# دور الذكاء الاصطناعي في تعزيز الأمن السيبراني من خلال المصادقة المتعددة العوامل (MFA)

The role of artificial intelligence in enhancing cybersecurity through multi-factor authentication (MFA)

إعداد: ديمة أمين غندور

إشراف: د. محمد المحمد

**ملخص:**

هل سألت نفسك يوماً عند فتحك لبعض المواقع الإلكترونية ماذا يعني "أثبت أنك لست روبوت" أو "التحقق من أنك إنسان!"، او حاولت الدخول والتسجيل في موقع ويب او التسجيل في أحد تطبيقات التواصل الاجتماعي او حاولت إجراء تحويل مالي وطلب منك ادخال كود مرسل لك برسالة أو الى بريدك الالكتروني، فما هذه الإشارات ولماذا تستخدم؟ تابع قراءة المقال لتتعرف عليهم..

تلعب المصادقة المتعددة العوامل ( MFA:Multi-Factor Authentication) دوراً حيويًا في تعزيز الأمن السيبراني من خلال طلب أكثر من شكل تحقق للوصول إلى الأنظمة. مع تزايد التهديدات السيبرانية، أصبحت أنظمة MFA التقليدية بحاجة إلى التطور، وهنا يأتي دور الذكاء الاصطناعي (AI) لتعزيز فعاليتها[1,2]. حيث نستعرض في هذه المقالة دور الذكاء الاصطناعي في تعزيز الأمن السيبراني، من خلال تحسين التقنيات التقليدية مثل التشفير والمصادقة متعددة العوامل، واستخدام التعلم الآلي لاكتشاف الهجمات. حيث يستطيع الذكاء الاصطناعي تحليل سلوكيات المستخدمين، وتحسين التعرف البيومتري Biometric، والكشف عن التهديدات في الوقت الفعلي، مما يجعل أنظمة MFA أكثر ذكاءً وقدرة على التكيف. بالإضافة إلى ذلك، يسهم الذكاء الاصطناعي في تقليل الإزعاج للمستخدمين الشرعيين من خلال تقليل طلبات التحقق غير الضرورية. ومع ذلك، تظل هناك تحديات تتعلق بخصوصية البيانات والتكلفة والهجمات المتطورة. في المستقبل، من المتوقع أن تصبح أنظمة MFA المدعومة بالذكاء الاصطناعي أكثر تطورًا وقدرة على مواجهة التهديدات السيبرانية المعقدة، مما يعزز الأمن الرقمي بشكل عام.

كما يناقش التحديات المرتبطة بالذكاء الاصطناعي، مثل التزييف العميق والتحيز، ويؤكد على أهمية التوازن بين الأتمتة والخبراء البشريين. وفي نهاية البحث يختتم بتوصيات لتحسين الأنظمة الأمنية لمواجهة التهديدات الرقمية المتزايدة.

**الكلمات المفتاحية:** التشفير، المصادقة، تحليل البيانات، الذكاء الاصطناعي، الأمن السيبراني

## abstract

Have you ever wondered what "Prove you're not a robot" or "Verify you're human" means when you open a website? Or have you tried to log in and register on a website, social media app, or make a financial transaction and been asked to enter a code sent to you via text or email? Read on to learn more.

Multi-Factor Authentication (MFA) plays a vital role in enhancing cybersecurity by requiring more than one form of authentication to access systems. With the rise of cyber threats, traditional MFA systems need to evolve, and this is where artificial intelligence (AI) comes in to enhance their effectiveness. [1,2] In this article, we explore the role of AI in enhancing cybersecurity by improving traditional techniques such as encryption and multi-factor authentication, and using machine learning to detect attacks. AI can analyze user behavior, improve biometric identification, and detect threats in real time, making MFA systems smarter and more adaptable. Additionally, AI contributes to reducing inconvenience for legitimate users by eliminating unnecessary verification requests. However, challenges remain related to data privacy, cost, and sophisticated attacks. In the future, AI-powered MFA systems are expected to become more sophisticated and capable of countering complex cyber threats, enhancing overall digital security.

It also discusses challenges associated with AI, such as deepfakes and bias, and emphasizes the importance of balancing automation with human expertise. The paper concludes with recommendations for improving security systems to address growing digital threats.

