Journal of Universal Computer Science, vol. 31, no. 14 (2025), 1690-1716
submitted: 17/3/2025, accepted: 30/6/2025, appeared: 28/12/2025

Development of Reliable Access Control Mechanisms Using Artificial Intelligence for Corporate Data Protection

Przemyslaw Jatkiewicz
(University of Gdańsk, Gdańsk, Poland
https://orcid.org/0009-0007-6882-7097, jat.przemyslaw@gmail.com)

Abstract: The study aims to analyse the vulnerabilities of traditional access control methods and define optimization objectives, constraints, and decision-making processes based on data for the effective implementation of artificial intelligence to enhance corporate data protection. The research methodology addressed various approaches, including machine learning, user behaviour analysis and neural networks, and data protection methods such as anonymisation, encryption and federated learning. Traditional access control methods, such as passwords, biometrics and multi-factor authentication, were discussed, as well as their shortcomings, including vulnerability to data breaches, phishing attacks and infrastructure threats. The use of artificial intelligence to strengthen access control mechanisms, such as machine learning, user behaviour analysis and neural networks, was emphasised. Artificial intelligence significantly improves security by enabling the analysis and processing of large amounts of data, detecting anomalies and predicting threats based on the analysis of user behaviour and biometric data. The study also examined methods of protecting data used to train artificial intelligence, including anonymisation, differential privacy, encryption and federated learning. Privacy issues the risks of data leakage when using artificial intelligence and the need to comply with ethical norms and standards were addressed. The successful integration of AI-oriented solutions into corporate security systems in various industries, including the financial sector, healthcare, and retail, is presented. Evaluating the effectiveness of artificial intelligence in access control systems is based on indicators such as the speed of the system's response to changes in user behaviour, the number of false positives and successfully prevented incidents. The study also developed recommendations for improving access control mechanisms using artificial intelligence, including the introduction of machine learning-based systems to detect anomalies in user behaviour, and the integration of AI with multi-factor authentication to create flexible and reliable data protection mechanisms.

Keywords: Authentication, Biometrics, Machine Learning, Neural Networks, Integration
Categories: H, I, E
DOI: 10.3897/jucs.153217

1 Introduction

In the modern world, where the volume of data and the number of cyber threats is growing at an incredible rate, ensuring the security of corporate data is a top priority for organisations. Traditional access control methods, such as passwords, biometrics and multi-factor authentication (MFA) are widely used to protect information. However, despite their widespread use, these methods have significant drawbacks, including vulnerability to attacks such as phishing, and password leakage, and the complexity and cost of implementing biometric systems. The emergence of artificial intelligence (AI) in cybersecurity created new opportunities to improve the effectiveness of access control systems. AI is capable of analysing large amounts of data in real-time, detecting anomalies and adapting to new threats. The use of machine learning techniques, including neural networks and user behavior analysis, can significantly improve the accuracy of identifying and predicting potential threats, providing a higher level of data protection.

One of the key challenges is the need to ensure reliable protection of data used to train AI models. Traditional methods of protecting information, such as encryption and access control, while still important, are not always able to provide sufficient protection against modern threats. This creates the need to develop and apply new approaches, such as anonymisation, pseudonymisation and differential privacy. However, their implementation is fraught with several challenges, including maintaining the accuracy of AI models, protecting privacy, and complying with legal requirements such as the General Data Protection Regulation (GDPR) [GDPR 2016] and other data protection standards. The research problem is how to effectively implement data protection methods in AI training while maintaining high-quality analysis results and compliance with regulatory requirements.

The main problem is that modern cybersecurity threats are becoming increasingly sophisticated and capable of circumventing traditional defence methods. [Mazur 2023] analysed the impact of AI on data protection and proposed regulatory measures that can be applied to protect personal information following the GDPR. As a result, the author emphasised the importance of balancing technological development with legal restrictions to ensure adequate data protection. [Shaik et al. 2022] emphasised the importance of implementing multi-level access control and data encryption systems to counter modern threats. It is necessary to explore ways to increase the transparency and interpretability of decisions made by AI, especially in the context of data protection and access control.

Another challenge is the difficulty of determining the appropriate allocation of access rights to data within corporate structures that involve hierarchies and employee roles. [Humayun et al. 2024] revealed that the use of AI can significantly increase the level of security of the Internet of Things (IoT). [Neelakrishnan 2024] emphasised that AI can be key in proactive data protection in cloud applications. The study proposed AI-based techniques for dynamic risk assessment and secure data access. Although the research focuses on external threats, more research is needed on protection against internal threats, such as unauthorised access by employees, as well as mechanisms to prevent errors and abuse by internal users.

The goal of [Peng et al. 2019] was to examine the consequences of credential leaks and credential sharing on phishing sites. The study provides insight into how users interact with phishing sites, specifically focusing on the behaviors following the leakage of sensitive information such as passwords. The study also emphasizes the lack of user awareness regarding the risks associated with phishing, underscoring how easily attackers can exploit these vulnerabilities to gain unauthorized access to sensitive data. This research highlights the widespread nature of credential leaks and phishing attacks, stressing their significant consequences, such as financial loss, reputational damage, and unauthorized access to personal and organizational data.

[Nadeem et al. 2023] focused on the various techniques for detecting and preventing phishing attacks, providing an overview of current prevention mechanisms. The article delves into the different types of phishing attacks, including spear-phishing, and explores the effectiveness of traditional detection methods such as email filtering and machine learning-based approaches. The research further outlines the implications of successful phishing attacks, which often lead to significant data breaches, unauthorized access to sensitive information, and financial theft. This study provides a detailed account of the continued rise of phishing attacks and their damaging effects on both individuals and organizations.

A pressing issue is that AI for access control must comply with [GDPR 2016], ensuring the protection of personal data and the right to privacy. [Hasal et al. 2021] noted that chatbots require enhanced protection to prevent security threats and ensure data confidentiality. [Bera et al. 2021] proposed the use of AI and blockchain technologies to control access and protect against malicious attacks on the Internet of Things. It is necessary to study in more detail the risks associated with the full automation of access control and data protection processes using AI to avoid situations where the system may improperly restrict access or create vulnerabilities.

The problem identified in the research area is determined by the importance for companies to not only develop robust AI for access control but also to integrate it with already existing security systems. [Omotunde & Ahmed 2023] identified that modern databases require stronger security mechanisms such as MFA and improved access control techniques to protect against advanced threats and data breaches. [Saeed et al. 2024] noted that the use of AI and digital twins brings new challenges for data protection such as the need to ensure data integrity, prevent leaks and protect sensitive information when different systems interact. Modern cybersecurity threats are constantly evolving, and research is required on methods that allow AI to adapt to new types of attacks and learn quickly to prevent them.

The study aimed to identify vulnerabilities in traditional access control methods and establish optimization objectives, constraints, and data-driven decision-making processes for the effective use of AI to enhance corporate data protection. The following tasks were formulated as part of this goal:

1. Analyse traditional access control methods and identify their vulnerabilities.
2. Investigation of the possibilities of using AI to improve the efficiency and security of access control.
3. Development of recommendations for integrating AI into corporate data protection systems.

The novelty of the research lies in the integration of AI into access control systems, which significantly improves the security of corporate data compared to traditional authentication methods such as passwords, biometrics, and MFA. For the first time, the effectiveness of using machine learning, user behavior analysis, and neural networks to improve authentication accuracy and prevent potential threats in real time has been investigated.

2 Materials and Methods

The study examines data classification and clustering techniques as key methods for detecting anomalies and potential threats in access control systems. Classification allows data to be divided into categories, enabling the identification of malicious or suspicious actions based on existing user behavior patterns. Clustering, in turn, helps to group similar data samples, allowing the detection of deviations from normal behavior patterns that may indicate unauthorized access. Machine learning algorithms are used to detect anomalies. These algorithms are trained on a large amount of historical data, analyzing user behavior and detecting anomalies in real time. This allows the system to quickly respond to new threats and adapt to changes in user behavior, which significantly improves the accuracy of anomaly detection and reduces the risk of unauthorized access. These approaches improve the security and adaptability of the system compared to traditional authentication methods.

The first step was to investigate existing access control methods such as passwords and personal identification numbers (PINs). The focus was on an analysis of authentication technologies and their vulnerabilities, including data breaches, phishing and brute force attacks. The research process examined different approaches to creating passwords, their complexity and their resistance to cracking techniques. Biometric systems based on fingerprints, facial recognition and retina recognition were also studied. The risks of biometric data tampering, the lack of accuracy when the user's physical characteristics change, and the potential for misuse of this data were emphasised. In addition, traditional MFA models, including combinations of passwords and one-time codes, were analysed, as well as the factors that make them vulnerable to infrastructure attacks.

