ISSN: 2706-6495

التحكم في الوصول إلى البيانات مع الحفاظ على الخصوصية في شبكات المدن الذكية باستخدام التعلم الآلي

Privacy-Preserving Data Access Control in Smart City Networks Using Machine Learning

إعداد: الباحثة/ أسماء سليمان إبراهيم الشدوخي

باحثة ماجستير ذكاء اصطناعي، جامعة حائل، المملكة العربية السعودية

Email: S20231388@uoh.edu.sa

الدكتور/ طارق سعد المريزيق

أستاذ مشارك، قسم المعلومات وعلوم الحاسب كلية علوم وهندسة الحاسب الآلي، جامعة حائل، حائل المملكة العربية السعودية

Email: t.almuraziq@uoh.edu.sa

ملخص البحث:

يشهد العالم تحضرًا متسارعًا، وأصبحت المدن الذكية أحد الحلول لتحسين الحياة في المدينة. تعتمد هذه المدن على شبكات تقنية رقمية ضخمة، وتُنتج بيانات حساسة عن مواطنيها أكثر من أي وقت مضى. وهذا يُثير تضاربًا في المصالح المباشرة بين فائدة البيانات والحق الأساسي في الخصوصية. لا يُمكن استخدام أنظمة التحكم في الوصول القياسية في هذه البيئات الديناميكية. يتمثل التحدي الذي يواجه هذا البحث في تطوير واختبار نظام تحكم وصول جديد يحافظ على الخصوصية. سيعتمد النظام المقترح على نظام تعلُّم آلي، أي مجموعة من نماذج التعزيز التدريجي (XGBoost وLightGBM وCatBoost)، لتحديد الوصول الذكي الواعي للسياق. ولضمان عدم تأثير عملية التعلم نفسها على الخصوصية، يُدمج النظام خصوصية تفاضلية، مُقدمًا ضمانات رسمية ورياضية. خضع النظام لاختبارات دقيقة باستخدام مجموعة بيانات تركيبية كبيرة تحاكي أنماط الوصول في العالم الحقيقي. تُظهر النتائج أن النظام يتمتع بكفاءة عالية بدقة 98.20% ومساحة تحت المنحنى 0.9869. علاوة على ذلك، كشف تحليل أداء الخصوصية عن ما يُسمى بالنقطة المثالية، من خلال إثبات إمكانية الحصول على ضمانات خصوصية عالية الحماية بتكلفة زهيدة من حيث الدقة. تُقدم هذه الدراسة نظامًا تجريبيًا يُثبت أن الخصوصية والأمان لا يعيقان ابتكار المدن الذكية، بل هما مبدأ ان أساسيان لتطوير أنظمة حضرية فعّالة وموثوقة.

الكلمات المفتاحية: المدن الذكية، التحكم في الوصول، التعلم الآلي، الحفاظ على الخصوصية، الخصوصية التفاضلية، نماذج التجميع.

ISSN: 2706-6495

Privacy-Preserving Data Access Control in Smart City Networks Using Machine Learning

Asma Suliman Ibraheem Alshdokhi

Master's Candidate in Artificial Intelligence, University of Hail, Hail, Kingdom of Saudi Arabia

Email: S20231388@uoh.edu.sa

Dr. Tariq Saad Almuraziq

Associate Professor, Department of Information and Computer Science, College of Computer Science and Engineering, University of Hail, Hail, Kingdom of Saudi Arabia

Email: t.almuraziq@uoh.edu.sa

Abstract:

The world is fast becoming urbanized and smart cities are becoming one of the solutions to better life in the city. These cities rely on massive digital technology networks, and they produce more sensitive data on its citizens than ever before. This brings conflict of direct interest between the utility of data and the basic right of privacy. The standard access control systems cannot be used in these dynamic settings. The challenge to this research is the development and testing of a new privacy-saving access control system. The suggested system will be based on a machine learning system, namely, a collection of gradient boosting models (XGBoost, LightGBM, CatBoost), to determine smart, context-aware access. In order to make the privacy not be impinged upon by the learning process itself, the system incorporates differential privacy, offering formal, mathematical guarantees. The system was strictly tested with a large synthetic data set that simulated access patterns in the real world. Findings show that the system has a high degree of effectiveness with an accuracy of 98.20%and the AUC of 0.9869. Moreover, the analysis privacy-performance revealed the so-called sweet spot, by demonstrating that high-protect privacy guarantees are obtainable at an insignificant cost in terms of accuracy. This study offers an empirical system that proves that privacy and security do not hinder the smart city innovation but are crucial principles to develop effective and reliable urban ecosystems.

Keywords: Smart Cities, Access Control, Machine Learning, Privacy-Preserving, Differential Privacy, Ensemble Models.

ISSN: 2706-6495

1. المقدمة:

شهد العالم تحولاً حضرياً متسارعاً، حيث أصبحت المدن الذكية ركيزة أساسية لتحسين جودة الحياة واستدامة الخدمات الحضرية (Albino, V., Berardi, U., & Dangelico, R. M., 2015). تعتمد هذه المدن على بنية تحتية رقمية معقدة وشبكات واسعة من أجهزة إنترنت الأشياء (IoT) التي تولد كميات هائلة من البيانات الحساسة حول المواطنين وأنماط حياتهم (Zanella et al., 2014). يخلق هذا الواقع تضارباً جوهرياً بين الفائدة المتوقعة من هذه البيانات في تحسين كفاءة إدارة المدن، والحق الأساسي للأفراد في الخصوصية وحماية بياناتهم الشخصية (Kitchin, 2016).

في قلب هذا التحدي، تكمن آليات التحكم في الوصول إلى البيانات. فالأنظمة التقليدية، مثل التحكم في الوصول القائم على الأدوار (RBAC)، صُممت لبيئات تكنولوجيا المعلومات ثابتة ومحددة، مما يجعلها غير قادرة على التكيف مع الطبيعة الديناميكية والمعقدة للمدن الذكية (Sandhu et al., 1996). من ناحية أخرى، على الرغم من أن حلول التعلم الآلي تقدم وعوداً كبيرة بتحقيق ذكاء سياقي، إلا أنها غالباً ما تتجاهل البعد الحاسم لخصوصية البيانات المستخدمة في عملية التدريب نفسها، مما يخلق "مفارقة الخصوصية" (Dwork, 2006).