**Keywords**: Encryption, Authentication, Data Analysis, Artificial Intelligence, Cybersecurity

## 1.مقدمة:

في عصرنا الرقمي الحالي أصبحت البيانات والمعلومات العمود الفقري للتقدم والابتكار في شتى المجالات مما يفرض علينا ضرورة حمايتها وتأمينها ضد التهديدات المتزايدة والمتطورة، ففي ظل الاعتماد الكبير على الشبكات والأنظمة الحاسوبية في تخزين ونقل المعلومات يبرز تحدي الحفاظ على سرية البيانات وضمان تكاملها وتوفير الدخول المصرح به إليها كأهم أهداف للأمن السيبراني. [ 2]

حيث تتراوح أساليب الحماية من الطرق التقليدية إلى التقنيات الحديثة التي تسهم في الكشف المبكر عن المخاطر وتحليلها، ومن هنا تبرز أهمية تقنيات الذكاء الاصطناعي في تعزيز الموثوقية والأمان في الأنظمة الحاسوبية، حيث يهدف البحث إلى دراسة دور الذكاء الاصطناعي في تعزيز أمان الأنظمة الحاسوبية عبر مراقبة الأنظمة، التعرف على التهديدات، والتصدي لها بسرعة، مع تحليل مميزات وتحديات تطبيق هذه التقنيات في البيئات الحديثة.[3]

حيث يتم تأمين وحماية هذه الأنظمة الحاسوبية من خلال عدة طرق مثل:

- الجدران النارية
- أنظمة مكافحة الفيروسات
- التشفير
- المصادقة

وكما هو معروف فإن الجدران النارية وأنظمة مكافحة الفيروسات هي معروفة ومستخدمة من قبل الجميع وحتى انها صارت موجودة من ضمن النظام الحاسوبي سواء في الحواسيب او في الهواتف المحمولة.

**أما بالنسبة للتشفير:** فيمكن أن نعرفه على انه عملية تحويل البيانات من شكلها الأصلي إلى صيغة غير مفهومة (نص مشفر) باستخدام خوارزميات رياضية، وله العديد من الأنواع مثل:

1. **التشفير بالمفتاح المتماثل:** والذي يعتمد على استخدام مفتاح وحيد للتشفير وفك التشفير **مثل خوارزميات:**

DES (Data Encryption Standard) و AES (Advanced Encryption Standard)

2. **التشفير بالمفتاح غير المتماثل:** ويكون باستخدام مفتاحين، مفتاح عام للتشفير، ومفتاح خاص لفك التشفير.

**مثل خوارزمية:** RSA (Rivest-Shamir-Adleman)

3. **التشفير أثناء النقل والتخزين:** ويعمل على حماية البيانات أثناء انتقالها عبر الإنترنت واثناء تخزينها في الأقراص الصلبة او في قواعد البيانات، **مثل:** بروتوكول HTTPS وVPN.

وهي تعد من طرق الحماية الفعالة والمستخدمة في العديد من المجالات مثل BitLocker في Windows و FileVault في macOS والعديد من الطرق الأخرى.

**والنوع الآخر من الحماية هو المصادقةAuthentication :**

وهي عملية التحقق من هوية المستخدم أو الجهاز لضمان أن الشخص أو النظام الذي يحاول الوصول إلى مورد معين هو ما يدعيه. حيث تُعد المصادقة خطوة أساسية في تأمين الأنظمة والمعلومات، لأنها تمنع الوصول غير المصرح به وتحمي البيانات الحساسة.[1,4]

تُعد المصادقة جزأً أساسياً في حماية الأنظمة الرقمية، حيث يتم من خلالها التأكد من هوية المستخدمين قبل السماح لهم بالوصول إلى المعلومات أو الموارد المحمية.

تتضمن بروتوكولات المصادقة التقليدية عادةً استخدام اسم المستخدم وكلمة المرور وهي آلية تعتمد على "عامل المعرفة" (Knowledge Factor)، أي المعلومات التي يعرفها المستخدم. ومع ذلك، ومع تطور أساليب الهجمات الإلكترونية، أظهرت الدراسات أن الاعتماد على عامل واحد فقط، مثل كلمة المرور، لم يعد كافياً لضمان أمان الأنظمة، حيث يمكن اختراق كلمات المرور و سرقتها بطرق مختلفة مثل هجمات القوة الغاشمة (Brute Force) وهجمات التصيد (Phishing).[3,5,6]

**2.المصادقة المتعددة العوامل**

لتعزيز الأمان، ظهرت **المصادقة متعددة العوامل** (Multi-Factor Authentication - MFA)، هي طريقة أمنية تتطلب من المستخدم تقديم أكثر من شكل واحد من أشكال التحقق للوصول إلى حساب أو نظام.[7,8,9]

