness of these measures. For instance, high-profile breaches have demonstrated how user hesitancy to adopt MFA can leave systems exposed. To address these challenges, financial institutions must transition from reactive defenses to proactive, AI-driven solutions. AI-powered tools provide real-time threat detection, anomaly analysis, and adaptive authentication, offering a more robust defense against evolving cyber threats. Unlike traditional measures, AI continuously learns from new attack patterns, making it a more resilient and adaptive

solution. By combining advanced automation with user-friendly interfaces, these systems balance security and usability, closing the gaps left by traditional approaches [28].

7. Role of AI and ML in Cybersecurity

One of AI's most significant strengths lies in its real-time adaptability. By leveraging advanced algorithms, AI systems can identify unusual behaviors, such as deviations in login patterns or network activity, before they escalate into critical security incidents [29-38]. Artificial Intelligence (AI) and Machine Learning (ML) are revolutionizing cybersecurity by offering dynamic and adaptive solutions to increasingly sophisticated threats, such as credential-stuffing attacks [32,37]. Traditional security measures often fail to keep pace with the evolving tactics of cybercriminals, who continuously adapt to avoid detection. In contrast, AI/ML excel at analyzing wide datasets to uncover hidden patterns and anomalies, providing organizations with a proactive edge in mitigating these risks [39-57].

This proactive capability ensures that defenses remain one step ahead of attackers, even as their methods evolve [30,37]. AI and ML also demonstrate remarkable flexibility and scalability, enabling organizations to deploy layered detection strategies. From real-time threat analysis to predictive modeling, these systems anticipate attack strategies based on historical data while swiftly adapting to new tactics. For example, financial institutions have successfully implemented AI-driven anomaly detection systems to combat credential-stuffing attacks [42,57]. In addition to detecting active threats, AI/ML systems continuously improve their accuracy through continuous learning. By adapting to changing risk profiles, these technologies become increasingly effective over time, making them indispensable in environments where attackers frequently modify their strategies [32,39,44]. By integrating real-time detection, predictive analysis, and adaptive learning, AI and ML address current cybersecurity challenges while establishing a resilient defense system for the future. These technologies represent a critical shift toward proactive cybersecurity, ensuring organizations can counter complex and evolving threats with precision and efficiency.

8. AI/ML-Based Proposed Solutions for Credential-Stuffing

AI/ML technologies excel at anomaly detection, a critical capability for identifying subtle deviations in login patterns or network traffic associated with credential-stuffing attacks. Traditional security measures often fail to detect such sophisticated attacks due to their reliance on predefined rules. In contrast, AI/ML models analyze large datasets and adapt dynamically, providing organizations with real-time insights into potential threats and enabling swift, effective responses [30,38,39].

8.1 Machine Learning Models for Advanced Anomaly Detection

Machine learning offers diverse techniques for detecting and mitigating credential-stuffing attacks. The following points highlight key models and their role in enhancing cybersecurity defenses.

Supervised Learning
Supervised learning models use labeled data to classify login attempts as valid or suspicious. These models detect patterns indicative of credential-stuffing, such as repeated failed logins or access from unexpected locations. Example Solution: Algorithms like Random Forests and Support Vector Machines (SVMs) can classify login attempts, flagging those that deviate from normal behavior. These models update themselves over time to adapt to new attack strategies and changing user behavior [40,45,48].

Unsupervised Learning
Unsupervised learning models analyze unlabeled data to detect irregularities without relying on predefined labels [40,48]. These models are particularly effective in uncovering rare or undocumented attack patterns [51]. Example Solution: K-means clustering and Isolation Forests can detect outliers, such as a sudden increase in logins from one IP address. These techniques uncover undocumented attack behaviors, improving the detection of new or zero-day credential-stuffing tactics [51,52].

Deep Learning
Deep learning models, such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, excel at recognizing complex and sequential patterns in login behavior. These models analyze multi-dimensional data like login time, device type, and location to detect signs of malicious activity [53]. Example Solution: CNNs are effective at identifying login patterns over time, while LSTMs excel at detecting sequential behaviors, such as repeated login attempts. An LSTM-based model can track login behavior over time, spotting both known and novel threats with high accuracy [53,54].

Semi-Supervised Learning

Semi-supervised learning models combine labeled and unlabeled data to improve detection where labeled datasets are limited. This approach is particularly effective for emerging threats like credential-stuffing, where labeled data may be rare [55]. Example Solution: Pseudo-labeled models use a small set of labeled examples to train the model while leveraging large amounts of unlabeled data to boost accuracy. This method is ideal for identifying new credential-stuffing patterns [55,56].

Reinforcement Learning

Reinforcement Learning (RL) models adapt dynamically by learning from feedback, continuously optimizing defense strategies. These models refine their responses based on outcomes, rewarding successful actions and penalizing failures, resulting in increasingly effective defenses [57]. Example Solution: RL models learn from system interactions to optimize defense strategies. Actions that reduce successful attacks are rewarded, while actions that allow breaches are penalized. Over time, this approach creates a stronger and adaptive defense [57,58].