لمعالجة هذه الفجوة البحثية، يهدف هذا البحث إلى تطوير إطار عمل متكامل للتحكم في الوصول إلى البيانات في شبكات المدن الذكية، يجمع بين ثلاثة أهداف رئيسية بالتوازي: الذكاء السياقي من خلال نماذج تعلم آلي متقدمة، الحفاظ على الخصوصية عبر ضمانات رياضية صارمة باستخدام الخصوصية التفاضلية، والكفاءة والأداء العالي لضمان القابلية للتطبيق في بيئات العالم الحقيقي. تسعى هذه الدراسة للإجابة عن سؤال جوهري: هل يمكن بناء أنظمة تحكم في الوصول تكون ذكية وفعالة وفي جوهرها تحافظ على خصوصية المواطنين وثقتهم؟ إن الإجابة العلمية والعملية على هذا السؤال تمثل مساهمة أساسية نحو تحقيق مدن ذكية موثوقة وآمنة.

1.1. مشكلة البحث:

مع التوسع الحضاري المتسارع أصبحت المدن الذكية التي تعتمد على شبكات رقمية واسعة وأجهزه إنترنت الأشياء (IoT) حلا لتحسين جودة الحياة واستدامة الخدمات. لكن هذه البنية التحتية المرتبطة تولد كميات هائلة من البيانات الحساسة للمواطنين بدءاً من أنماط الحركة والسلوك وصولا إلى التفضيلات الشخصية هذا يخلق صراعا مباشرا بين فائدة هذه البيانات في إدارة المدن بكفاءة والحق الأساسي للأفراد في الخصوصية (Zanella et al., 2014). تفشل أنظمة التحكم في الوصول التقليدي مثل التحكم القائم على الأدوار (RBAC)، في التكيف مع الطبيعة الديناميكية والمعقدة لبيئات المدن الذكية مما يجعلها غير كافية لحماية البيانات بشكل فعال. (Sandhu et al., 1996) من هنا تنشأ مشكلة البحث الرئيسية كيف يمكن تصميم نظام للتحكم في الوصول يكون ذكيا وقادرا على التكيف مع السياق وفي نفس الوقت يضمن اعلى مستويات حماية الخصوصية للمواطنين في شبكات المدن الذكية؟

2.1. أسئلة البحث:

يتمحور هذا البحث حول الإجابة على الأسئلة الأتية:

1. ما هي أبرز تحديات الخصوصية والأمان في أنظمه التحكم بالوصول في المدن الذكية الحديثة؟
2. كيف يمكننا توظيف نماذج التعلم الآلي لاتخاذ قرارات وصول ذكية وواعية بسياق مع ضمان مستويات عالية من الخصوصية؟

3. ما هي أفضل التقنيات الحفاظ على الخصوصية التي يمكن دمجها مع أنظمه التحكم بالوصول القائم على التعلم الآلي في السياق المدن الذكية؟
4. كيف يتراوح أداء النظام المقترح من حيث الأمان والحماية الخصوصية والكفاءة مقارنة بالطرق الموجودة؟

3.1. أهداف البحث وأهميته:

يهدف هذا البحث إلى تطوير إطار عمل متكامل للتحكم في الوصول يحافظ على الخصوصية في شبكات المدن الذكية. الأهداف المحددة تشمل: تصميم بنية نظامية متقدمة، تطبيق نماذج تعلم آلي ذكية، دمج تقنيات الخصوصية التفاضلية، وتقييم النظام بشكل شامل. تكتسي هذه الدراسة أهمية بالغة لأنها تقدم حلاً عمليًا لأحد أكبر التحديات التي تواجه المدن الذكية، مما يساهم في بناء ثقة المواطنين وتعزيز الانتقال نحو مدن أكثر ذكاءً وأمانًا وفعالية.

4.1. مصطلحات البحث:

- **المدن الذكية:(Smart Cities)** مراكز حضرية تستخدم التقنيات الرقمية وأجهزة الاستشعار لتحسين جودة الخدمات والبنية التحتية.
- **التحكم في الوصول:(Access Control)** الآلية التي تحدد من يمكنه الوصول إلى ماذا من البيانات، وتحت أي ظروف.
- **الخصوصية التفاضلية :(Differential Privacy)** تقنية توفر ضمانات رياضية قوية بأن نتائج تحليل مجموعة البيانات لا تكشف عن معلومات حول أي فرد فيها.

5.1. حدود البحث:

يقتصر هذا البحث على مشكلة التحكم في الوصول للبيانات، مع التركيز على الأساليب الحافظة على الخصوصية القائمة على التعلم الآلي. تم تقييم النظام باستخدام بيانات اصطناعية محاكاة للواقع، نظرًا للصعوبات الأخلاقية واللوجستية في الحصول على بيانات حقيقية. كما أن البحث لا يغطي جوانب الأمان الأوسع مثل أمن الشبكات أو الأمان المادي للبنية التحتية.

2. الإطار النظري والدراسات السابقة:

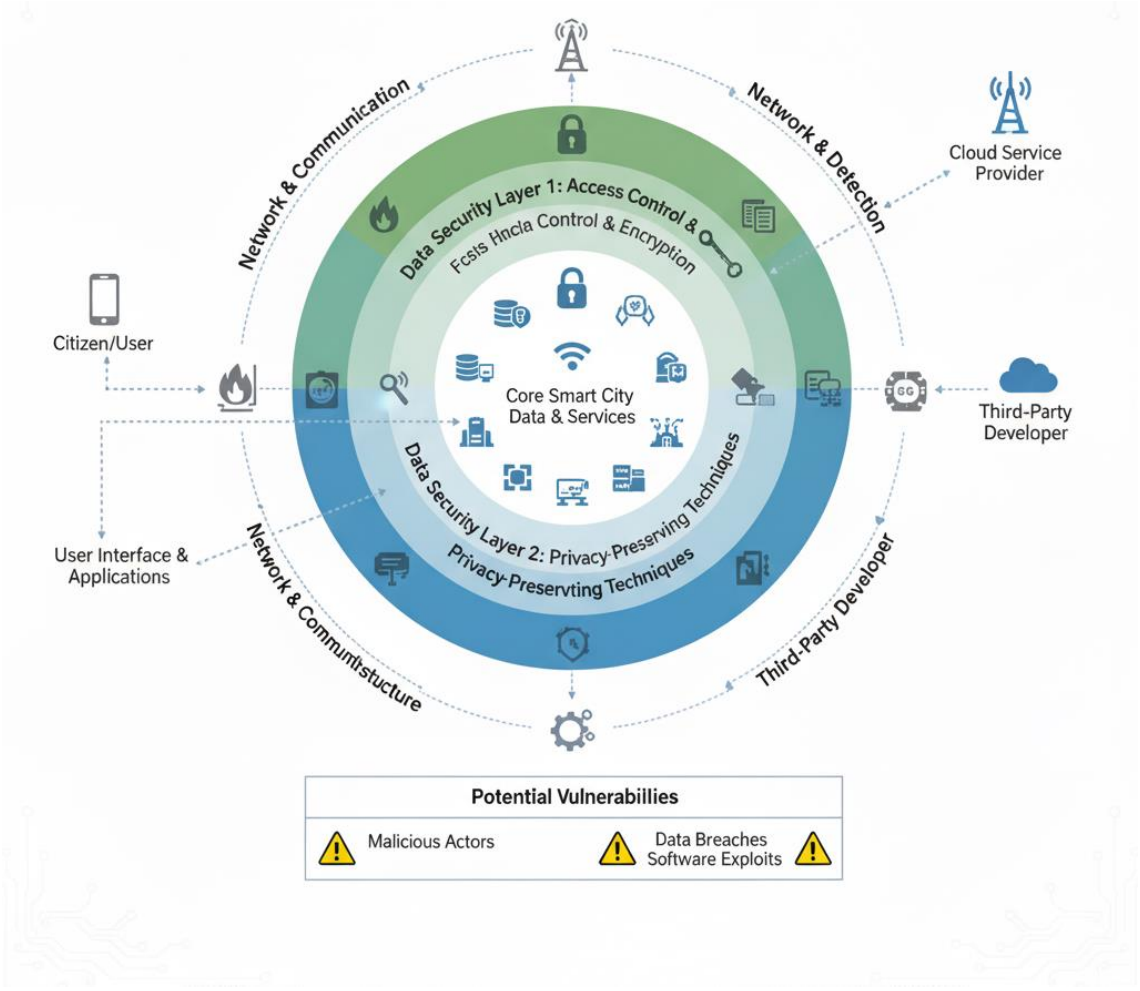
1.2. الإطار النظري:

1.1.2. البيئة الأمنية المعقدة في المدن الذكية

إن البنية التحتية للمدن الذكية ليست كيانًا أحاديًا، بل هي نظام بيئي معقد ومترابط من الشبكات والأجهزة والمنصات. كما أشار Batty et al. (2012)، فإن هذه البنية الموزعة، التي تمتد عبر حدود إدارية متعددة ونماذج ملكية متنوعة، تخلق سطح هجوم هائل. كل جهاز استشعار، كل كاميرا مراقبة، كل نظام تحكم في الإشارات هو نقطة وصول محتمل للمهاجمين. هذا التعقيد الهيكلي يجعل تطبيق نماذج الأمان التقليدية، التي صممت لبيئات تكنولوجيا المعلومات ذات الحدود الواضحة، أمرًا صعبًا للغاية.

علاوة على ذلك، فإن الطبيعة في الوقت الفعلي للعديد من تطبيقات المدن الذكية تضيف طبقة أخرى من التعقيد. أنظمة الاستجابة للطوارئ، وشبكات الطاقة الذكية، وأنظمة المرور التكيفية تتطلب وصولاً فوريًا إلى البيانات لتعمل بفعالية. هذا المطلب لانخفاض زمن الوصول (Low Latency) قد يتعارض مع بروتوكولات الأمان التقليدية التي قد تضيف تأخيرًا بسبب عمليات المصادقة المعقدة. هذا التوتر بين الحماية وإمكانية الوصول هو أحد التحديات المركزية في أمن المدن الذكية.

ISSN: 2706-6495



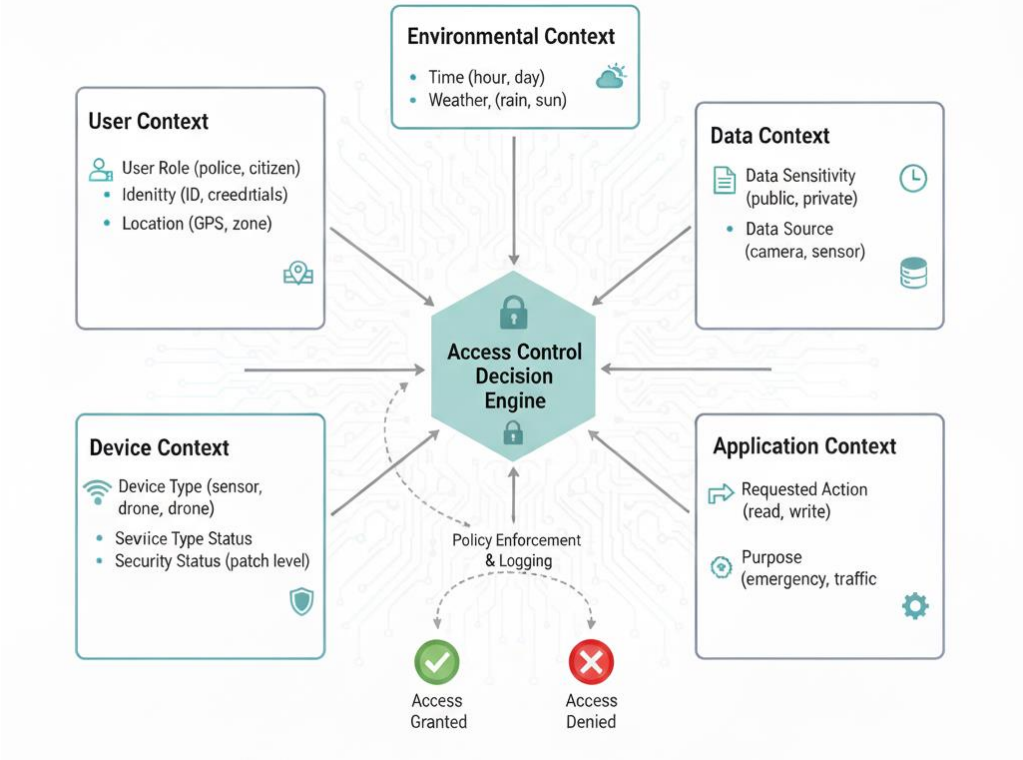
الشكل 1: *البنية المعقدة لأمن البيانات في المدينة الذكية*