أي تقنية تجمع بين عاملين أو أكثر من عوامل المصادقة المختلفة. وتُقسم العوامل المستخدمة عادةً إلى ثلاثة أنواع رئيسية:

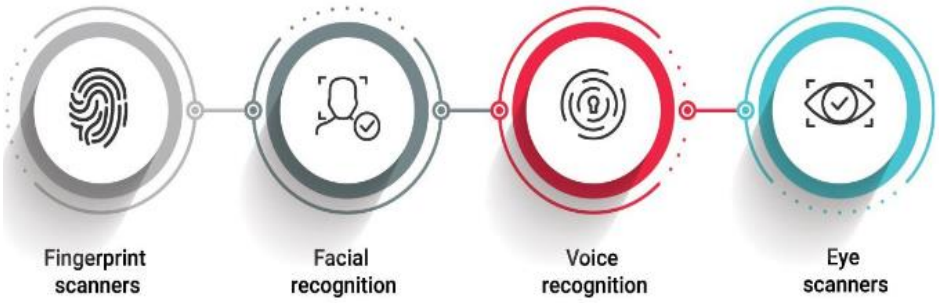
- عامل المعرفة شيء تعرفه (Something You Know): مثل كلمة المرور أو رقم التعريف الشخصي (PIN).

ومن ابرز التقنيات OTP ( كلمات المرور لمرة واحدة) ترسل كود تحقق عبر الرسائل النصية أو البريد الالكتروني.

- عامل الملكية ( Ownership Factor) شيء تمتلكه (Something You Have): مثل الهاتف المحمول أو البطاقة الذكية او بطاقة التعريف أو Hardware Tokens (الرموز المادية) أجهزة توليد الرموز[5,6] (شكل 1).


الشكل (1) المصادقة باستخدام الرموز المادية

- العامل البيومتري ( Biometric Factor) شيء أنت عليه (Something You Are):الذي يعتمد على الصفات الحيوية التي تميز شخص عن آخر. وهو ما يسمى **المصادقة البيومترية** حيث تعتمد على السمات البيولوجية مثل بصمات الأصابع وقزحية العين والأصوات وميزات الوجه بالإضافة الى شكل الأذن للتحقق من هوية المستخدم (شكل 2).




الشكل (2) أنواع المصادقة البيومترية

من خلال دمج هذه العوامل، تسهم MFA في تقليل اختراق الأنظمة الرقمية، حيث يصبح من الصعب على المهاجمين تجاوز جميع العوامل في الوقت ذاته.[3]

ونلاحظ ان المصادقة مستخدمة حالياً بكثرة وأحد أبرز الأمثلة هي استخدام دولة الامارات للمصادقة البيومترية حيث يتم الدخول الى البلد عن طريق بصمة العين بدلاً من اظهار جواز السفر.

### 3.دور الذكاء الصنعي في تعزيز الأمان:

لقد كان للذكاء الصنعي دور مهم في جميع المجالات ولا سيما في الآونة الأخيرة حيث لوحظ أنه أصبح بإمكاننا توفير الكثير من الوقت والجهد من خلاله فهو يستطيع القيام بالكثير من الأعمال التي تكون شاقة وتأخذ وقتاً طويلاً من الانسان بدقائق معدودة وذلك لأن AI يتسم بالعديد من الميزات مثل:

1. القدرة على التعلم والتكيف

2. الأتمتة والكفاءة
3. تحليل البيانات الضخمة بسرعة
4. اتخاذ القرارات المعقدة
5. التكيف في الزمن الحقيقي

ويعتمد على مجموعة من التقنيات مثل:

التعلم الآلي(Machine Learning) ,التعلم العميق(Deep Learning), معالجة اللغة الطبيعية (NLP) والرؤية الحاسوبية(Computer Vision) . [10,11]

ومن أهم الأمثلة على المصادقة المعتمدة على الذكاء الصنعي:

تطبيقات مثلGoogle Authenticator، وهي عند عرض الموقع الإلكتروني لخيار "أثبت أنك لست روبوت" وتسمى عوامل CAPTCHA و reCAPTCHA حيث مهمتها الحد من دخول الروبوتات -التي قد تدخل الى المواقع وتسبب ضرراً فيها أو تقوم بحقن بعض الفيروسات- وذلك من خلال الطلب من المستخدمين اختيار بعض الصور أو طلب كتابة نص مشوه او غيرها من الأدوات، حيث يقوم بتحليل سرعة الكتابة أو من خلال تتبعه لحركة الفأرة عند الضغط على مربع "يتم التحقق من أنك انسان" لأن الروبوت تكون حركته خطية أما الانسان فيقوم بتحريك الفأرة بطريقة عشوائية، كما أنه يوجد العديد من الطرق الاخرى.