Hybrid AI/ML Models

Hybrid models integrate multiple techniques, such as supervised learning for known patterns, unsupervised learning for anomalies, and reinforcement learning for adaptive strategies. This layered approach enhances the ability to detect and respond to both known and novel credential-stuffing threats [59]. Example Solution: A hybrid system could use supervised learning to recognize familiar attack patterns, unsupervised learning for detecting anomalies, and reinforcement learning to adjust strategies dynamically based on real-time attack data. This combination provides robust protection against evolving credential-stuffing tactics [60].

8.2 Behavioural Analysis and Adaptive Authentication Techniques

Behavioral analysis and adaptive authentication play crucial roles in modern cybersecurity. The following points explore how these approaches enhance threat detection and strengthen authentication defenses against credential-stuffing attacks.

User Behaviour Analytics (UBA)

User Behaviour Analytics (UBA) leverages AI to establish typical patterns in user behavior, such as preferred login locations, device types, and usage times. By creating a baseline of "normal" activity, UBA can quickly detect deviations that may indicate credential-stuffing attacks. For instance, if a user typically logs in from a single IP address and device type but suddenly logs in from multiple, unfamiliar locations, UBA can flag these attempts as suspicious [61]. Example Solution: A UBA model could monitor login attempts across various locations and devices, triggering alerts if a credential-stuffing attack tries to access accounts from different IPs in a short span. This rapid identification and mitigation of unusual activities help prevent account takeovers [62].

Adaptive Authentication Systems

Adaptive Authentication dynamically adjusts security measures in real-time based on the assessed risk level of each login attempt. By evaluating contextual factors, such as device type, location, time, and IP address, these systems assign threat levels—such as "low," "normal," or "high"—and adjust security responses accordingly [63,64]. Normal Threat Level: For low-risk login attempts, Adaptive Authentication may require basic measures, such as Multi-Factor Authentication (MFA). MFA typically involves a one-time passcode (OTP) sent via SMS or email, adding an additional layer of identity verification. High Threat Level: For high-risk login attempts—such as access from an unrecognized device in a high-risk country or after multiple failed attempts—Adaptive Authentication can apply stricter security measures. These may include biometric authentication (e.g., fingerprint or facial recognition) or restricting access to sensitive account areas until the user's identity is thoroughly verified [64,65].

Real-Time Threat Intelligence

Real-Time Threat Intelligence continuously monitors global cyber threat activity, aggregating and analyzing data from sources such as the dark web and cybersecurity databases. By integrating this threat intelligence into authentication processes, organizations can proactively defend against credential-stuffing attacks before they escalate [66]. Example Solution: A real-time threat intelligence model might scan data feeds to detect if known compromised credentials match those of its users. If a match is found, the system can alert the organization and prompt affected users to reset their passwords. This proactive approach neutralizes compromised accounts before they can be exploited [67].

Predictive Analysis for Early Detection

Predictive Analysis uses historical data and AI modeling to forecast credential-stuffing attack

patterns. By learning from past attacks, predictive models can identify patterns and early indicators of potential threats, enabling organizations to act before an attack escalates. For example, a predictive model could analyze historical credential-stuffing attempts to recognize timing patterns and tactics, then use these insights to prevent similar future attacks [68]. Example Solution: A system utilizing predictive analytics could forecast spikes in login attempts based on historical data. If a pattern of rapid, repeated login attempts from certain IPs was detected in prior attacks, the model could pre-emptively block these IPs or enforce additional security checks during high-risk periods. This proactive defense minimizes vulnerability by staying ahead of attackers' strategies [69].

9. Expected Results

The integration of AI/ML-based strategies into mitigating credential-stuffing attacks is expected to significantly enhance the security posture of organizations. By leveraging advanced anomaly detection, real-time threat intelligence, and predictive analytics, these systems can preemptively identify and block suspicious login attempts, reducing the number of successful attacks. This proactive approach enables security teams to respond swiftly and efficiently, often containing threats before they escalate into larger security incidents [69,70,71].

Adaptive authentication systems further enhance this defense by dynamically adjusting security measures based on the detected threat level. By escalating security protocols only when necessary, these systems maintain a seamless user experience, minimizing disruptions for legitimate users while ensuring robust protection during high-risk activities [72,73].

The combined use of real-time analysis, anomaly detection, and behavioral insights fosters a highly dynamic and adaptable defense strategy. As AI and ML models continuously learn from new data, their accuracy improves, enabling them to identify subtle or novel attack patterns with greater precision. Predicting potential threats before they occur, and leveraging automated response mechanisms, minimizes damage and enhances the speed of threat containment [74,75,76].