The second stage analysed the potential of AI to improve the security of access control systems. The capabilities of machine learning to analyse user behaviour and detect anomalies in real-time were considered. The use of machine learning algorithms can identify suspicious activity and automatically respond to potential threats. The use of neural networks to improve the accuracy of biometric technologies such as facial and fingerprint recognition has also been explored. They can significantly improve security by adapting to changes in user appearance. Adaptive MFA schemes that rely on analysing the behaviour and context of user actions have also been considered.

The study assessed the effectiveness of implementing AI in existing access control systems. The key benefits include increased accuracy of biometric identification, automation of the threat detection process, and the ability to analyse big data to predict potential breaches. The assessment was carried out using a SWOT analysis, which was used to systematise the benefits and risks of implementing new technologies. A threat scenario analysis was also carried out to assess the possible consequences of unsuccessful AI implementation.

Data protection techniques used in training AI models were investigated to expand the understanding of the role of AI in access control systems. Protection of user privacy in the context of biometric systems and user behaviour was addressed. Anonymisation, pseudonymisation and differential privacy techniques were considered to minimise the risk of data breaches and ensure compliance with legislation such as [GDPR 2016]. The use of data encryption at all stages of processing and storage was also discussed as a way to mitigate risks. Importantly, user data should be protected not only at the processing stage but also during storage.

In the final stage, a scenario analysis of the threats associated with the introduction of AI was performed. This included the risks of misusing the technology to bypass existing defences, as well as ethical and privacy issues when processing personal data. The importance of continuously monitoring AI models and updating them regularly to minimise vulnerabilities was explored, which is critical for security. The need for clear policies and standards to protect user data and for organisations to train employees on how to handle this data correctly was also highlighted.

In the process of the research, a methodology was developed, including the stages of analysing existing access control methods and assessing the possibilities of applying AI to improve security. Based on the analysis of existing approaches and technologies, several recommendations for improving access control systems were formulated. It is recommended to integrate machine learning systems to analyse user behaviour, thereby increasing the accuracy of anomaly detection and improving security. In addition, recommendations for combining AI with traditional authentication methods, such as passwords, biometrics and one-time codes, to create more flexible and secure access control mechanisms were developed. The development of security standards and policies to protect user data, including the use of anonymisation and differential privacy techniques, is also important, minimizing the risks of data breaches and promoting compliance with privacy standards.

3 Results

3.1. Traditional access control methods: Assessment and weaknesses

Traditional access control methods such as passwords, biometrics and MFA are widely used to protect corporate data, but each has its characteristics, advantages and disadvantages. Passwords are the most common authentication method used to protect user accounts and prevent unauthorised access. The advantages of passwords are ease of implementation and low cost. However, their security is often insufficient. Passwords can be easily obtained through brute-force attacks, as well as stolen through phishing or data breaches. Moreover, many users use the same passwords for multiple services, increasing the risk of compromise.

However, biometrics also has its weaknesses. Both false positive and false negative rates remain significant concerns. False positives occur when the system incorrectly grants access to an unauthorized individual, while false negatives happen when the system fails to recognize an authorized user. Additionally, biometrics are difficult to change if compromised, making them vulnerable to theft. Moreover, the cost of implementing biometric systems is quite high.

MFA combines two or more authentication methods such as password, biometrics and a one-time code sent to a mobile device [Mohammed et al. 2023]. This method significantly increases the security level as an attacker will need to overcome multiple layers of defence. However, MFA can be inconvenient for users as it requires multiple steps and its effectiveness depends on how secure all the methods used are. For instance, codes sent via SMS are vulnerable to attacks such as message interception, and access to the mobile device may be restricted.

Adaptive authentication can be formalized as a sequential decision-making task using the Partially Observable Markov Decision Process (POMDP) model. In this model, the authentication process is viewed as a sequence of decisions where the system must make decisions about the level of access to resources based on partial information about the user and the current situation.

In this context, each state in POMDP can represent the user's current situation, including their behavior profile, authentication type (e.g., password, biometrics, token), and contextual factors such as time of day, location, or the device from which access is being made. User information is partially observable, as not all aspects of behavior can be tracked directly. Therefore, the system makes assumptions about the user's state based on available observations.

The decision at each stage will be to select authentication methods or request additional verification, depending on the assessment of the current risk. For example, if a user logs in from an unusual location or device, the system may decide to increase the authentication level by requesting additional verification or denying access. An important part of this model is determining the risk threshold at which additional security measures need to be initiated.

To formalize the task as a POMDP, it is necessary to define a cost function that minimizes the probability of unauthorized access (type I errors) while reducing the probability of requesting additional authentication under normal conditions (type II errors). In addition, in POMDP models, it is important to consider different strategies that adapt to changes in user behavior and the environment, optimizing the authentication process in real time based on new data. To evaluate the effectiveness of adaptive authentication and compare different methods, simulation platforms and datasets such as NSL-KDD or CICIDS, which are standard datasets for testing security systems, can be used. These platforms allow for the analysis of real and synthetic data, providing simulation of various authentication scenarios and real-time anomaly detection [Abdulrahman & Alhayani 2023].

Metrics that can be used to evaluate the effectiveness of models include accuracy, which determines the correctness of user identification, precision, which measures the ratio of correct positive results to all positive results, and latency, which estimates the time required to complete the authentication or anomaly detection process. Using these metrics allows you to evaluate the performance of the system in real-world conditions and optimize it to improve security and user convenience.

To demonstrate the effectiveness of AI solutions in access control, a small-scale experiment was conducted using a synthetic dataset that simulates typical information about user attempts to access the system. This experiment took into account characteristics such as login time, device type, user location, login frequency, and the presence of suspicious activity. For the experiment, 1,000 records were created, with each record representing a user's attempt to access the system. The features used were time of day (in 24-hour format), device type (phone or computer), location (normal or suspicious), login frequency per day, and a suspicious activity flag (where 1 means suspicious activity and 0 means normal access).

The Random Forest machine learning algorithm was used to analyze and detect anomalies. This method was chosen because of its ability to work effectively with large amounts of data and detect complex patterns in user behavior. The model was trained on 70% of the data, and the remaining 30% was used to test the results. After training the model, the results showed a classification accuracy of 71.67%, a detection accuracy of suspicious access attempts of 23.26%, and a recall rate of 16.13%. This indicates that the model can detect suspicious activity, but its ability to detect real anomalies needs improvement. The detection accuracy and the model's ability to adapt to changing conditions require further optimization of the algorithms, which will reduce the number of false positives and increase the effectiveness of anomaly detection.

Among the major problems of traditional access control systems are password leaks and phishing [Peng et al. 2019]. Password leaks occur when hackers gain access to the database where user passwords are stored, which can cause unauthorised access to accounts and sensitive data [Metelskyi & Kravchuk 2023]. The causes of these leaks are often related to the use of weak passwords, reusing them for different accounts, or improper data storage (e.g., lack of hashing). The consequences of password leaks can include financial loss, loss of reputation, and compromised customer data. Phishing is another common threat. Attackers deceive users by creating fake web pages or sending false messages to obtain passwords or other sensitive information [Kravchuk et al. 2024]. The main problem is low awareness among users who may not notice signs of phishing, such as incorrect URLs or unsafe sites. The consequences of phishing can be severe: data theft, financial loss and leakage of sensitive information. There is also the threat of infrastructure attacks that allow attackers to bypass traditional access controls. These attacks can involve compromising servers, networks or applications, as well as exploiting vulnerabilities related to system misconfiguration or outdated software. The consequences of such attacks can range from unauthorised access to data corruption or destruction, which can significantly disrupt a company's operations. As a result, traditional access control systems face several serious vulnerabilities. Although common, methods such as passwords, biometrics and MFA do not provide complete protection against threats such as data breaches, phishing and infrastructure attacks.

The Real-Time Anomaly Detection module is responsible for monitoring and analyzing user behavior in real time to detect suspicious activity that may indicate unauthorized access attempts or other threats. The data flow begins with the collection of information about user actions, such as login time, login location, device used, IP address, etc. This data is processed by machine learning algorithms or other methods, such as classification and clustering. The system compares the information obtained with normal user behavior patterns and detects anomalies. If a deviation from the usual profile is detected, the system decides on further actions. This may include requesting additional authentication, restricting access to sensitive data, or completely blocking access to the system. The decision-making logic is based on thresholds set for each parameter, such as login time or location, as well as the degree of deviation from normal behavior.

The Adaptive Access Control module allows you to dynamically change the access level depending on changes in user behavior or circumstances, such as time of day or location. The system continuously assesses risk based on changes in user behavior, such as new access attempts from unusual locations or the use of a new device. Depending on the risk assessment, the system automatically adapts the access level. For example, if a user attempts to access sensitive data at an unusual time or from an unfamiliar location, access may be restricted or require additional authentication. A dynamic profile is created for each user, which is updated in real time to reflect changes in their behavior. The module can also adjust the access level depending on the context, taking into account whether the user has special permissions or a role in the organization.