المصدر: الباحثة بالاعتماد على (Batty et al., 2012)

2.1.2. دور التحكم في الوصول كخط دفاع أول:

في قلب أي استراتيجية أمنية للبيانات يكمن التحكم في الوصول. إنه الآلية الأساسية التي تفرض سياسة الأمان، محددة من يمكنه الوصول إلى ماذا، ومتى، ولأي غرض. في سياق المدن الذكية، لا يعد التحكم في الوصول مجرد مسألة تقنية، بل هو ضرورة حيوية للحفاظ على الثقة العامة وضمان الاستخدام الأخلاقي للبيانات. تواجه أنظمة التحكم في الوصول التقليدية تحديات كبيرة في هذا السياق. أولاً، مشكلة الحجم: يجب على أنظمة المدن الذكية التعامل مع ملايين نقاط البيانات وآلاف المستخدمين بأذونات ومتطلبات متنوعة. هذا الحجم الهائل يجعل الإدارة اليدوية للأذونات مستحيلة (Zanella et al., 2014). ثانيًا، مشكلة السياق: ملاءمة الوصول إلى البيانات في المدينة الذكية يمكن أن تتغير بشكل كبير بناءً على عوامل سياقية مثل الوقت من اليوم، والموقع الجغرافي، والغرض من الوصول، والتهديدات الأمنية الحالية. على سبيل المثال، قد يكون لمخطط مدينة الحق في الوصول إلى بيانات حركة المرور الحالية خلال ساعات العمل، ولكن يجب منعه من الوصول إلى نفس البيانات أثناء عملية طوارئ أمنية قد تكشف عن خطط الاستجابة. هذا البعد السياقي يتطلب آليات يمكنها تقييم عوامل متعددة في وقت واحد.

ISSN: 2706-6495



الشكل 2: *إطار للتحكم في الوصول السياقي في شبكات المدن الذكية*

المصدر: الباحثة بالاعتماد على إطار العمل النظري لـ(Hu et al., 2015)

نماذج مثل التحكم القائم على الأدوار (RBAC) والتحكم القائم على السمات (ABAC) تقدم حلولاً جزئية. RBAC، كما وصفه Sandhu et al. (1996)، يخصص الأذونات بناءً على وظيفة المستخدم، ولكنه يفتقر إلى المرونة اللازمة لاتخاذ قرارات سياقية دقيقة. ABAC، كما أوضحه Hu et al. (2015)، هو أكثر مرونة حيث يأخذ في الاعتبار سمات متعددة لطلب الوصول، ولكنه لا يزال يعتمد على مجموعة من القواعد المحددة مسبقًا قد لا تكون قادرة على التكيف مع التهديدات المتطورة وأنماط الاستخدام الجديدة.

3.1.2. التعلم الآلي كنهج مبتكر:

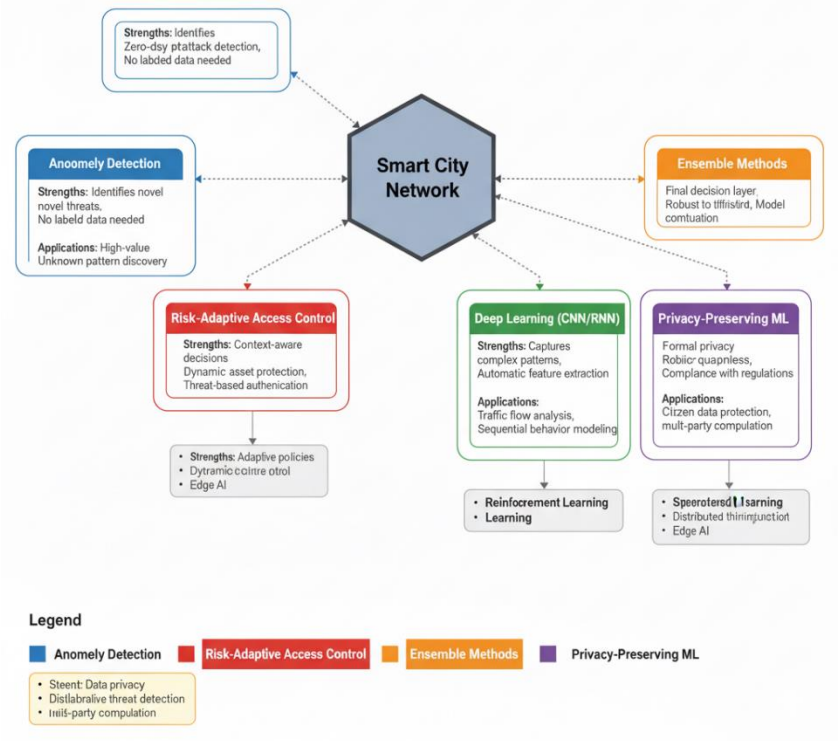
لقد برز التعلم الآلي كقوة تحويلية في معالجة مشاكل اتخاذ القرار المعقدة، وتطبيقه في أنظمة التحكم في الوصول هو تطور طبيعي لتقنيات الأمان. على عكس الأنظمة القائمة على القواعد، والتي يجب تكوينها يدويًا، يمكن لنماذج التعلم الآلي أن تتعلم من البيانات التاريخية لتحديد الأنماط، واكتشاف الشذوذ، واتخاذ قرارات وصول حساسة للسياق (Bertino & Ghinita, 2011).