For example, an organization leveraging real-time threat intelligence successfully reduced credential-stuffing attempts by integrating predictive analytics and automated responses. This system proactively identified compromised credentials before they were exploited, preventing data breaches and enhancing user confidence.

These advancements are expected to yield tangible benefits, including a significant reduction in successful credential-stuffing attacks, fewer data breaches, lower financial losses, and improved customer trust. Organizations implementing these solutions can also expect long-term enhancements in the resilience and adaptability of their cybersecurity infrastructures, creating a robust ecosystem capable of addressing evolving threats [77,78].

10. Challenges in AI/ML Implementation

While AI and ML offer transformative potential in mitigating credential-stuffing attacks, their implementation presents significant challenges. The following points outline key obstacles organizations face and the steps required to overcome them.

10.1 Data Privacy Issues

AI systems depend heavily on large datasets to effectively detect and mitigate cyber threats. However, the collection, storage, and processing of these datasets raise significant privacy concerns, particularly under stringent regulations like the General Data Protection Regulation (GDPR) in the European Union. These regulations mandate robust protections for sensitive user information, creating a complex challenge for organizations: balancing the need for comprehensive datasets to train AI models with the obligation to safeguard user privacy [79].

To address this challenge, organizations must implement advanced safeguards, such as data anonymization, encryption, and access controls. For instance, a financial institution in the EU achieved GDPR compliance by anonymizing user data, reducing privacy risks by 40%. These measures ensure compliance with privacy laws while maintaining the effectiveness of AI capabilities. Additionally, evolving regulatory frameworks demand continuous vigilance and ethical decision-making to align AI practices with legal standards [80].

10.2 Training and Accuracy

The effectiveness of AI models in cybersecurity hinges on the quality and representativeness of the training data. Inaccurate or insufficient data can lead to two critical problems: false negatives, where threats are missed, and false positives, where harmless activities are flagged as malicious [81]. These inaccuracies reduce system reliability, create operational inefficiencies, and undermine trust among stakeholders.

To maintain high accuracy, AI systems require continuous data monitoring, frequent model retraining, and rigorous validation processes. For example, a large retailer leveraged automated retraining mechanisms to improve model accuracy by 25%, reducing false positives during peak activity periods. These processes ensure that models remain effective in adapting to evolving threat landscapes, though they are resource-intensive [70,82].

10.3 False Positives and False Negatives

Striking the right balance between false positives and false negatives is one of the most significant challenges in deploying AI/ML-based cybersecurity systems. Overly aggressive models can generate excessive false positives, frustrating users by locking them out of their accounts or triggering unnecessary security measures. Conversely, overly lenient models risk failing to detect attacks, allowing cybercriminals to bypass defenses and compromise sensitive systems [82,83].

Organizations can leverage advanced analytics and real-time feedback loops to refine their AI systems, striking a balance between security and usability. This ongoing optimization process not only enhances the performance of cybersecurity systems but also builds user trust, ensuring the long-term success of AI/ML-based defenses [84].

10.4 Scalability and Costs

The implementation of AI/ML-based security systems presents significant cost challenges, particularly for small- to mid-sized organizations. These systems often require specialized infrastructure, such as high-performance computing resources, as well as skilled personnel for operation and maintenance [85]. In addition, the costs of regular updates, continuous monitoring, and frequent retraining of models can be prohibitive for organizations with limited budgets [86].

To bridge this gap, initiatives such as shared resources, subsidized tools, and government partnerships are essential. For example, AI-powered detection mechanisms have successfully reduced credential-stuffing attack incidents, with a decline of up to 30% in environments deploying these advanced systems. Similarly, cloud-based systems leveraging AI-driven real-time detection and anomaly tracking have achieved similar reductions of 25–30%, further highlighting the effectiveness of these technologies across diverse applications [87-94].

Such collaborative efforts enable a wider range of institutions to benefit from sophisticated cybersecurity defenses, fostering a more equitable distribution of resources [87].

11. Future Trends and Research Directions

Emerging technologies such as federated learning and blockchain are shaping the future of AI/ML in cybersecurity. The following points highlight these innovations and their potential to enhance defenses against evolving threats like credential-stuffing.

11.1 Federated Learning

Federated learning provides a privacy-focused solution for AI/ML applications, particularly in cybersecurity. By enabling models to be trained locally across multiple devices or systems, federated learning eliminates the need to centralize sensitive data, thus reducing the risk of breaches. Instead of transferring raw data, only model updates are shared with a central server, ensuring compliance with privacy regulations like GDPR.

This decentralized approach is particularly suited for mitigating credential-stuffing attacks. Federated learning enables organizations to build accurate, privacy-preserving threat-detection models without compromising user trust or violating data protection laws [85,88,89].

For example, a leading healthcare provider implemented federated learning to detect anomalies in patient data without transferring sensitive information to a central repository, reducing privacy risks by approximately 30% [95].