As a result, both modules integrate AI technologies to improve access security. The Real-Time Anomaly Detection module actively detects deviations in user behavior, while Adaptive Access Control allows for flexible access adjustment based on current conditions and behavioral changes, providing more accurate and secure access control without significant inconvenience to users. The application of AI in access control mechanisms significantly improves security, thanks to AI's ability to effectively analyse and process large amounts of data to identify anomalies and threats [Patricheev 2025]. There are several main AI approaches used to improve access control systems, including machine learning, user behaviour analysis and neural networks.

Machine learning (ML) is a data analysis technique in which algorithms are trained on large amounts of historical information to identify patterns and anomalies [Nti et al. 2022]. In the context of access control, this can include training patterns on user behaviour data as well as using algorithms to automatically detect threats. Machine learning can analyse large amounts of data in real-time, identifying suspicious behaviour faster than traditional systems and adapting to changes in user behaviour, improving the accuracy of threat detection over time [Jurkevičius & Pleskach 2025]. In authentication systems, machine learning can be used to create dynamic profiles of users that are updated based on their actions, such as log-in frequency, activity times and access to specific data. If the algorithm detects deviations from normal behaviour, it can request additional authentication or block access. Figure 1 illustrates a comparison between traditional methods and methods with AI in access control systems, highlighting how AI significantly improves a system's ability to detect threats.

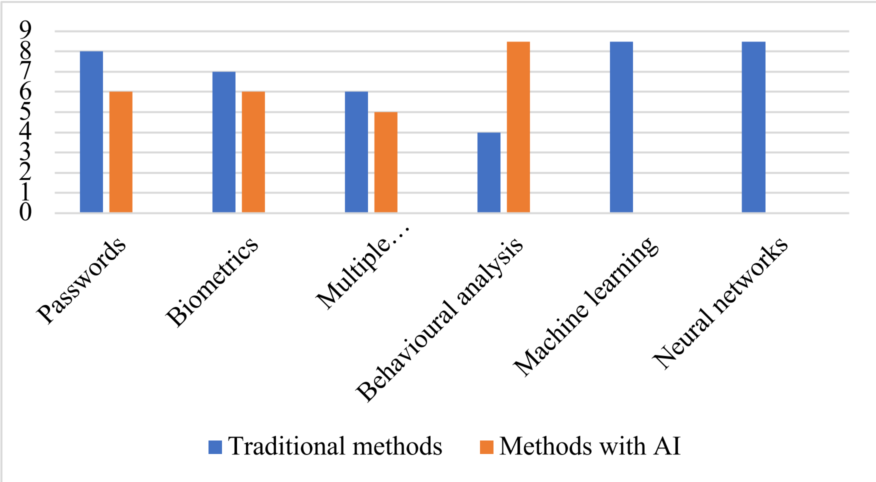

Figure 1: Comparison of traditional and AI methods in access control systems

Source: compiled by the author based on [Attkan & Ranga 2022].

User Behaviour Analytics (UBA) uses AI to monitor and analyse a user's actions in a system to detect deviations from their usual behaviour [Martín et al. 2021]. This can include analysing login times and locations, devices used, IP addresses and actions within the system. Such analysis can identify anomalies that may indicate an attempted hacking or unauthorised access and provide proactive protection by preventing attacks at the detection stage. For instance, if an employee normally works in the office during business hours and suddenly accesses sensitive data overnight from another region, the system can initiate a review, request additional authentication or restrict access.

Neural networks, especially deep neural networks, can be used to analyse and recognise complex patterns in data. In the context of access control, neural networks can be trained on large amounts of data to recognise faces, fingerprints or other biometric data, and to analyse user behaviour [Zile et al. 2023]. Neural networks can efficiently recognise complex patterns, rendering them capable of biometric authentication and anomaly analysis. For example, neural networks can be used to recognise faces in video surveillance systems, providing automatic verification of employees' identity and their access to certain areas in a company. To develop effective data protection mechanisms in the context of AI training, several key areas can be identified, such as machine learning algorithms for analysing user behaviour, biometric authentication methods and advanced approaches to MFA using AI.

Machine learning algorithms for analysing user behaviour are substantial for detecting anomalies and potential security threats [Aviv et al. 2024]. These algorithms can analyse data about users' actions on the platform, such as time spent in the system, types of requests, frequently used functions, and patterns of interaction with various interface elements. Using classification and clustering techniques, systems can automatically identify deviations from normal behaviour, thus preventing fraud or unauthorised access. Neural networks, decision tree-based models and support vector methods (SVM) are often used to implement such algorithms, which can be trained on large amounts of data and provide real-time accuracy.

Biometric authentication methods are an important aspect to enhance the security of access to systems [Sarkar & Singh 2020]. Current methods include facial recognition, fingerprint recognition, iris recognition, and voice analysis. The use of biometrics using AI algorithms such as convolutional neural networks (CNNs) significantly improve the recognition accuracy, making this approach less vulnerable to forgery [Dai et al. 2025]. For instance, facial recognition systems can analyse tens of thousands of points on a face, creating a unique "biometric profile" of each user. Importantly, such systems should provide a high level of security, using encryption methods to store biometric data, and should also provide the capability to update it regularly.

Encryption is a critical element in ensuring data security in AI systems, especially when processing sensitive information [Dufeniuk 2025]. There are two main types of encryption: symmetric and asymmetric. Symmetric encryption uses the same key to encrypt and decrypt data. This method provides fast encryption, but its security depends on keeping the key confidential. In the context of AI systems, where large amounts of data can be processed in real time, symmetric encryption is useful for fast and efficient information transfer, but requires secure key management.

Asymmetric encryption uses a pair of keys: one for encryption (public key) and one for decryption (private key). This provides greater security because the private key is never transmitted. In AI systems, asymmetric encryption is widely used to protect communications and provide authentication, as it allows for data confidentiality and integrity without the need to exchange secret keys [Issayeva et al. 2024].

Advanced approaches to MFA using AI include a combination of multiple layers of security, making unauthorised access much more difficult. The key components of MFA are something the user knows (a password), something they have (such as a mobile device or token), and something related to their unique biometric data. The use of AI in these systems allows contextual data such as the user's location, access time and behaviour in the system to be analysed to make decisions about access levels in real-time. In addition, AI can predict the risk of hacking based on analysing these factors and suggest additional security measures if necessary. These mechanisms can not only strengthen data protection during AI training but also make systems more adaptive, which will provide a high degree of security and reduce the likelihood of unauthorised access.

Examples of the use of AI in authentication systems include face recognition and user behaviour analysis [Trifkovic et al. 2017]. Face recognition uses AI to analyse facial characteristics (e.g., distance between eyes, shape of nose and angle of mouth) and compare them with pre-stored data to identify the user [Olabanji et al. 2024]. This method is convenient as users do not need to remember passwords, though it still requires physical devices such as cameras or sensors for access. Modern face recognition algorithms provide high accuracy and can work even in low light or with minimal distortion. For instance, large companies and government agencies are already implementing facial recognition systems to ensure employee safety and prevent unauthorised access to office space or server rooms. In airports, such systems are used to speed up passenger screening on flights.

User behaviour analysis, in addition to traditional authentication methods, can utilize AI to automatically verify users' identities as they work. The system tracks and analyses daily user behaviour, such as the time and place of login, what actions are performed, and what access type is used. This approach provides the ability to continuously verify users in real-time, reducing the risk of unauthorised access. For instance, if the system notices that a user is working at an unusual time or from a new device, it can request additional authentication or restrict access to sensitive data. In addition, in systems with MFA, AI improves the verification process by integrating multiple factors such as biometrics, one-time passwords and behavioural analysis. The system can use neural networks to analyse real-time data on user actions and combine this with other authentication methods for enhanced security. This combination of authentication factors can significantly improve security. Large companies are already implementing MFA to protect corporate resources, combining traditional methods such as passwords and tokens with AI elements such as biometrics and behavioural analysis.

3.2. Applications of AI in access control systems

AI in access control systems provides a higher level of security compared to traditional methods [Hashmi et al. 2024]. Machine learning, user behaviour analysis and neural networks not only improve authentication accuracy but also prevent potential threats through deeper analysis and prediction of anomalies. Such approaches as facial recognition, user behaviour analysis and MFA with AI elements are actively implemented in modern systems, improving the protection of corporate data.

Integration of AI into MFA systems has several significant advantages. Firstly, it can significantly improve the accuracy and security of the system. AI can improve the recognition of biometric data such as faces, fingerprints and irises, making it more difficult to fake these characteristics. Secondly, analysing user behaviour also helps to create a unique "digital fingerprint" of the individual, which covers parameters such as typing speed, mouse movement or interaction with the device. The use of MFA factors (biometrics, behaviour, devices) in combination further enhances security by reducing the likelihood of unauthorised access.