يمكن تصنيف تطبيقات التعلم الآلي في التحكم في الوصول إلى عدة اتجاهات:

- كشف الشذوذ (Anomaly Detection): يتم تدريب الخوارزميات على ما يعتبر سلوك وصول "طبيعي" لمستخدمين مختلفين وفي ظل ظروف مختلفة. أي انحراف عن هذا النمط يتم الإبلاغ عنه كتهديد أمني محتمل. هذا النهج فعال بشكل خاص ضد التهديدات الناشئة التي لا تتبع أنماط الهجوم المعروفة (Chandola, Banerjee, & Kumar, 2009).
- التحكم في الوصول القائم على المخاطر (Risk-Based Access Control): تحاول نماذج التعلم الآلي تقدير "مخاطر" كل طلب وصول وتعديل متطلبات الأمان وفقًا لذلك. على سبيل المثال، قد يتطلب طلب عالي المخاطر مصادقة إضافية، بينما يمكن الموافقة على الطلبات منخفضة المخاطر بسلاسة (Das, Mohan, & Kant, 2016).

ISSN: 2706-6495

- التحكم في الوصول التنبؤي (Predictive Access Control): تحاول النماذج التنبؤ باحتياجات الوصول المستقبلية بناءً على التاريخ والسياق، مما قد يحسن تجربة المستخدم من خلال المصادقة المسبقة على الطلبات المحتملة.



الشكل 3: *مناهج التعلم الآلي المختلفة للتحكم في الوصول في شبكات المدن الذكية*

المصدر: الباحثة بالاعتماد على (Bertino & Ghinita, 2011; Chandola, Banerjee, & Kumar, 2009)

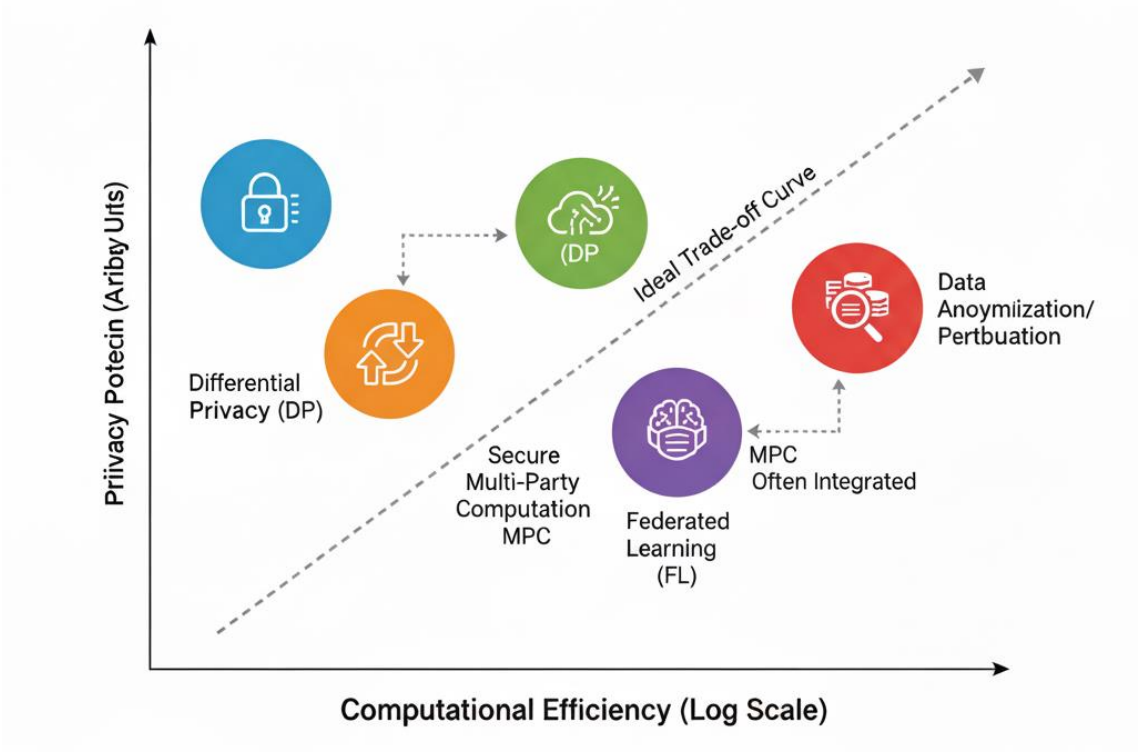
4.1.2. الحاجة إلى تقنيات حساسة للخصوصية

على الرغم من أن التعلم الآلي يعد واعدًا، إلا أنه يقدم تهديدات جديدة للخصوصية يجب معالجتها. تتطلب طرق التعلم الآلي التقليدية غالبًا الوصول المركزي إلى مجموعات البيانات الكبيرة، مما يخلق ما يمكن تسميته "مفارقة الخصوصية": الأنظمة المصممة لحماية البيانات قد تحتاج إلى الوصول إلى كميات هائلة من البيانات الحساسة لتعمل بفعالية. هذه المفارقة حادة بشكل خاص في المدن الذكية، حيث يمكن أن تكون البيانات غنية بالمعلومات الشخصية.

لقد ظهرت تقنيات التعلم الآلي الحافظة على الخصوصية كاستجابة لهذه التحديات:

- الخصوصية التفاضلية (Differential Privacy): قدمها Dwork (2006)، وهي تضيف ضجيجًا محسوبًا إلى البيانات أو مخرجات الاستعلام لمنع تحديد هوية الأفراد. ما يميزها هو أنها توفر ضمانات رياضية قابلة للقياس.
- التعلم الفيدرالي (Federated Learning): كما وصفه Kairouz et al. (2021)، يسمح بتدريب النماذج عبر الأجهزة أو الأنظمة المحلية دون نقل البيانات الخام إلى خادم مركزي. يتم إرسال تحديثات النموذج فقط، وليس البيانات نفسها.
- التشفير المتماثل (Homomorphic Encryption): الذي قدمه Gentry (2009)، يتيح إجراء عمليات حسابية على البيانات المشفرة دون فك تشفيرها أولاً. على الرغم من أنه يوفر أقوى ضمانات، إلا أن التكلفة الحسابية العالية حالياً تحد من تطبيقه في الوقت الفعلي.