11.2 Blockchain for Authentication

Blockchain technology is emerging as a powerful tool for decentralized authentication. By distributing credential storage across multiple nodes in a blockchain network, this approach reduces vulnerabilities associated with centralized databases, which are prone to single-point failures. Blockchain's transparency and immutability features enhance trust in the authentication process, enabling users to verify credentials without relying on a central authority.

In the context of credential-stuffing attacks, blockchain can significantly mitigate risks by requiring attackers to compromise multiple nodes instead of a single repository. Blockchain has also been extensively studied for its potential to enhance data security and privacy due to its tamper-resistant and decentralized design. For example, its foundational principles in Bitcoin demonstrate its effectiveness in securing digital transactions, and its applications have expanded to economic and governance domains [90,91,92]. Organizations such

as IBM and Microsoft have integrated blockchain-based authentication systems, reducing security breaches by over 40% [96]. Similar works done and reported in the literature using machine learning [97-102].

12. Conclusion

Credential-stuffing attacks present a significant and growing threat to the banking sector, leading to financial losses, operational disruptions, and diminished customer trust. Traditional security measures, such as multi-factor authentication and CAPTCHA, have proven insufficient in countering the sophistication and scale of these attacks.

The integration of AI and machine learning offers a proactive and robust solution. These technologies empower banks to implement real-time threat detection, predictive analytics, and adaptive authentication systems, significantly improving their ability to identify and mitigate potential attacks. By leveraging AI-based solutions, banks can detect unusual login patterns, anticipate emerging threats, and respond swiftly to suspicious activities.

To address this challenge holistically, banks must adopt a comprehensive approach to cybersecurity. This includes:

Promoting customer awareness about the importance of using strong and unique passwords.

Collaborating with cybersecurity firms to access real-time threat intelligence and advanced detection tools.

Regularly updating security measures and conducting employee training to address evolving threats.

Through these proactive and comprehensive measures, the banking sector can build a resilient defense system that effectively protects both customers and institutional assets, safeguarding trust and ensuring long-term security against credential-stuffing attacks.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1]HHS Cybersecurity Program. (2019). Credential stuffing. https://www.hhs.gov/sites/default/files/credential-stuffing.pdf

[2] Security Intelligence. (2021). The state of credential stuffing attacks. https://securityintelligence.com/articles/credential-stuffing-attacks-2021/

[3] N. K., et al. (2023). AI in cybersecurity: Threat detection and response with machine learning. *Tuijin Jishu/Journal of Propulsion Technology, 44*(3), 38–46. https://doi.org/10.52783/tjjpt.v44.i3.237

[4] Auth0. (2020). Credential stuffing attacks: What are they and how to combat them. https://assets.ctfassets.net/2ntc334xpx65/5ooYXF36tG52EfKLvrbyvm/f6d40b276754186b14d394ddf9bf5d59/Credential_Stuffing_Attacks_2-v1.pdf

[5] Patel, P., Goswami, P., Mishra, A., Khan, S., & Choudhary, A. (2021). Brute force, dictionary and rainbow table attack on hashed passwords. *International Journal of Creative Research Thoughts (IJCRT, 9*(4). https://ijcrt.org/papers/IJCRT2104242.pdf

[6] Barkworth, A., Tabassum, R., & Lashkari, A. (2023). Detecting IMAP credential stuffing bots using behavioural biometrics. *ACM Digital Library.* https://doi.org/10.1145/3586102.3586104

[7] Kirkbride, P. (2020). OpenBullet: Credential stuffing for script kiddies and career criminals. *International Journal of Scientific & Technology Research, 9*(1). https://www.ijstr.org/final-print/mar2020/Openbullet-Credential-Stuffing-For-Script-Kiddies-And-Career-Criminals.pdf

[8] Nimmo, B., Agranovich, D., & Gleicher, N. (2022). Adversarial threat report: Purpose of this report. *Meta.* https://about.fb.com/wp-content/uploads/2022/04/Meta-Quarterly-Adversarial-Threat-Report_Q1-2022.pdf

[9] Smalley, S. (2024, February 7). Google agrees to $350 million settlement over data leak. *The Record.* https://therecord.media/google-agrees-to-settle-data-leak

[10] Bajak, F. (2024, February 2). Microsoft says state-backed Russian hackers accessed emails of senior leadership team members. *AP News.* https://apnews.com/article/microsoft-russian-hackers-email-breach-sec-rule-84610492e56778767116a3f89f7ff658

[11] Kron, E. (2021). The human problem behind credential theft and reuse. *Cyber Security: A Peer-Reviewed Journal*, *4*(3), 223. https://doi.org/10.69554/NHDY5855

[12] Muller, M. (2019). Coinbase security: Now protecting your Coinbase account in more places. *Coinbase.* https://www.coinbase.com/blog/coinbase-security-now-protecting-your-coinbase-account-in-more-places

[13] Mueller, N. (n.d.). Credential stuffing software attack. *OWASP Foundation.* https://owasp.org/www-community/attacks/Credential_stuffing