### 1.3.تقنيات الذكاء الصنعي لدعم الأمن السيبراني

بعض الطرق والاستراتيجيات التي يمكن الاستفادة منها في الذكاء الصنعي نوجزها من خلال النقاط التالية[12] :

1. **اكتشاف التهديدات والاستجابة لها**: استخدام الذكاء الاصطناعي في رصد الأنماط غير الطبيعية وتحليل البيانات الكبيرة لاكتشاف الهجمات الإلكترونية بسرعة.
2. **تعزيز الاستجابة للهجمات**: تقنيات الذكاء الاصطناعي تساعد على اتخاذ قرارات سريعة وفعّالة أثناء الهجمات لتقليل الأضرار.
3. **التحليلات التنبؤية (Predictive Analytics)** تمثل أحد أبرز استخدامات تقنيات الذكاء الاصطناعي في تعزيز **الأمن السيبراني**، وتعتمد على خوارزميات الذكاء الاصطناعي (مثل التعلم الآلي) لتحليل البيانات السابقة والتعرف على الأنماط التي تسبق الحوادث الأمنية، ومن ثم التنبؤ بالتهديدات المستقبلية قبل وقوعها.

**وبالتالي يمكن الاستفادة من التحليلات التنبؤية لدعم الأمن السيبراني من خلال:**

أ- **التنبؤ بالهجمات قبل وقوعها**:من خلال تحليل سلوك المستخدمين وحركة الشبكة لاكتشاف أنماط تؤشر إلى تهديد قادم (مثل محاولات الاختراق أو تسريب البيانات).

ب- **تصنيف التهديدات حسب الخطورة**:التحليلات التنبؤية تساعد في تحديد أولويات الاستجابة، عبر تصنيف الهجمات المحتملة وفقًا لمدى تأثيرها وخطورتها.

ت- **رصد الثغرات الأمنية المستقبلية**:التنبؤ بالمناطق أو التطبيقات الأكثر عرضة للهجوم، مما يسمح بإجراء صيانة وقائية مسبقة.

ث- **تحسين نظم كشف التسلل(IDS)** :بدمج التحليلات التنبؤية مع أنظمة الكشف، تصبح أكثر قدرة على التمييز بين الأنشطة العادية والخبيثة بدقة أعلى.

ج- **التقليل من الإنذارات الكاذبة(False Positives)** :عبر التعلم من البيانات السابقة وتحسين خوارزميات التوقع، ما يقلل من التشتت ويزيد من فعالية فرق الأمن.

4. **تعزيز قدرات الأمن السيبراني**:من خلال تحليل التهديدات والتعلّم المستمر، يمكن تعزيز قدرة الأنظمة على التنبؤ بالهجمات ومنعها.
5. **التعلم المستمر**:الذكاء الاصطناعي يعتمد على التعلّم المستمر لتحسين مستوى الحماية مع كل تهديد جديد يتم رصده.

كما يساعد الذكاء الاصطناعي في **التحديثات التلقائية** حيث يمكّن الأنظمة من تحديث قواعد البيانات الأمنية تلقائيًا دون تدخل بشري.

### 2.3 كيف يعزز الذكاء الاصطناعي أنظمة MFA؟

مع تزايد تعقيد الهجمات السيبرانية، أصبحت أنظمة MFA التقليدية بحاجة إلى التطور لمواكبة التهديدات الجديدة. هنا يأتي دور الذكاء الاصطناعي، حيث يمكنه تحسين أنظمة MFA بعدة طرق:

#### 1.2.3. تحليل السلوكيات والتعرف على الأنماط

يستخدم الذكاء الاصطناعي تقنيات مثل التعلم الآلي (Machine Learning) لتحليل سلوكيات المستخدمين والتعرف على الأنماط الطبيعية لهم. على سبيل المثال، يمكن للنظام أن يتعلم كيفية كتابة المستخدم لكلمة المرور، أو الأوقات التي يكون فيها نشطاً، أو حتى الأجهزة التي يستخدمها عادةً(حاسب أو هاتف أو غير ذلك.). إذا تم اكتشاف أي نشاط غير عادي، مثل محاولة الوصول من موقع جغرافي مختلف أو في وقت غير معتاد، يمكن للنظام أن يطلب عوامل تحقق إضافية أو حتى يمنع الوصول بشكل مؤقت.[1,12]