AI is capable of dynamic adaptation to changes and new threats. The system can learn from past incidents, improving authentication methods in real-time [Arif et al. 2024]. This approach also improves the responsiveness to threats by analysing large amounts of data and identifying unusual patterns such as changes in the user's usual behaviour. This makes the system more flexible and adaptive. At the same time, the use of AI can simplify authentication processes for users, reducing the need for frequent password entry and improving the user experience. Instead, more convenient and secure methods such as facial recognition or behavioural analysis can be used, reducing reliance on traditional passwords.

Despite these advantages, there are also certain risks. There is the potential for recognition errors or false positives, where the system may misidentify a user or an intruder. In addition, the use of AI can create vulnerabilities if insecure algorithms or imperfect models are used, which can be exploited by attackers to circumvent the system. Privacy breaches associated with storing and analysing biometric information can also pose a threat if such data ends up in the hands of third parties. In addition, AI systems can be subjected to attacks aimed at manipulating their learning, which can affect their performance. Ethical issues surrounding the use of biometrics and behavioural analytics also require attention, as such technologies may raise concerns about the invasion of user privacy.

Continuous improvement and adaptation of security systems using AI is possible due to the process of model learning, which allows the system to continuously improve its algorithms and increase authentication accuracy. AI systems can monitor user behaviour in real time, detecting deviations and reacting promptly to them, which reduces security risks [Borisova et al. 2020]. Regular updates to models and algorithms help the system adapt to new threats and attack methods. AI can also be integrated into other security systems, such as distributed denial of service (DDoS) protection and firewalls, to create comprehensive protection for users and organisations.

Continuous learning and adaptation are critical features for AI-based access control systems to effectively respond to evolving security threats. These systems need to automatically incorporate new threat data to stay ahead of emerging vulnerabilities. One of the primary mechanisms for continuous learning involves the use of online learning algorithms, which allow the system to learn from new data in real-time without the need for retraining the entire model. This ensures that the system can adjust to new patterns of user behavior, identify novel attack vectors, and enhance its detection capabilities over time.

AI-based systems can automatically incorporate new threat data through incremental learning. In this approach, the system updates its model by integrating new data points as they become available. For example, when a new type of phishing attack is detected, the system can automatically adjust its detection model by incorporating these new attack signatures, ensuring that the system's knowledge remains up-to-date. This can be done by using algorithms that focus on anomaly detection, continuously monitoring the behavior of users and adapting the model based on deviations from expected patterns. This allows the system to quickly adapt to unforeseen threats, improving its responsiveness without the need for manual intervention [Zianko & Nechyporenko 2023].

To implement these adaptive mechanisms without disrupting ongoing security operations, one practical approach is model versioning. Instead of retraining the entire model, which may be computationally expensive and risk downtime, the system can operate with multiple model versions. The new model is first tested on a subset of data or in a simulated environment to evaluate its performance before being fully integrated into the live system. If the updated model performs better or provides more accurate predictions, it can then be rolled out without disrupting the current security operations. Another important aspect of continuous learning is differential privacy, which ensures that the new data used for training does not compromise user privacy or violate regulatory standards. This allows the system to gather insights from user behavior data while keeping personal information confidential, especially in environments where sensitive data is involved. By applying differential privacy, access control systems can continue to learn from real-time data while mitigating the risk of privacy breaches.

Methods for protecting data used for AI training are critical for the privacy and security of personal information [Oseni et al. 2021]. One of the most common methods is data anonymisation, which involves removing or replacing identifying elements of information to make it unreadable to third parties. This allows the data to be used to train models without the risk of exposing personal information. Another important technique is access control, which restricts the use of data to authorised users only, minimising the risk of leaks or unauthorised access. Differential privacy adds random noise to the data, ensuring its privacy and protecting it from backward analysis. This method extracts useful information while maintaining privacy protection. Data encryption is used to protect data at all stages of data processing. Encryption algorithms keep the data secure by making it inaccessible to unauthorised users. Lastly, federated learning is a technique in which data remains on users' devices and model training is done locally. This reduces the risk of data leaks as the information is not transferred to a central repository. Figure 2 illustrates the five main approaches to data protection.

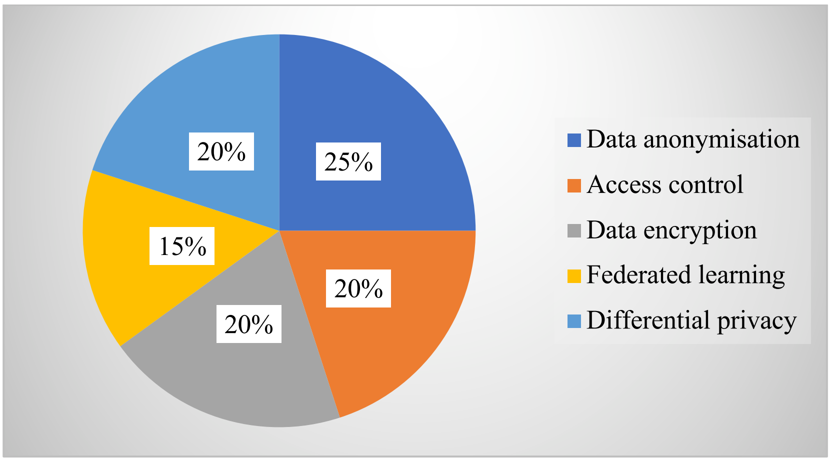

Figure 2: Data protection methods for AI training

Source: compiled by the author based on [Yanamala & Suryadevara 2023].

Nevertheless, privacy concerns remain an important topic when processing data using AI. One of the main concerns is the possibility of data leaks that may occur due to unauthorised access or insufficient security measures. The application of machine learning algorithms can also lead to unintentional disclosure of personal information if the model is trained on sensitive data.

Biometric recognition is an important component for improving authentication accuracy in access control systems. The interaction between biometric recognition and behavioral profiling is that biometric data (e.g., fingerprints, face or iris scans) is used to create an accurate biometric profile of the user that is unique to each individual.

However, to improve security, the system can also use a behavioral profile of the user, which analyzes their usual activity in the system, such as login frequency, types of requests, and functions used. When biometric recognition and behavioral profiling interact, the system can use behavioral deviations as additional indicators to detect anomalous behavior, such as when a user attempts to log in at an unusual time or from a different device. If such deviations are detected, the system can request additional authentication or block access, thereby increasing the level of security.

As for blockchain auditing and federated learning, these two methods can also work together to provide a higher level of protection for the data used to train AI models. Blockchain auditing provides the ability to track all transactions and access to data stored in the system. Each access or change to the data is recorded in the blockchain, creating a reliable and immutable audit trail. Interaction with federated learning avoids the need to transfer data to a central server for model training. Instead, the model is trained locally on each user's device, while maintaining data confidentiality. Once the model is trained locally, only the updated model parameters are transferred to the central server. This reduces the risk of data leaks, as the confidential information itself does not leave the user's device. Blockchain auditing interacts with federated learning, ensuring that all changes to model parameters are recorded, creating a transparent and secure system where every stage of data processing and model training can be tracked and verified.

The integration of blockchain technology with AI can significantly enhance the security and transparency of access control systems. Blockchain provides a decentralized and immutable ledger, which ensures that all access transactions are securely recorded and cannot be tampered with. When combined with AI, blockchain can provide an extra layer of trust by verifying that the data being processed or accessed is legitimate and hasn't been altered.

For instance, AI can be used to analyze user behavior in real time, detecting anomalies or unauthorized access attempts. Meanwhile, blockchain can record every access event in a secure, transparent, and verifiable manner. This creates an auditable trail of user interactions, making it easier to track access patterns and quickly identify any suspicious activities. Moreover, blockchain's decentralized nature can help address some of the vulnerabilities in centralized systems, such as single points of failure. By using blockchain, the access control system can ensure that even if one part of the system is compromised, the integrity of access records is maintained.

In terms of transparency, blockchain enables all stakeholders to have access to a consistent and tamper-proof record of access control activities. This is particularly important in organizations that need to comply with regulatory standards, as it makes it easier to provide proof of compliance. Blockchain's smart contract functionality can be used in conjunction with AI to automate and enforce security policies. For example, a smart contract can be set up to automatically adjust access permissions based on certain conditions detected by AI, such as changes in user behavior or the identification of potential security threats.

The issue of "peripheral disclosure" is that anonymised data can be combined with other sources to recover personal data [Zhang et al. 2022]. Peripheral disclosure refers to the risk that anonymized data, when combined with other publicly available or seemingly unrelated data sources, can be re-identified, revealing personal information. Even if data is anonymized, the integration with other datasets may expose individuals' identities or sensitive details, undermining the intended privacy protections. These risks require strict security and ethical protocols. Integration of AI into corporate infrastructure requires meticulous planning, compatibility with existing systems, and employee training. It is also essential to secure data at all levels, from storage to transmission. The use of encryption, access control and activity monitoring will help prevent leaks and protect against threats. Organisations must develop ethical guidelines and comply with privacy standards, such as [GDPR 2016], to mitigate risks and increase trust from customers and partners.