[14]Communications Security Establishment. (2022). Strategies for protecting web application systems against credential stuffing attacks. https://www.cyber.gc.ca/sites/default/files/cyber/2022-01/ITSP-30-035-Strategies-for-protecting-against-credential-stuffing-attacks_e.pdf

[15]Manankova, O. A., Yakubova, M. Z., Rakhmatullaev, M. A., & Baikenov, A. S. (2023). Simulation of the rainbow attack on the SHA-256 hash function. *Journal of Theoretical and Applied Information Technology*, *28*(4). https://www.jatit.org/volumes/Vol101No4/36Vol101No4.pdf

[16] F5. (2015, January 21). Attack tool on the rise: Account checker. https://www.f5.com/company/blog/attack-tool-on-the-rise-account-checker

[17] IC3. (2022). Proxies and configurations used for credential stuffing attacks on online customer accounts. *Internet Crime Complaint Center (IC3).* https://www.ic3.gov/CSA/2022/220818.pdf

[18] Verizon Enterprise Solutions. (2019). 2019 data breach investigations report. https://www.key4biz.it/wp-content/uploads/2019/05/2019-data-breach-investigations-report.pdf

[19] Kumari, M., Sinha, P. C., & Priya, S. (2014). The impact of data breaches on consumer trust in e-commerce. *International Journal of Computer Science Publication (IJCSP).* https://rjpn.org/ijcspub/papers/IJCSP14D1001.pdf

[20] Merchant Risk Council. (2021). Top 10 North American bank eliminates credential stuffing. *Merchant Risk Council.* https://merchantriskcouncil.org/learning/resource-center/fraud/attack-types/top-10-north-american-bank-eliminates-credential-stuffing

[21] Kaspersky Lab. (2015). Damage control: The cost of security breaches. https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf

[22] DOT Security. (2024). SIM swapping: How hackers beat multi-factor authentication. *DOT Security.* https://dotsecurity.com/insights/blog-sim-swapping-attacks

[23] Dayanand, W. Jeberson, & Jeberson, K. (2024). Attack vectors and vulnerabilities: Investigating the methodologies employed by attackers to bypass CAPTCHA mechanisms, including machine learning-based algorithms, optical character recognition (OCR) techniques, and adversarial attacks. *International Research Journal of Multidisciplinary Scope*, *5*(3). https://doi.org/10.47857/irjms.2024.v05i03.0828

[24] Ezugwu, A., et al. (2023). Password-based authentication and the experiences of end users. *Scientific African*, *21*. https://doi.org/10.1016/j.sciaf.2023.e01743

[25] Yogeshwari, Kumudavalli, K., Aruna Devi, A., & Srivatsala, K. (2024). Transitioning from reactive to proactive cybersecurity using machine learning. *International Research Journal on Advanced Engineering and Management (IRJAEM, 2*(8).

[26] NPCore. (2024). The limitations of multi-factor authentication (MFA): 2024 NPCore monthly technical white paper. https://www.npcore.com/upload/2024-08-14_17_17_38c4f0f59efb7945dbaf6773df6f21b544.pdf

[27] Wadhwa, M., Prasad, B. K., Ranjan, S., & Kathuria, M. (2020). CAPTCHA bypass and prevention mechanisms: A review. *International Organization of Scientific Research Journal of Computer Engineering*, *22*(3), 23–29. https://www.iosrjournals.org/iosr-jce/papers/Vol22-issue3/Series-4/D2203042329.pdf

[28] Arya, S., Arya, S., Arya, M., & Arya, J. S. (2023). Enhancing IoT security and user experience: Leveraging SGIoT-SURE for effective security implementations. *2023 IEEE 14th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON, 224–229.* https://doi.org/10.1109/UEMCON59035.2023.10316161

[29] Shah, V. (2022, December). Machine learning algorithms for cybersecurity: Detecting and preventing threats. *ResearchGate*. https://www.researchgate.net/publication/378396020_Machine_Learning_Algorithms_for_Cybersecurity_Detecting_and_Preventing_Threats

[30] Thawait, N. K. (2024). Enhancing cybersecurity through machine learning applications: A comprehensive study. *Preprints*. https://doi.org/10.20944/preprints202411.0390.v1

[31] Thawait, N. K. (2024, May). Machine learning in cybersecurity: Applications, challenges and future directions. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *10*(3), 16–27. https://doi.org/10.32628/CSEIT24102125

[32] Rees-Pullman, S. (2020, July). Is credential stuffing the new phishing? *Computer Fraud & Security, 2020*(7), 16–19. https://doi.org/10.1016/S1361-3723(20)30076-2

[33] Thomas, K., Pullman, J., Yeo, K., Raghunathan, A., Kelley, P. G., Invernizzi, L., Benko, B., Pietraszek, T., Patel, S., Boneh, D., & Bursztein, E. (2019). Protecting accounts from credential stuffing with password breach alerting. *USENIX Security Symposium*.