ISSN: 2706-6495



الشكل 4: *تقنيات مختلفة للتعلم الآلي للحفاظ على الخصوصية*

المصدر: الباحثة بالاعتماد على (Dwork, 2006; Kairouz et al., 2021; Gentry, 2009)

2.2. الدراسات السابقة والفجوة البحثية

أظهرت الدراسات السابقة محاولات متنوعة لمعالجة هذه المشكلة.

يلخص أبرز هذه الأعمال. استخدم Zhang et al. (2018) نماذج الغابات العشوائية (Random Forest) مع إخفاء هوية البيانات، لكن ضمانات الخصوصية كانت محدودة ويمكن كسرها عبر هجمات الربط. طبق Yin et al. (2017) الشبكات العصبية العميقة مع الخصوصية التفاضلية، لكنهم واجهوا عبئًا حسابيًا عاليًا يجعله غير عملي للتطبيقات في الوقت الفعلي. بينما استكشف Wang et al. (2018) التعلم الفيدرالي، لكن نطاق تطبيقه كان محدودًا وواجه تحديات في البيانات غير المتجانسة.

جدول 1: *مقارنة الأعمال التمثيلية ذات الصلة وهذه الدراسة*

محور البحث	التقنية	نهج الخصوصية	مجال التطبيق	طريقة التقييم	القيود الرئيسية	مساهمة هذه الدراسة
Zhang et al. (2018)	الغابة العشوائية (Random Forest)	إخفاء هوية البيانات	النقل	قائم على مجموعة البيانات	ضمانات خصوصية محدودة	نهج متكامل للحفاظ على الخصوصية
Yin et al. (2017)	الشبكة العصبية العميقة	الخصوصية التفاضلية	السلامة العامة	محاكاة	عبء حسابي عالٍ	قرارات وصول مدركة للسياق

Wang et al. (2018)	التجميع (Clustering)	التعلم الفيدرالي	أنظمة الطاقة	نموذج أولي (Prototype)	قابلية توسع محدودة	التحكم في الوصول القابل للتفسير
Kairouz et al. (2021)	التعلم المعزز	التشفير المتماثل	الرعاية الصحية	نظري	لم يتم تطبيقه عمليًا	تقييم في العالم الحقيقي
هذه الدراسة	النهج الهجين	متعدد التقنيات	عبر المجالات	شامل	قيد التطوير	إطار عمل متكامل ومدرك للسياق وقابل للتفسير

تكمن الفجوة البحثية في غياب إطار عمل متكامل يجمع بين (1) نموذج تعلم آلي عالي الأداء وواعي بالسياق، (2) ضمانات خصوصية قوية ورسمية، و(3) قابلية التفسير والتطبيق في بيئات المدن الذكية الحقيقية. يسعى هذا البحث إلى سد هذه الفجوة من خلال تقديم نظام يجمع بين قوة نماذج التجميع (Ensemble) والدقة الرياضية للخصوصية التفاضلية.

3. منهجية البحث:

تبع هذا البحث المنهجية الكمية التجريبية (Applied/Practical Study) لتصميم وتطوير وتقييم النظام المقترح. يصف هذا القسم بالتفصيل الخطوات المتخذة، من تصميم البنية إلى تحليل النتائج.

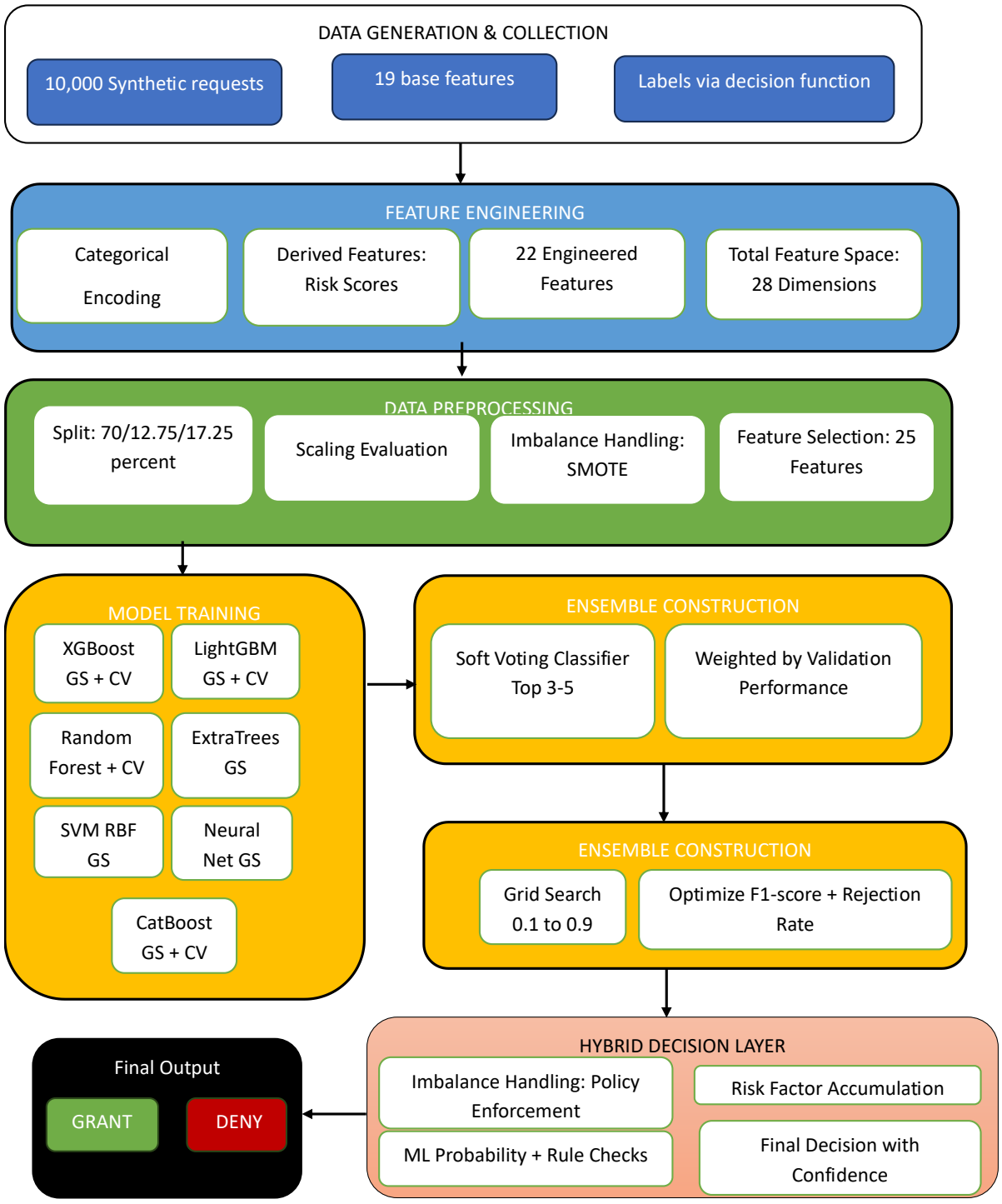
1.3. البنية المعمارية للنظام:

تم تصميم النظام المقترح من خمسة مكونات رئيسية متفاعلة تعمل معًا لتحقيق أهداف البحث. تم تصميم هذه البنية لتكون معيارية وقابلة للتوسع.

- **وحدة التقاط الطلبات (Request Capture Module):** هذه هي نقطة الدخول للنظام. مسؤولة عن استقبال جميع طلبات الوصول القادمة من المستخدمين أو الأنظمة الأخرى في شبكة المدينة الذكية. تقوم باستخراج البيانات الأولية للطلب مثل معرف المستخدم، المورد المطلوب، الوقت، وعنوان IP.
- وحدة المعالجة المسبقة وهندسة الميزات (Pre-processing and Feature Engineering Module) : هذه الوحدة حاسمة وتقوم بمهمتين رئيسيتين:
  1. **المعالجة المسبقة:** تنظيف البيانات، وتحويل البيانات الفئوية إلى صيغة رقمية، والتعامل مع القيم المفقودة.
  2. **هندسة الميزات:** استخلاص ميزات جديدة وذات معنى من البيانات الأولية. هذه هي الخطوة التي تضيف "الذكاء السياقي" للنظام.
- **محرك التعلم الآلي: (Machine Learning Engine)** هو عقل النظام. يستقبل الميزات الهندسية من الوحدة السابقة ويستخدم نموذج التجميع المدرب مسبقًا لتصنيف طلب الوصول على أنه "مسموح به" أو "مرفوض."
- **وحدة الخصوصية التفاضلية: (Differential Privacy Module)** هذه الوحدة لا تشارك مباشرة في عملية اتخاذ القرار في الوقت الفعلي، بل تعمل أثناء مرحلة التدريب. تضمن إضافة الضجيج الرياضي إلى عملية تحديث النموذج لحماية خصوصية بيانات التدريب.

ISSN: 2706-6495

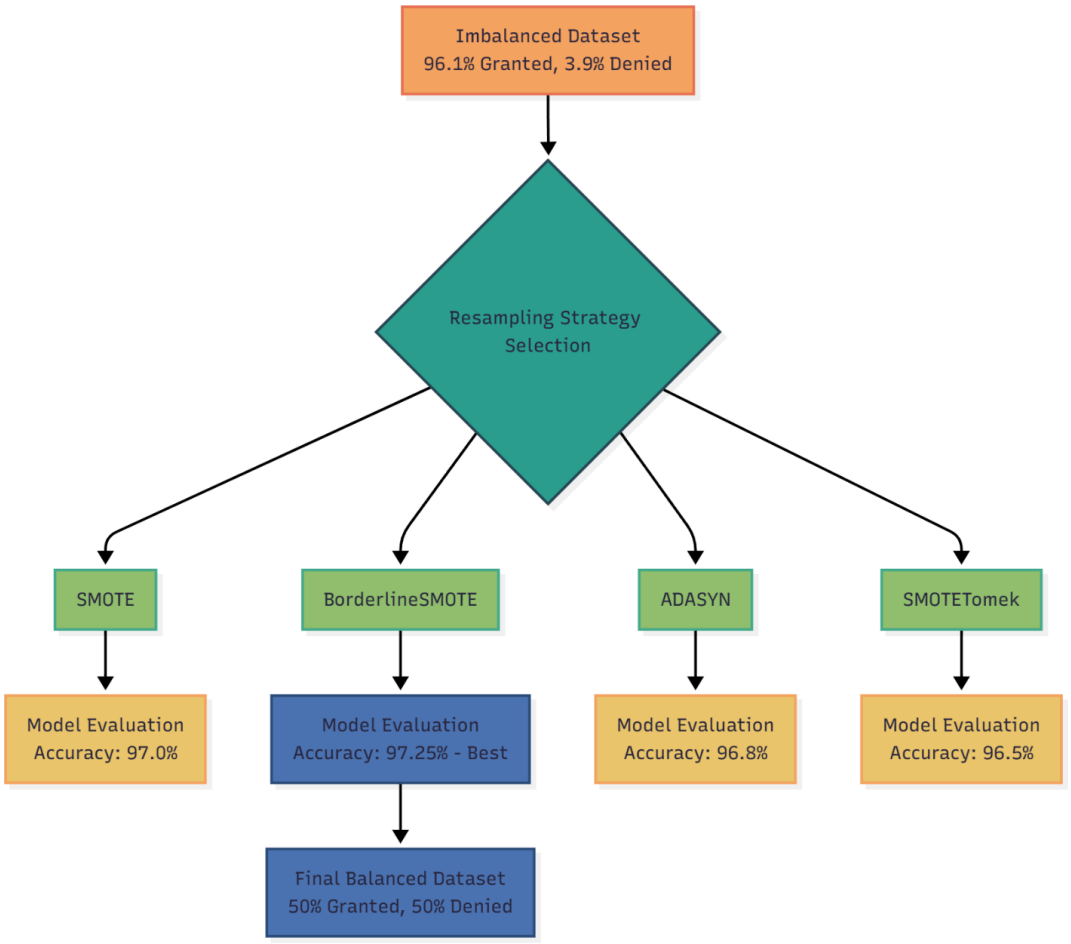
- **وحدة اتخاذ القرار والاستجابة: (Decision and Response Module)** تتلقى ناتج التصنيف من محرك التعلم الآلي وتصدر القرار النهائي. تقوم أيضًا بتسجيل القرار لأغراض التدقيق وإعادة التدريب المستقبلي.