Examples of successful integration of AI-based solutions into corporate security systems can be found in various industries [Younus et al. 2024]. In the financial sector, for instance, AI is actively used for fraud prevention. Machine learning algorithms analyse large amounts of data in real-time, identifying suspicious transactions and preventing fraudulent activities. In healthcare, AI is being used to control access to medical records, providing secure and efficient access to data based on biometric identification or behavioural analysis. In retail, AI helps prevent theft and fraud by analysing shopping habits and customer behaviour in-store or online [Mohajer et al. 2025].

Evaluation of the effectiveness of AI in access control systems involves measuring several key metrics. These may include how quickly the system reacts to changes in user behaviour, the number of false positives and the number of incidents successfully prevented. Effectiveness is also determined by the level of adaptability of the system: how capable it is of detecting anomalies, even if they fall outside of predetermined patterns. For instance, in some cases, AI systems can detect unauthorised access attempts by analysing user behaviour, not just static factors such as passwords or access keys. It is also necessary to assess how an AI system interacts with other security systems and how it improves the security processes of the organisation.

In addition, the impact of AI on reducing security risks and costs must be factored in to fully assess its effectiveness. For instance, AI systems can automate many of the processes associated with monitoring and verifying access, which reduces the burden on staff, speeds up response to threats and minimises human error. This in turn improves the overall security effectiveness of the company, reducing the likelihood of data breaches or unauthorised access.

3.3. Strategies for integration and data protection in AI-enhanced access control

Based on the assessment of the effectiveness of AI in access control systems, several recommendations can be made to improve the operation of these systems and increase security.To improve access control mechanisms using AI, it is recommended that systems based on machine learning be implemented to analyse user behaviour and detect anomalies. Such systems can adapt to changes in employee behaviour, enabling effective detection of unusual actions that may indicate unauthorised access attempts. This enhances the security of corporate data because AI systems not only use pre-defined rules but also learn new behaviours, effectively identifying threats that fall outside of normal scenarios. Importantly, the system should be able to collect and analyse data on user actions such as login time, query frequency and location to help identify deviations and block unwanted actions in a timely manner.

Cognitive biases such as automation bias, alert fatigue, and overconfidence can significantly influence the response of security personnel to AI-generated alerts. Automation bias occurs when personnel rely too heavily on automated systems, often ignoring warning signs or failing to verify alerts generated by AI. This can lead to critical security threats being overlooked, as the automated system is trusted over human judgment. Alert fatigue happens when security personnel are overwhelmed by a high volume of alerts, causing them to become desensitized and potentially overlook or dismiss genuine threats. This reduces the effectiveness of alert systems and can lead to delayed responses to critical incidents. Overconfidence refers to the belief that the security system is infallible, leading to complacency in monitoring and response. Security personnel may underestimate the risks or overestimate the system's ability to detect threats, which can result in inadequate responses. These biases highlight the importance of training, system design, and human-computer interaction to mitigate their negative impacts and ensure effective security operations [Andrukhov et al. 2024].

To create more secure and flexible access control mechanisms, it is recommended to integrate AI with MFA. It is important to combine traditional authentication methods, such as passwords and biometrics, with AI-based solutions, which will significantly increase the level of data protection. MFA, combined with user behaviour analysis, will create a multi-layered security system that will not only protect data from external threats but will also effectively detect anomalies in employee behaviour, minimising the risks of unauthorised access.

Regular updates and training of AI algorithms are essential to ensure their sustainability and effectiveness. Algorithms must be regularly updated based on new data to respond quickly to new threats. The more relevant and diverse the data on which AI models are trained, the more accurately the system will be able to predict and prevent potential incidents. For instance, AI models can be trained on fresh data about new types of attacks, changes in employee workflows, and new vulnerability exploitation patterns. Regular algorithm updates improve the accuracy of the system and allow it to adapt to constantly changing conditions.

The AI-based corporate data protection model includes several key components, each of which is substantial in ensuring security (Table 1).

No.	Stage	Components
1.	Defining the requirements and goals of the system	• Task description: Define the objectives of the data protection model, including leakage prevention, threat detection, response automation and risk mitigation. • Infrastructure analysis: Conduct an audit of the existing corporate infrastructure, including servers, databases, cloud storage, networks and applications in use. • Identification of risks: Identify the main threats (phishing, DDoS attacks, data leaks) and determine critical resources. • Technical requirements: Set requirements for hardware, AI algorithm performance, data processing speed, and integration with existing systems.

2.	Development of an access control system (first component)	• MFA: Implement the use of biometric data (face recognition, fingerprints) and security tokens. • Behaviour analysis: Implement machine learning algorithms to build user profiles. For instance, track the frequency of logins, devices used, geolocation, and time of activity. • Adaptive access control: Use contextual data (e.g., time of day or user role) to dynamically configure access rights.
3.	Creating a data monitoring and analysis module (second component)	• Implementation of monitoring: Configure data collection from logs, network traffic, database queries, and user activity. • Anomaly analysis: Apply clustering methods (e.g., K-means) and neural networks to identify deviations from normal behaviour. • Real-time implementation: Set up real-time data processing using streaming platforms such as Apache Kafka or Apache Flink.
4.	Development of an intelligent incident response system (third component)	• Automation of response: Create scripts to automatically block suspicious activity (for example, blocking IP addresses or isolating compromised devices). • Attack simulation: Implement a tool for simulating attacks to test the system. • The use of AI algorithms: Introduce learning from historical data to predict the impact of attacks and optimise response strategies.
5.	Development of a risk management module (fourth component)	• Risk forecasting: Use predictive analytics to assess the likelihood of incidents. • Vulnerability assessment: Integrate data from a vulnerability database (e.g., CVE) to analyse system weaknesses. • Development of recommendations: Continuously update recommendations for improving security based on new data.
6.	Integration of blockchain technologies (additional component)	• Storage of access data: Configure the use of the blockchain to record all access transactions, ensuring their immutability. • Transparency: Ensure that data is available for audit. • Security: Use decentralised storage to protect data from modification.
7.	Testing and implementation	• Conducting tests: Test the model on real data to verify the effectiveness of threat detection and adaptability.

		• Result analysis: Evaluate system performance, false alarm rate and response time. • Integration with infrastructure: Configure the model for integration into the existing systems.
8.	Personnel training and operation	• Employee training: Conduct trainings for information security specialists and system users. • Monitoring: Set up regular monitoring of model performance and algorithm updates. • System update: Introduce new versions of algorithms based on the analysis of new threats and incidents.
9.	Performance evaluation and improvement	• Metrics: Use key performance indicators (e.g., response time, number of incidents prevented). • Adaptation: Continuously adapt the model to changing threats and infrastructure.

Table 1: Stages of developing a corporate data protection model based on AI

Source: compiled by the author

To effectively implement an AI-based corporate data protection model, several key components are necessary to ensure a comprehensive security framework. These components are designed to address various aspects of data protection, including threat detection, response automation, risk mitigation, and infrastructure analysis. The following table outlines the stages and components involved in developing and implementing such a model, detailing the necessary steps for each phase to achieve optimal security and adaptability. Table 1 provides a structured overview of these stages, highlighting the critical components required for a successful AI-driven data protection system.

Risk forecasting in a data protection system involves the use of machine learning methods and data analytics to assess the likelihood of security incidents based on historical data. Risk forecasting is based on the analysis of characteristics such as attack types (e.g., phishing, DDoS), user behavior, and infrastructure status. This allows the model to assess the likelihood that a particular event (such as an unauthorized access attempt) might occur in the future. Risk forecasting includes the use of predictive models trained on historical data and enables the system to detect potential threats before they arise [Smetaniuk & Tsisar 2024].

User profile deviation involves comparing the current behavior of a user with their typical profile, which helps detect anomalies. The user profile consists of various behavioral characteristics, such as login time, devices used, location, login frequency, and the types of queries they typically make. When a user's current activity deviates from their usual profile, the system identifies such behavior as suspicious. This process helps detect potentially unauthorized actions, for example, when a user logs into the system from a new device or at an unusual time [Podorozhnyuk & Lialiuk 2024].

Anomaly detection thresholds are defined to identify deviations from normal user behavior or typical system patterns. These thresholds can be adaptive, meaning they change depending on conditions such as new types of threats or changes in user behavior. For each type of anomaly (e.g., logging in at an unusual time or from a suspicious location), a specific threshold is set that indicates the level of deviation at which the system should initiate additional checks or restrict access. The thresholds are determined based on the analysis of user behavior data, allowing the system to respond more accurately to new or unusual threats.

To successfully implement AI in an access control system, it is also important to invest in employee training and conduct regular technology testing. Employees should be trained in the proper use of AI systems and how to respond to emerging threats. This will not only help improve the efficiency of the system but also minimise the risks associated with the human factor. Regular testing and audits of the system will help identify weaknesses in AI, improve the accuracy of threat detection and ensure a high level of user confidence in the security system.