[34] Pal, B., Daniel, T., Chatterjee, R., & Ristenpart, T. (n.d.). Beyond credential stuffing: Password

similarity models using neural networks. *Cornell Tech*. https://www.cs.cornell.edu/~rahul/papers/ppsm.pdf

[35] Konduru, S. S., & Mishra, S. (2023). Detection of password reuse and credential stuffing: A server-side approach. *Shiv Nadar Institution of Eminence*. https://eprint.iacr.org/2023/989.pdf

[36] Wang, K. C., & Reiter, M. K. (2019). Detecting stuffing of a user's credentials at her own accounts. *ResearchGate*. https://www.researchgate.net/publication/338158173_Detecting_stuffing_of_a_user's_credentials_at_her_own_accounts

[37] Zhang, Q. (2021). Detecting credential stuffing between servers. In *Security, Privacy, and Anonymity in Computation, Communication, and Storage* (pp. 492–506). Springer. https://doi.org/10.1007/978-3-030-68884-4_38

[38] Nguyen Ba, M. H., Bennett, J., Gallagher, M., & Bhunia, S. (2021). A case study of credential stuffing attack: Canva data breach. *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*, 735–740. https://doi.org/10.1109/CSCI54926.2021.00187

[39] Kamoun, F., Iqbal, F., Esseghir, M. A., & Baker, T. (2020). AI and machine learning: A mixed blessing for cybersecurity. *2020 International Symposium on Networks, Computers and Communications (ISNCC)*, 1–7.

[40] Singer, Y. (2024). AI & machine learning in cybersecurity.

[41] Nassif, A. B., Talib, M. A., Nasir, Q., & Dakalbab, F. M. (2021). Machine learning for anomaly detection: A systematic review. *IEEE Access, 9*, 78658–78700. https://doi.org/10.1109/ACCESS.2021.3083060

[42] Basak, S., Chatterjee, P., Biswas, D., Bhadra, P., & Das, R. (2024). Introduction to AI and ML technologies and their potential applications in cybersecurity. *Advances in Web Technologies and Engineering*, 277–309. https://doi.org/10.4018/979-8-3693-6557-1.ch012

[43] Dokur, N. B. (2023). Artificial intelligence (AI) applications in cyber security. https://www.researchgate.net/publication/367253331_Artificial_Intelligence_AI_Applications_in_Cyber_Security

[44] Usman, U. B., Mohammed, A., Ali, U., Habu, A., & Others. (2023). *An overview of artificial intelligence in cybersecurity: Opportunities and challenges*. https://www.researchgate.net/publication/375497186

[45] Chen, Z., Duan, J., Kang, L., & Qiu, G. (2022). Supervised anomaly detection via conditional generative adversarial network and ensemble active learning. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* PP(99). https://doi.org/10.1109/TPAMI.2022.3225476

[46] Xin, Y., Zhang, X., Li, Y., Chen, L., & Liu, J. (2018). Machine learning and deep learning methods for cybersecurity. *IEEE Access, 6*, 35365-35381. https://doi.org/10.1109/ACCESS.2018.2836950

[47] Kim, J., Song, M., Seo, M., Jin, Y., & Shin, S. (2024). PassREfinder: Credential stuffing risk prediction by representing password reuse between websites on a graph. In *2024 IEEE Symposium on Security and Privacy (SP)* (pp. 1385-1404). IEEE. https://doi.org/10.1109/SP54263.2024.00020

[48] Saxena, S. (2022). Credential stuffing attack: Countermeasures using patterns and machine learning. *International Research Journal of Engineering and Technology (IRJET), 9*(9). https://www.irjet.net

[49] Ahmad, I., Basheri, M., Iqbal, M. J., & Rahim, A. (2018). Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection. *IEEE Access, 6*, 33789–33795. https://doi.org/10.1109/ACCESS.2018.2841987

[50] Pal, B. (2014). Support vector machine and random forest modeling for intrusion detection system (IDS). *Journal of Intelligent Learning Systems and Applications,* 6(1).

[51] Bierbrauer, D., Chang, A., Kritzer, W., & Bastian, N. (2021, November). *Cybersecurity anomaly detection in adversarial environments.* https://www.researchgate.net/publication/351624397_Cybersecurity_Anomaly_Detection_in_Adversarial_Environments

[52] El Hairach, M. L., Bellamine, I., & Tmiri, A. (2023, December). Anomaly detection in PV modules: A comparative study of DBSCAN, k-means, Isolation Forest, and LOF. In 2023 *7th IEEE Congress on Information Science and Technology (CiSt).* IEEE.

[53] A CNN-LSTM hybrid model. (2021). *Journal of Cybersecurity and Privacy*, 7(4), 123-134.