#### 2.2.3. التعرف البيومتري الذكي

أصبحت تقنيات التعرف البيومتري مثل البصمة والصوت والوجه أكثر دقة بفضل الذكاء الاصطناعي. يمكن للأنظمة المدعومة بالذكاء الاصطناعي تحليل السمات البيومترية بدقة عالية، مما يجعل من الصعب على المهاجمين تزييفها. على سبيل المثال، يمكن للذكاء الاصطناعي اكتشاف الفرق بين صورة حقيقية لوجه المستخدم وصورة ثابتة أو فيديو مسجل.

#### 3.2.3. التكيف مع التهديدات في الوقت الفعلي

أحد أكبر مزايا الذكاء الاصطناعي هو قدرته على التكيف مع التهديدات الجديدة في الوقت الفعلي. يمكن لأنظمة MFA المدعومة بالذكاء الاصطناعي مراقبة الأنشطة المشبوهة والاستجابة لها بشكل تلقائي. على سبيل المثال، إذا تم اكتشاف محاولة اختراق متكررة، يمكن للنظام أن يزيد من عدد عوامل التحقق المطلوبة أو يمنع الوصول تماماً حتى يتم التحقق من هوية المستخدم.

#### 4.2.3. تقليل الإزعاج للمستخدمين الشرعيين

في كثير من الأحيان، يمكن أن تكون أنظمة MFA التقليدية مزعجة للمستخدمين بسبب الحاجة المتكررة لإدخال عوامل تحقق إضافية. بفضل الذكاء الاصطناعي، يمكن للنظام أن يتعلم متى يكون المستخدم شرعياً ومتى يكون هناك خطر محتمل. هذا يعني أن المستخدمين الشرعيين لن يحتاجوا إلى إدخال عوامل تحقق إضافية إلا في حالات الشك، مما يحسن تجربة المستخدم مع الحفاظ على الأمان.

#### 5.2.3 الكشف عن الهجمات المنسقة

بعض الهجمات السيبرانية تكون منسقة وتستهدف عدة حسابات في نفس الوقت. يمكن للذكاء الاصطناعي تحليل الأنماط عبر عدة حسابات واكتشاف الهجمات المنسقة التي قد لا يتم اكتشافها بواسطة أنظمة MFA التقليدية. على سبيل المثال، إذا تم اكتشاف محاولات وصول متزامنة من عدة مواقع جغرافية مختلفة، يمكن للنظام أن يتخذ إجراءات وقائية.

### 4.التحديات والمستقبل

على الرغم من الفوائد الكبيرة التي يوفرها الذكاء الاصطناعي في تعزيز أنظمة MFA، إلا أن هناك بعض التحديات والمخاطر المرتبطة بتطبيقه في الأمن السيبراني، والتي يجب مراعاتها. من بين هذه التحديات:

- التزييف العميق (Deepfake): يمكن استخدام الذكاء الاصطناعي لإنشاء محتوى مزيف يصعب اكتشافه
- خصوصية البيانات: يتطلب الذكاء الاصطناعي كميات كبيرة من البيانات لتدريب النماذج، مما يثير مخاوف حول خصوصية المستخدمين.
- التحيز في النماذج: قد تكون نماذج الذكاء الاصطناعي متحيزة بسبب البيانات المستخدمة في تدريبها
- التكلفة: قد تكون أنظمة MFA المدعومة بالذكاء الاصطناعي مكلفة في التطبيق والصيانة.
- الهجمات المتطورة: مع تطور الذكاء الاصطناعي، تتطور أيضًا تقنيات الهجوم، يمكن للمهاجمين استغلال الثغرات في أنظمة الذكاء الاصطناعي لتنفيذ هجمات إلكترونية، مما يتطلب تحديثًا مستمرًا لأنظمة الحماية.