A SWOT analysis of traditional access control methods and the integration of AI into these systems revealed strengths, weaknesses, opportunities, and threats to corporate data security. Let's look at the results of this analysis with a methodological structure and quantitative results that confirm the conclusions. Traditional access control methods, such as passwords, biometrics, and MFA, have certain advantages. Passwords are the most common method, providing access at low cost, but their security is inadequate due to their vulnerability to hacking and phishing. Biometric methods provide a high level of security due to the unique characteristics of the individual, which reduces the likelihood of abuse. However, as the analysis results show, high cost and accuracy issues remain significant drawbacks of biometrics.

The weaknesses of traditional access control methods lie in vulnerabilities such as password leaks and phishing attacks, which can lead to serious consequences, including financial losses and leaks of sensitive information. Infrastructure attacks pose a serious threat because they can allow attackers to bypass traditional access control systems, increasing the risks for organizations. The study found that traditional methods are not always able to respond effectively to new threats and changing conditions. The integration of AI into access control systems significantly increases security. AI enables the effective analysis and processing of large amounts of data to detect anomalies and threats, improving authentication accuracy and preventing potential threats. The use of machine learning, user behavior analysis, and neural networks allows systems to adapt to new threats and changes in user behavior, making them more flexible and effective. The proposed recommendations for integrating machine learning for user behavior analysis and combining AI with traditional authentication methods can significantly improve security.

There are certain threats associated with the use of AI, in particular the possibility of data privacy and security breaches due to improper storage or processing of biometric data. The use of machine learning can lead to unauthorized disclosure of personal information if the model is trained on sensitive data. In addition, there is a risk of manipulation of AI algorithms, which can negatively affect the performance and accuracy of the system. Using blockchain auditing to track transactions and ensure transparency in data processing is an important step in mitigating these threats.

The study evaluated the effectiveness of AI in access control systems across several metrics, including response speed to changes in user behavior, number of false positives, and number of successfully prevented incidents. The results showed that AI integration can significantly improve system adaptability, reducing the number of false positives and increasing the accuracy of anomaly detection. In further research, it is important to focus on developing new AI algorithms to improve authentication accuracy and speed, as well as reduce the number of false positives. Studying methods of analyzing user behavior to detect anomalies and creating adaptive access control systems are important areas for future research.

4 Discussion

The shortcomings of traditional access control methods such as passwords, biometrics and MFA need to be discussed in depth. Passwords remain one of the most common authentication methods, but there are many challenges associated with their use. Often users choose simple passwords that are easy to crack. Even complex passwords can be stolen in data breaches, compromising account security. In addition, users often use the same password on different resources, which exacerbates the situation: compromise of one service can lead to data leaks on other platforms.

The sources provided discuss various applications of AI in access control systems, particularly focusing on its role in enhancing security, detecting malicious activities, and improving authentication and authorization processes. [Mayeke et al. 2024] provide an extensive multi-dimensional analysis of evolving access control strategies within the cybersecurity field, addressing security risks and system assurance in cyber engineering. Although AI is not the central focus, the study underscores the importance of advanced technologies, like AI, to manage the complexities of modern security threats. It outlines how AI can be integrated into access control systems to enhance threat detection and effectively mitigate risks by adapting to the dynamic nature of cybersecurity challenges.

[Bera et al. 2021] explore an AI-driven, blockchain-based access control system for detecting and mitigating malicious activities in the Internet of Everything (IoE). The research highlights how AI can be effectively applied for real-time anomaly detection and monitoring in IoE environments, combining AI and blockchain to provide strong security and integrity. This approach demonstrates the power of AI in strengthening access control by automating threat detection and improving the system's response to potential security breaches. [Olabanji et al. 2024] investigates the application of AI in enhancing identity and access management (IAM) within cloud-based systems. The study explores how AI can optimize user authentication, authorization, and access control in cloud environments. Through the use of AI for intelligent identity verification and automated decision-making processes, the research highlights AI's potential to streamline and fortify cloud infrastructure access control, making it more adaptive and efficient in managing access rights and ensuring secure operations.

[Omotunde & Ahmed 2023] delve into the various security measures applied in database systems, particularly focusing on authentication and access control. While it does not focus primarily on AI, it touches upon how AI can enhance traditional access control systems. The paper acknowledges AI's role in automating authentication processes, improving the precision of access control, and detecting anomalies, although AI's application is not the main subject of the study.

Biometric data, such as fingerprints or iris, offer a high degree of security but have their limitations [Rexhepi et al. 2023]. If they are compromised, they cannot be replaced, posing serious risks. Some technologies allow biometrics to be tampered with, further reducing the level of protection. In addition, the collection and storage of biometric information raises questions about confidentiality and the potential for misuse. The study [A. Mohajer et al. 2025] examines the use of adaptive strategies such as TD3 (Twin Delayed Deep Deterministic Policy Gradient) for shipment optimization and adaptive network management in mobile computing. This includes load distribution based on observed network conditions, which improves accuracy and adaptability in resource optimization decisions. In the context of authentication, similar adaptive approaches can be used to determine user trust levels and adapt security levels based on user behavior or changing network conditions.

Compared to other works analyzing adaptive authentication solutions, such as machine learning methods for analyzing user behavior, TD3 strategies may be more effective for dynamic and scalable systems where conditions change rapidly (e.g., changes in mobile networks or mobile environments). AI-based strategies, such as deep neural networks or user behavior analysis, are typically focused on more static parameters and may require regular updates to ensure real-time adaptability. The research [A. Mohajer et al. 2025] proposes an innovative approach that combines traffic-aware network slicing with adaptive strategies to improve processing in mobile networks. This allows for better efficiency, as load distribution is performed based on actual changing network conditions. Compared to other systems that use a static or predefined approach to authentication, adaptive strategies can reduce false positives and improve efficiency by dynamically adjusting authentication parameters. [Arora & Bhatia 2022] also emphasised the existence of technologies that allow for the forgery of biometric data. This confirms the assertion that the level of protection can be reduced if attackers use modern methods to bypass biometric systems.

MFA is considered a more secure method, as it requires confirmation through several factors, such as a combination of password and SMS code [Yevseiev et al. 2021]. However, this system has disadvantages. Users may be inconvenienced by having to go through MFA steps, which can sometimes cause delays and negative emotions. Moreover, losing access to secondary authentication methods, such as a mobile phone, can be a serious problem, making it impossible to access an account.

[Henricks & Kettani 2019] also noted that MFA steps can create delays and negative experiences, which confirms the results of this analysis. This indicates the importance of considering user experience when designing and implementing MFA systems. Although highly secure, redundant authentication steps can lead to user frustration, which in turn can reduce security compliance.

Traditional authentication methods such as passwords and biometrics face serious threats, including password leaks and phishing. Leaks allow attackers to gain access to accounts, while phishing manipulates users into revealing sensitive information. This emphasises the need for modern solutions that can provide a higher level of security. The introduction of AI significantly improves security by enabling the analysis of large amounts of data to identify anomalies and threats [Mazur & Flogaitis 2023]. The use of machine learning and user behaviour analysis helps to detect suspicious activity, allowing the system to respond automatically, for example by blocking access or requesting additional confirmation. Neural networks enable the creation of dynamic user profiles that adapt to changes in user behaviour. Real-time analysis of these profiles prevents unauthorised access and minimises inconvenience to users. In this way, AI makes authentication more accurate and adaptive, improving overall security.

The findings coincide with [Nadeem et al. 2023], who in their study notes that traditional measures such as passwords are insufficient to protect against such attacks, which emphasises the importance of more modern technologies to prevent phishing. [Dai & Boroomand 2022] emphasised that AI, neural networks and real-time analysis can significantly improve the accuracy and adaptability of security in big data systems. Technologies such as machine learning and neural networks can more effectively detect and prevent threats such as phishing and provide better security, as this study confirms.

AI-assisted user behaviour analysis is a powerful tool for improving security by identifying behavioural anomalies that may indicate unauthorised access attempts. This method proactively responds to potential threats, which significantly improves the protection of systems compared to traditional methods such as passwords or MFA. However, using AI for behavioural analysis is not without its drawbacks. There is a risk of false positives, where the system may misinterpret a user's actions as suspicious, which can cause inconvenience and even block legitimate access. In addition, the processing of large amounts of personal data requires special attention to privacy and data protection issues. Leakage or misuse of data can lead to serious consequences, such as violation of users' rights or privacy. The implementation of such technologies requires adherence to strict ethical standards to balance security and user rights. Thus, the process of integrating AI into security systems must be carefully considered, addressing not only the technical aspects but also the possible social and ethical implications.

[Shaik et al. 2022] also noted that the use of AI to analyse deviations from normal behaviour allows real-time adaptation of security systems, which significantly increases the accuracy and proactivity of protection. Furthermore, the author emphasised the risks associated with false positives and possible data leakage, which confirms the importance of ethical standards and privacy protection in such systems. This points to the need for a comprehensive approach to integrating AI into access control systems, recognising both its benefits and potential risks.