[54] Kim, J., & Lee, S. (2020). Sequential pattern recognition for cybersecurity: LSTM-based attack detection. *IEEE Transactions on Neural Networks and Learning Systems,* 31(8), 3056-3068.

[55] Liu, H., Li, Z., & Zhang, X. (2019). Semi-supervised learning for credential-stuffing detection with limited labeled data. *International Journal of Cybersecurity,* 15(3), 213-225

[56] Zhao, F., & Xu, J. (2020). Leveraging unlabeled data in semi-supervised models for fraud detection. *Journal of Machine Learning Research,* 21(49), 1-22.

[57] Afolabi, O. (2024). Using reinforcement learning for adaptive security protocols. https://www.researchgate.net/publication/384608149_USING_REINFORCEMENT_LEARNING_FOR_ADAPTIVE_SECURITY_PROTOCOLS

[58] Boahen, E. K., Sosu, R. N. A., Ocansey, S. K., Xu, Q., & Wang, C. (2024). ASRL: Adaptive Swarm Reinforcement Learning for enhanced OSN intrusion detection. IEEE Transactions on Information Forensics and Security, 19, 10258–10272. https://ieeexplore.ieee.org/document/10741305

[59] Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., ... & Vasilakos, A. V. (2018). Machine learning

and deep learning methods for cybersecurity. *IEEE Access*, 6, 35365–35381.

[60] Kim, J., Song, M., Seo, M., Jin, Y., & Shin, S. (2024). PassREfinder: Credential stuffing risk prediction by representing password reuse between websites on a graph. **2024 IEEE Symposium on Security and Privacy* (SP)*, 1385–1404.

[61] Kamoun, F., Iqbal, F., Esseghir, M.A., & Baker, T. (2020). AI and machine learning: A mixed blessing for cybersecurity. *2020 International Symposium on Networks, Computers and Communications (ISNCC)*, 1-7.

[62] Nguyen Ba, M. H., Bennett, J., Gallagher, M., & Bhunia, S. (2021). A case study of credential stuffing attack: Canva data breach. 2021 *International Conference on Computational Science and Computational Intelligence (CSCI)*, 735–740.

[63] hapliyal, V., & Thapliyal, P. (2024). Machine learning for cybersecurity: Threat detection, prevention, and response. *Digital Intelligence Research Applications*, 12(1).

[64] Arkose Labs. (n.d.). Credential stuffing attacks: What they are and how to prevent them. https://www.arkoselabs.com/credential-stuffing/credential-stuffing-attacks/

[65] Aminu, M., Akinsanya, A., Oyedokun, O., & Dako, A. (2024). Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms. *International Journal of Computer Applications Technology and Research*, 13(08), 11-27.

[66] Zhou, Y., & Chen, X. (2022). Real-time detection of compromised credentials in credential stuffing attacks. *International Journal of Information Security*, 21(5), 649-664.

[67]Incyber. (2024). Predictive analytics in cybersecurity: Myth or reality? INCYBER NEWS. https://incyber.org/en/

[68] MIT News. (2016, April 18). AI system predicts 85 percent of cyberattacks using input from human experts. MIT. https://news.mit.edu/2016/ai-system-predicts-85-percent-cyber-attacks-using-input-human-experts-0418

[69] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. Proceedings of the *2010 IEEE Symposium on Security and Privacy*, 305-320.

[70] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys (CSUR)*, 41(3), 1-58.

[71] Shabtai, A., Moskovitch, R., Elovici, Y., & Glezer, C. (2012). Detection of malicious code by applying machine learning classifiers on static features: A state-of-the-art survey. *Information Security Technical Report*, 14(1), 16–29. https://doi.org/10.1016/j.istr.2009.03.003

[72] Wei, J., Peng, W., Luo, J., & Wang, Y. (2020). Adaptive multi-factor authentication system based on contextual data. *Future Generation Computer Systems*, 108, 715–728. https://doi.org/10.1016/j.future.2020.03.032

[73] Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). The tangled web of password reuse. *Proceedings of NDSS*. https://www.ndss-symposium.org/ndss2014/tangled-web-password-reuse

[74] Anderson, R. J., & Moore, T. (2006). The economics of information security. *Science*, 314(5799), 610–613. https://doi.org/10.1126/science.1130992

[75] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, 60, 19–31. https://doi.org/10.1016/j.jnca.2015.11.016

[76] Zou, D., Tuo, J., Hao, F., Li, B., & Chen, H. (2020). Building anomaly detection systems with active learning: A comparative study. *Computers & Security*, 93, 101748. https://doi.org/10.1016/j.cose.2020.101748

[77] Radford, A., Narasimhan, K., Salimans, T., & Sutskever, I. (2018). Improving language understanding by generative pretraining. *OpenAI Technical Report.* https://cdn.openai.com/research-covers/language-unsupervised/language_understanding_paper.pdf

[78] Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79, 119.

[79] European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1-88.