مع ذلك، فإن مستقبل الذكاء الاصطناعي في مجال الأمن السيبراني يبدو واعداً. مع استمرار التطورات التكنولوجية، من المتوقع أن تصبح أنظمة MFA أكثر ذكاءً وقدرة على التكيف مع التهديدات السيبرانية المتطورة.[13,14]

**5. التوصيات الاستراتيجية**

1. **تبني خطط للتحول نحو تشفير مقاوم للكم** (PQ-Crypto) بدءًا من الآن.
2. **الاستثمار في البحث والتطوير المشترك** بين قطاعات الأمن السيبراني والذكاء الاصطناعي والحوسبة الكمية.
3. **تدريب الكوادر** على مفاهيم الحوسبة الكمية وتأثيراتها على الأمن الرقمي.
4. **المراقبة النشطة للتطورات في الحوسبة الكمية** لتقدير زمن "نقطة الانفجار الكمي (Quantum Break Point)".
5. **تعزيز الشراكات الدولية** لتطوير معايير حماية عالمية لما بعد الحوسبة الكمية.

في ظل تسارع التحولات الرقمية، فإن الذكاء الاصطناعي سيبقى سلاحًا ذو حدين في الأمن السيبراني، أما الحوسبة الكمية فستكون القفزة الكبرى التالية، التي إما أن تُحدث خللًا هائلًا في الأمن الرقمي، أو أن تُستثمر لحماية المستقبل الرقمي للبشرية.
لذلك فالاستعداد المبكر هو الفيصل بين من يقود هذا المستقبل، ومن يصبح ضحية له.

**الخاتمة:**

وفي الختام نلاحظ أنه ومع تزايد اعتمادنا على التكنولوجيا في مختلف جوانب الحياة، تبرز الحاجة إلى تطوير حلول متقدمة تجمع بين الذكاء الاصطناعي والاستراتيجيات الأمنية التقليدية لضمان السرية والتكاملية والدخول المصرح به للبيانات. وبناءً على ما تم عرضه، يتضح أن مستقبل الأمن السيبراني يعتمد بشكل كبير على الابتكار المستمر والتكيف مع المستجدات الرقمية. لذا، فإن تطوير سياسات أمنية أكثر صرامة، وتعزيز الوعي الأمني، والاعتماد على تقنيات الذكاء الاصطناعي بشكل مسؤول، ستشكل الركائز الأساسية لحماية البيانات والأنظمة في المستقبل.

حيث يعد الذكاء الاصطناعي أداة قوية لتعزيز الأمن السيبراني، خاصة عندما يتعلق الأمر بالمصادقة المتعددة العوامل (MFA). من خلال تحليل السلوكيات، وتحسين التعرف البيومتري، والاستجابة للتهديدات في الوقت الفعلي، يمكن للذكاء الاصطناعي أن يجعل أنظمة MFA أكثر فعالية وأقل إزعاجاً للمستخدمين. ومع استمرار تطور التهديدات السيبرانية، سيكون الذكاء الاصطناعي عنصراً أساسياً في بناء أنظمة أمنية قادرة على مواجهة التحديات المستقبلية.

## References المراجع والمصادر:


1. Multi-Factor Authentication in Large Scale. Be. Pavel Brousek ,2019
2. Artificial Intelligence Cybersecurity Challenges [2020].
3. Hacking: The Art of Exploitation, 2nd Edition JON ERICKSON. 2008
4. A Two Factor Authentication Scheme . Costa , J.. 2FA2P2 Technical Report, 2017.
5. Analysis of Vulnerabilities That Can Occur When Generating One-Time Password. H,Kim and J,Han and C,Park and O,Yi, 2020
6. Focused on Two Factor Authentication Framework Using OTP – SMS Based on Blockchain, Eman.K 2019
7. The Role of Multi-factor Authentication for Modern Day Security, Joseph Williamson Kevin Curran, 2021
8. A Systematic Review on Multi-Factor Authentication Framework, Muhammad Syahreen1, Noor Hafizah2, Nurazean Maarop3, Mayasarah Maslinan,2024
9. Device Identity-Based User Authentication on Electronic Payment System for Secure E-Wallet Apps. Electronics M,ARIF. and Z,SHUKUR, 2022
10. Artificial Intelligence in Cybersecurity: Enhancing Threat Detection and Mitigation Basiru A. Olafuyi, 2023
11. Advancing cybersecurity with artificial intelligence and machine learning: Architectures, algorithms, and future directions in threat detection and mitigation, Souratn Jain ,2025
12. Enhancing Cybersecurity through AI and ML:Strategies, Challenges, and Future Directions, Maryam Roshanaei, Mahir R. Khan, Natalie N. Sylvester, 2024
13. Artificial Intelligence in Cyber Security: Research Advances, Challenges, and Opportunities, Zhimin Zhang ,Huansheng Ning, Feifei Shi, Fadi Farha [2022].
14. The Impact of Artificial Intelligence on the Future of Cybersecurity, MARIAM ALDHAMER,2024