Identified data protection methods such as anonymisation, access control, differential privacy and encryption are substantial in ensuring the security and confidentiality of personal information. Anonymisation can be used to hide identifying data but remains vulnerable to de-anonymisation methods, which require additional protection measures. Access control, which limits the range of users who have access to data, is effective, but it needs to be regularly reviewed and updated to prevent insider threats. Differential privacy is becoming an important tool, especially in the context of working with big data, as it allows for analysis while minimising the risk of leakage but requires careful configuration to balance data utility with privacy protection. Data encryption protects information during storage and transmission, but the complexity of managing cryptographic keys remains one of the challenges of this method [Petrova et al. 2018].

The results of the study are consistent with the findings of [Vasa & Thakkar 2022], who highlighted the importance of differential privacy for data protection in big data environments. The author indicated that this method allows privacy in analysing large data sets, which confirms its effectiveness in improving security. Similarly, [Pratomo et al. 2023] highlighted the importance of encryption and anonymisation as key tools for enhancing information security, preventing leaks and preserving privacy, which is consistent with the findings of this study.

When analysing the use of AI in access control systems, metrics such as responsiveness to changes in user behaviour, as well as effectiveness in detecting threats and preventing incidents, should be considered. These metrics are essential to understanding the success of AI technology adoption and its impact on corporate data security. While there are obvious benefits such as adaptability and the ability to predict threats, risks associated with potential AI errors, false positives, and ethical issues related to data privacy must be considered. A comprehensive strategy that combines traditional security methods with AI can significantly improve protection, creating more flexible and effective security mechanisms.

The results of this analysis are in line with the conclusions presented by [Mayeke et al. 2024], who emphasises the importance of assessing the effectiveness of access control systems and applying key metrics to evaluate their performance. This indicates a consensus that combined strategies that include both traditional methods and modern AI technologies can improve the level of security and reliability of corporate data systems.

5 Conclusions

The study determined that traditional access control methods, such as passwords, biometrics and multi-factor authentication, have their advantages and disadvantages. Passwords are the most common method, but their security is inadequate, as they are susceptible to hacking and phishing. Biometric methods provide a higher level of security but have problems with accuracy and implementation costs. Multi-factor authentication combines different methods to significantly increase security but can be inconvenient for users.

The study identified important vulnerabilities in traditional access control systems, such as password leaks and phishing attacks, which can lead to serious consequences, including financial loss and leakage of sensitive information. Infrastructure attacks also pose a serious threat, as they can allow attackers to bypass traditional access control mechanisms. The research emphasised that the integration of artificial intelligence into access control systems significantly improves security by enabling efficient analysis and processing of large amounts of data to identify anomalies and threats. The use of machine learning, user behaviour analysis, and neural networks can improve authentication accuracy and prevent potential threats. Artificial intelligence can adapt to changes and new threats, making systems more flexible and efficient.

The study also examined data protection techniques used for artificial intelligence training such as anonymisation, access control, differential privacy, encryption and federated learning. All these methods aim to ensure the privacy and security of personal information. Also, based on the results of the study, recommendations have been developed to improve the security of artificial intelligence-enabled access control systems. Recommendations have been proposed for integrating machine learning to analyse user behaviour, combining artificial intelligence with traditional authentication methods, and implementing clear security standards and policies.

Assessment of the effectiveness of artificial intelligence in access control systems includes measuring the speed of response to changes in user behaviour, the number of false positives and the number of successful incidents prevented. It is also important to consider the impact of artificial intelligence in reducing security risks and costs, as well as its ability to automate access monitoring and verification processes, which improves the overall effectiveness of the security system.

Further research in this area could include the development of new artificial intelligence algorithms to improve the accuracy and speed of authentication, as well as reduce the number of false positives. It is also worth exploring methods of analysing user behaviour to detect anomalies and create adaptive access control systems. An important area will be the study of the integration of artificial intelligence and blockchain technologies to improve security and transparency. However, this study is limited to the analysis of existing methods and technologies, not covering the deeper implementation of artificial intelligence in real corporate infrastructures, which requires additional experiments and research in practical application.

References

[Abdulrahman & Alhayani 2023] Abdulrahman, S., & Alhayani, B. (2023):“A comprehensive survey on the biometric systems based on physiological and behavioural characteristics”; Materials Today: Proceedings, 80(3), 2642-2646.

[Andrukhov et al. 2024] Andrukhov, V., Potiekha, A., & Tarapkin, P. (2024): “Analysis of methods of search, extraction and data processing in the Autodesk Revit system”; Modern Technology, Materials and Design in Construction, 36(1), 166-172.

[Arif et al. 2024] Arif, H., Kumar, A., Fahad, M., & Hussain, H. (2024): “Future horizons: AI-enhanced threat detection in cloud environments: Unveiling opportunities for research”; International Journal of Multidisciplinary Sciences and Arts, 3(1), 242-251.

[Arora & Bhatia 2022] Arora, S., & Bhatia, M. (2022): “Challenges and opportunities in biometric security: A survey”; Information Security Journal: A Global Perspective, 31(1), 28-48.

[Attkan & Ranga 2022] Attkan, A., & Ranga, V. (2022): “Cyber-physical security for IoT networks: A comprehensive review on traditional, blockchain and artificial intelligence based key-security”; Complex & Intelligent Systems, 8(4), 3559-3591.

[Aviv et al. 2024] Aviv, I., Svetinovic, D., & Lee, S.-W. (2024): “Requirements Engineering for Web3 Systems: Preface”; In Proceedings - 32nd IEEE International Requirements Engineering Conference Workshops, REW 2024 (pp. 326-327). Institute of Electrical and Electronics Engineers.

[Bera et al. 2021] Bera, B., Das, A. K., Obaidat, M. S., Vijayakumar, P., Hsiao, K. F., & Park, Y. (2021): “AI-enabled blockchain-based access control for malicious attacks detection and mitigation in IoE”; IEEE Consumer Electronics Magazine, 10(5), 82-92.

[Borisova et al. 2020] Borisova, A., Rakhimberdinova, M., Madiyarova, E., Riazantseva, I., & Mikidenko, N. (2020): “Staffing search and recruitment of personnel on the basis of artificial intelligience technologies”; Entrepreneurship and Sustainability Issues, 7(3), 2456-2469.

[Dai & Boroomand 2022] Dai, D., & Boroomand, S. (2022): "A review of artificial intelligence to enhance the security of big data systems: state-of-art, methodologies, applications, and challenges"; Archives of Computational Methods in Engineering, 29(2), 1291-1309.

[Dai et al. 2025] Dai, Z. C., Tan, M., Yang, Y., Liu, X., Wang, R., & Su, Y. X. (2025): "Massive Coordination of Distributed Energy Resources in VPP: A Mean Field RL-Based Bi-Level Optimization Approach"; In P. Shi (Eds.), IEEE Transactions on Cybernetics (pp. 1332-1346). IEEE.

[Dufeniuk 2025] Dufeniuk, O. (2025): "Digital databases of court decisions in criminal proceedings: Value, risks, and use optimisation"; Social and Legal Studios, 8(1), 10-19.

[GDPR 2016] "General Data Protection Regulation (GDPR)" (2016); https://gdpr-info.eu/

[Hasal et al. 2021] Hasal, M., Nowaková, J., Ahmed Saghair, K., Abdulla, H., Snášel, V., & Ogiela, L. (2021): "Chatbots: Security, privacy, data protection, and social aspects"; Concurrency and Computation: Practice and Experience, 33(19), e6426.

[Hashmi et al. 2024] Hashmi, E., Yamin, M., & Yayilgan, S. (2024): "Securing tomorrow: A comprehensive survey on the synergy of artificial intelligence and information security"; AI and Ethics. https://doi.org/10.1007/s43681-024-00529-z

[Henricks & Kettani 2019] Henricks, A., & Kettani, H. (2019): "On data protection using multi-factor authentication." In Proceedings of the 2019 International Conference on Information System and System Management (pp. 1-4). Association for Computing Machinery.

[Humayun et al. 2024] Humayun, M., Tariq, N., Alfayad, M., Zakwan, M., Alwakid, G., & Assiri, M. (2024): "Securing the Internet of Things in artificial intelligence era: A comprehensive survey"; IEEE Access, 12, 25469-25490.

[Issayeva et al. 2024] Issayeva, A., Niyazbekova, S., Semenov, A., Kerimkhulle, S., & Sayimova, M. (2024): "Digital technologies and the integration of a green economy: legal peculiarities and electronic transactions"; Reliability Theory and Applications, 19(6), 1088-1096.

[Jurkevičius & Pleskach 2025] Jurkevičius, V., & Pleskach, M. (2025): "The concept of digital human rights: The search for new justification approaches from a comparative perspective"; Social and Legal Studios, 8(1), 155-164.