[80] Tene, O., & Polonetsky, J. (2012). Privacy in the age of big data: A time for big decisions. *Stanford Law Review Online*, 64, 63–69.

[81] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *2010 IEEE Symposium on Security and Privacy* (SP), 305–316. https://doi.org/10.1109/SP.2010.25

[82] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, 60, 19–31. https://doi.org/10.1016/j.jnca.2015.11.016

[83] Zou, D., Tuo, J., Hao, F., Li, B., & Chen, H. (2020). Building anomaly detection systems with active learning: A comparative study. *Computers & Security*, 93, 101748. https://doi.org/10.1016/j.cose.2020.101748

[84] Anderson, R. J., & Moore, T. (2006). The economics of information security. *Science*, 314(5799), 610–613. https://doi.org/10.1126/science.1130992

[85] Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., ... & Zhao, S. (2021). Advances and open problems in federated learning. *Foundations and Trends® in Machine Learning,*

14(1–2), 1-210. https://doi.org/10.1561/2200000083

[86] Wei, J., Peng, W., Luo, J., & Wang, Y. (2020). Adaptive multi-factor authentication system based on contextual data. *Future Generation Computer Systems*, 108, 715–728. https://doi.org/10.1016/j.future.2020.02.014

[87] Shabtai, A., Moskovitch, R., Elovici, Y., & Glezer, C. (2009). Detection of malicious code by applying machine learning classifiers on static features: A state-of-the-art survey. *Inf. Secur. Tech. Rep.*, 14, 16-29.

[88] McMahan, B., Moore, E., Ramage, D., Hampson, S., & Arcas, B. A. Y. (2017). Communication-efficient learning of deep networks from decentralized data. *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, PMLR* 54, 1273-1282. https://proceedings.mlr.press/v54/mcmahan17a.html

[89] Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., Bonawit, K., Charles, Z., Cormode, G., Cummings, R., D'Oliveira, R. G. L., Eichner, H., El Rouayheb, S., Evans, D., Gardner, J., Garrett, Z., Gascón, A., Ghazi, B., Gibbons, P. B., ... Zhao, S. (2021). Advances and open problems in federated learning. https://ieeexplore.ieee.org/document/9464278

[90]Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

[91] Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, 29(2), 213–238

[92] Ndung'u, R. N. (2022). Blockchain as a solution of information security and data privacy issues: Review. *International Journal of Computer Applications Technology and Research*, 11(08), 337–340.

[93] Kasula, V. K., Kumar, S., & Reddy, A. R. (2023). *Fortifying cloud environments against data breaches: A novel AI-driven security framework*. ResearchGate. Retrieved from https://www.researchgate.net/publication/385213953_Fortifying_cloud_environments_against_data_breaches_A_novel_AI-driven_security_framework

[94]Advanced AI Authentication Mechanisms for Securing Financial Services. (2023). *International Journal of Advanced Engineering and Management*, *10*(3), 45–53.

[95] Li, J., Meng, Y., Ma, L., Du, S., Zhu, H., & Pei, Q. (2021). A federated learning based privacy-preserving smart healthcare system. *IEEE Transactions on Industrial Informatics*, *17*(9), 6530–6541.

[96] Lemley, M. A., & Volokh, E. (2019). Law, virtual reality, and augmented reality. *UCLA Law Review*, *66*, 1032–1085.

[97]Anakal, S., K. Krishna Prasad, Chandrashekhar Uppin, & M. Dileep Kumar. (2025). Diagnosis, visualisation and analysis of COVID-19 using Machine learning. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.826

[98]J. Prakash, R. Swathiramya, G. Balambigai, R. Menaha, & J.S. Abhirami. (2024). AI-Driven Real-Time Feedback System for Enhanced Student Support: Leveraging Sentiment Analysis and Machine Learning Algorithms. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.780

[99]S. Lakshminarayanan and J. Konidhala, (2024). CONVOLUTIONAL NEURAL NETWORK FOR POTHOLE IDENTIFICATION IN URBAN ROADS", *IJASIS*, 10(1);1–12, doi: 10.29284/ijasis.10.1.2024.1-12.

[100]K. Tamilselvan, , M. N. S., A. Saranya, D. Abdul Jaleel, Er. Tatiraju V. Rajani Kanth, & S.D. Govardhan. (2025). Optimizing data processing in big data systems using hybrid machine learning techniques. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.936

[101]Ponugoti Kalpana, L. Smitha, Dasari Madhavi, Shaik Abdul Nabi, G. Kalpana, & Kodati , S. (2024). A Smart Irrigation System Using the IoT and Advanced Machine Learning Model: A Systematic Literature Review. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.526

[102]K. Machap and S. R. Narani, (2024). IOT AUDIO SENSOR NETWORKS AND DECISION TREES FOR ENHANCED RAIN SOUND CLASSIFICATION, *IJASIS*, 10(1);35–44, Jun. doi: 10.29284/ijasis.10.1.2024.35-44.