[Kravchuk et al. 2024] Kravchuk, M., Kravchuk, V., Hrubinko, A., Podkovenko, T., & Ukhach, V. (2024): "Cyber security in Ukraine: Theoretical view and legal regulation"; Law, Policy and Security, 2(2), 28-38.

[Martín et al. 2021] Martín, A., Fernández-Isabel, A., Martín de Diego, I., & Beltrán, M. (2021): "A survey for user behavior analysis based on machine learning techniques: Current models and applications"; Applied Intelligence, 51(8), 6029-6055.

[Mayeke et al. 2024] Mayeke, N., Arigbabu, A., Olaniyi, O., Okunleye, O., & Adigwe, C. (2024): "Evolving access control paradigms: A comprehensive multi-dimensional analysis of security risks and system assurance in cyber engineering"; Asian Journal of Research in Computer Science, 17(5), 108-124.

[Mazur & Flogaitis 2023] Mazur, T., & Flogaitis, S. (2023): "Electronic parliament as a factor of sustainable development: History and prospects"; Law Journal of the National Academy of Internal Affairs, 13(2), 19-29.

[Mazur 2023] Mazur, J. (2023): "Artificial Intelligence vs data protection: How the GDPR can help to develop a precautionary regulatory approach to AI?" In A. Kornilakis, G. Nouskalis, V.

Pergantis, & T. Tzimas (Eds.), Artificial Intelligence and Normative Challenges: Law, Governance and Technology Series (pp. 215-233). Springer.

[Metelskyi & Kravchuk 2023] Metelskyi, I., & Kravchuk, M. (2023): "Features of cybercrime and its prevalence in Ukraine"; Law, Policy and Security, 1(1), 18-25.

[Mohajer et al. 2025] Mohajer, A., Hajipour, J., & Leung, V. C. M. (2025): "Dynamic offloading in mobile edge computing with traffic-aware network slicing and adaptive TD3 strategy"; *IEEE Communications Letters*, 29(1), 95-99.

[Mohammed et al. 2023] Mohammed, A., Dziyauddin, R., & Latiff, L. (2023): "Current multi-factor of authentication: Approaches, requirements, attacks and challenges"; International Journal of Advanced Computer Science and Applications, 14(1), 166-178

[Nadeem et al. 2023] Nadeem, M., Zahra, S., Abbasi, M., Arshad, A., Riaz, S., & Ahmed, W. (2023): "Phishing attack, its detections and prevention techniques"; International Journal of Wireless Security and Networks, 1(2), 13-25.

[Neelakrishnan 2024] Neelakrishnan, P. (2024): "AI-driven proactive cloud application data access security"; International Journal of Innovative Science and Research Technology*,* 9(4), 510-521.

[Nti et al. 2022] Nti, I., Quarcoo, J., Aning, J., & Fosu, G. (2022): "A mini-review of machine learning in big data analytics: Applications, challenges, and prospects"; Big Data Mining and Analytics*,* 5(2), 81-97.

[Olabanji et al., 2024] Olabanji, S., Olaniyi, O., Adigwe, C., Okunleye, O., & Oladoyinbo, T. (2024): "AI for identity and access management (IAM) in the cloud: Exploring the potential of artificial intelligence to improve user authentication, authorization, and access control within cloud-based systems"; Asian Journal of Research in Computer Science, 17(3), 38-56.

[Omotunde & Ahmed 2023] Omotunde, H., & Ahmed, M. (2023): "A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond"; Mesopotamian Journal of CyberSecurity*,* 2023, 115-133.

[Oseni et al. 2021] Oseni, A., Moustafa, N., Janicke, H., Liu, P., Tari, Z., & Vasilakos, A. (2021): "Security and privacy for artificial intelligence: Opportunities and challenges"; https://doi.org/10.48550/arXiv.2102.04661

[Patricheev 2025] Patricheev, I. (2025): "Legal paternalism's influence on the balancing data protection and fundamental rights"; Law Journal of the National Academy of Internal Affairs, 15(1), 48-58.

[Peng et al. 2019] Peng, P., Xu, C., Quinn, L., Hu, H., Viswanath, B., & Wang, G. (2019): "What happens after you leak your password: Understanding credential sharing on phishing sites." In Asia CCS'19: Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security (pp. 181-192). Association for Computing Machinery.

[Petrova et al. 2018] Petrova, M. M., Sushchenko, O., Trunina, I., & Dekhtyar, N. (2018): "Big data tools in processing information from open sources"; In 2018 IEEE 1st International Conference on System Analysis and Intelligent Computing, SAIC 2018 - Proceedings (article number: 8516800). Institute of Electrical and Electronics Engineers.

[Podorozhnyuk & Lialiuk 2024] Podorozhnyuk, V., & Lialiuk, O. (2024): "Integration of blockchain and metaverse into modern Web2 internet space and preparation of update to Web3 version"; Modern Technology, Materials and Design in Construction, 36(1), 103-107.

[Pratomo et al. 2023] Pratomo, A., Mokodenseho, S., & Aziz, A. (2023): "Data encryption and anonymization techniques for enhanced information system security and privacy"; West Science Information System and Technology, 1(1), 1-9.

[Rexhepi et al. 2023] Rexhepi, B. R., Kumar, A., Gowtham, M. S., Rajalakshmi, R., Paikaray, M. D., & Adhikari, P. K. (2023): "An Secured Intrusion Detection System Integrated with the Conditional Random Field For the Manet Network"; International Journal of Intelligent Systems and Applications in Engineering, 11(3s), 14-21.

[Saeed et al. 2024] Saeed, M. M., Saeed, R. A., & Ahmed, Z. E. (2024): "Data security and privacy in the age of AI and digital twins." In S. Ponnusamy, M. Assaf, J. Antari, S. Singh, S. Kalyanaraman (Eds.), Digital Twin Technology and AI Implementations in Future-Focused Businesses (pp. 99-124). IGI Global Scientific Publishing.

[Sarkar & Singh 2020] Sarkar, A., & Singh, B. (2020): "A review on performance, security and various biometric template protection schemes for biometric authentication systems"; Multimedia Tools and Applications, 79(37), 27721-27776.

[Shaik et al. 2022] Shaik, I., Chandran, N., & Rajan M. A. (2022): "Privacy and data protection in the enterprise world"; CSI Transactions on ICT, 10(1), 37-45.

[Shaik et al. 2023] Shaik, M., Gudala, L., & Sadhu, A. (2023): "Leveraging artificial intelligence for enhanced identity and access management within zero trust security architectures: A focus on user behavior analytics and adaptive authentication"; Australian Journal of Machine Learning Research & Applications, 3(2), 1-31.

[Smetaniuk & Tsisar 2024] Smetaniuk, O., & Tsisar, D. (2024): "Digital economy as a foundation for creating digital strategies of enterprises"; Innovation and Sustainability, 3, 68-75.

[Trifkovic et al. 2017] Trifkovic, B., Budak, I., Vukelic, D., Puskar, T., Jevremovic, D., Todorovic, A., Todorovic, A., & Postic, S. (2017): "Analysis of accuracy and precision of optical 3D digitisation devices in dental computer-aided-design and computer-aided-manufacturing systems"; Maejo International Journal of Science and Technology, 11(1), 45-57.

[Vasa & Thakkar 2022] Vasa, J., & Thakkar, A. (2022): "Deep learning: Differential privacy preservation in the era of big data"; Journal of Computer Information Systems, 63(3), 608-631.

[Yanamala & Suryadevara 2023] Yanamala, A., & Suryadevara, S. (2023): "Advances in data protection and artificial intelligence: trends and challenges"; International Journal of Advanced Engineering Technologies and Innovations, 1(1), 294-319.

[Yevseiev et al. 2021] Yevseiev, S., Laptiev, O., Lazarenko, S., Korchenko, A., & Manzhul, I. (2021): "Modeling the protection of personal data from trust and the amount of information on social networks"; EUREKA, Physics and Engineering, 2021(1), 24-31.

[Younus et al. 2024] Younus, A., Salih, A., Ahmed, O., Yazdeen, A., Abdullah, R., & Sami, T. (2024): "Web-based and cloud-computing influences on resource utilization optimization for sustainable enterprise systems with AI, IoT, and security".

[Zhang et al. 2022] Zhang, Y., Wu, T., Xian, X., & Xu, Y. (2022): "A brief survey on privacy-preserving methods for graph-structured data"; In J. Yao, Y. Xiao, P. You, G. Sun (Eds.), The International Conference on Image, Vision and Intelligent Systems (pp. 573-583). Springer.

[Zianko & Nechyporenko 2023] Zianko, V., & Nechyporenko, T. (2023): "Artificial intelligence in the financial sector of Ukraine: A driver of development and a factor of modernization"; Innovation and Sustainability, 3, 6-21.

[Zile et al. 2023] Zile, A., Palkova, K., & Vilks, A. (2023): "Study of the Influence of External Conditions and Materials on the Preservation of Hidden Prints under Water"; Pakistan Journal of Criminology, 15(2), 305-322.