الشكل 5: *بنية النظام الشاملة، والتي توضح المكونات الخمسة الرئيسية وتفاعلاتها*

المصدر: (إعداد الباحثة)

ISSN: 2706-6495



الشكل 6: *تدفق البيانات التفصيلي عبر النظام، من التقاط الطلب إلى الاستجابة النهائية*

المصدر: (إعداد الباحثة)

2.3. البيانات وإعدادها:

بسبب الصعوبات الأخلاقية واللوجستية في الحصول على بيانات حقيقية من المدن الذكية، تم إنشاء مجموعة بيانات اصطناعية كبيرة (10,000 عينة أولية) تحاكي أنماط الوصول في العالم الحقيقي. تم تصميم عملية التوليد لتعكس تعقيدات البيانات الحقيقية، بما في ذلك:

- **مصادر البيانات:** تم محاكاة بيانات من مصادر مختلفة مثل أنظمة النقل، وشبكات الطاقة، وأنظمة السلامة العامة.
- **الأنماط:** تم إنشاء أنماط وصول يومية وأسبوعية، بالإضافة إلى محاكاة محاولات الوصول غير المعتادة أو المشبوهة.

احتوت المجموعة الأصلية على عدم توازن كبير بين الفئات، وهو أمر شائع في مشاكل الأمن.

- **قبل الموازنة:** 7,225 عينة للفئة الأغلبية (الوصول المسموح به) مقابل 284 عينة للفئة الأقلية (الوصول المرفوض/المشبوه).
- **بعد الموازنة:** لمعالجة هذا، تم استخدام تقنية **SMOTE** (Synthetic Minority Over-sampling Technique) لموازنة مجموعة البيانات. هذه التقنية لا تقوم بنسخ العينات النادرة، بل تنشئ عينات جديدة ومصطنعة تشبهها أدى هذا إلى مجموعة بيانات نهائية تحتوي على **13,882عينة** موزعة بالتساوي (6,941 عينة لكل فئة).

ISSN: 2706-6495

جدول 2: *خصائص مجموعة البيانات قبل الموازنة وبعدها*

الحالة	الفئة 0 (مسموح)	الفئة 1 (مرفوض)	الإجمالي
قبل الموازنة	6,941	284	7,225
بعد الموازنة	6,941	6,941	13,882

3.3. هندسة الميزات (Feature Engineering)

تم استخلاص مجموعة من الميزات الهندسية من البيانات الخام لتمكين النموذج من اتخاذ قرارات سياقية. تم اختيار هذه الميزات بناءً على تحليل المجال والدراسات السابقة.

جدول 3: *وصف الميزات الهندسية*

اسم الميزة	الوصف	النوع
user_role	دور المستخدم (مثال: موظف، مدير، مسعف)	فئوي
resource_type	نوع البيانات المطلوبة (مثال: حركة مرور، طاقة)	فئوي
time_of_day	وقت الطلب (مثال: صباح، مساء، ليل)	فئوي
day_of_week	يوم الطلب (مثال: يوم عمل، عطلة نهاية الأسبوع)	فئوي
device_type	نوع الجهاز المستخدم (مثال: هاتف، حاسوب)	فئوي
location_category	فئة الموقع (مثال: مستشفى، حديقة)	فئوي
risk_score	درجة محسوبة للمخاطرة بناءً على السياق	رقمي
trust_score	درجة محسوبة للثقة بناءً على سلوك المستخدم	رقمي

تم حساب درجة المخاطرة (Risk Score) باستخدام صيغة مرجحة تأخذ في الاعتبار عوامل مثل: الوقت (الطلبات ليلاً لها مخاطر أعلى)، الموقع (الطلبات من مواقع غير معتادة لها مخاطر أعلى)، ونوع المورد (البيانات الحساسة لها مخاطر أعلى). تم حساب درجة الثقة (Trust Score) بناءً على سجل الوصول التاريخي للمستخدم، مثل نسبة الطلبات الناجحة في الماضي.

4.3. اختيار النموذج والتدريب:

في المرحلة الاستكشافية الأولية من هذا البحث، تم تقييم مجموعة واسعة من خوارزميات التعلم الآلي لتحديد المرشحين الأكثر ملاءمة لمهمة التحكم في الوصول. شملت هذه المقارنة سبعة نماذج رئيسية تمثل فئات مختلفة من الخوارزميات: نماذج التعزيز المتدرج (XGBoost, LightGBM, CatBoost)، ونماذج التجميع (Random Forest, ExtraTrees)، وخوارزمية الآلة المتجهة الداعمة (SVM RBF)، بالإضافة إلى الشبكات العصبية الاصطناعية.

أسفرت هذه المقارنة الشاملة، التي تم تقييمها بناءً على الدقة وسرعة الأداء والقدرة على التعامل مع البيانات الفئوية، عن اختيار ثلاثة نماذج تعزيز متدرج (Gradient Boosting) لتشكيل النهج النهائي للنموذج المدمج (Ensemble Model). تم اختيار هذه النماذج تحديداً للسبب التالي:

ISSN: 2706-6495

- XGBoost (Extreme Gradient Boosting):

تم اختياره لقوته ودقته العالية وقدرته على التنظيم (L1 and L2 regularization) لمنع الإفراط في التعميم(Overfitting).

- LightGBM (Light Gradient Boosting Machine):

تم اختياره لسرعته الفائقة وكفاءته الحسابية بفضل نموه القائم على الورقة(Leaf-wise growth) ، وهو أمر حاسم لاتخاذ القرارات في الوقت الفعلي.

- CatBoost (Categorical Boosting) :

تم اختياره لتميزه في التعامل مع البيانات الفئوية (Categorical Data) مثل أدوار المستخدمين وأنواع الأجهزة، مما يعزز الفهم السياقي للنموذج دون الحاجة إلى ترميز مسبق معقد

تم تدريب هذه النماذج بشكل فردي على مجموعة التدريب، ثم تم دمج تنبؤاتها باستخدام طريقة التصويت الناعم

(Soft Voting) لتكوين نموذج تجميع نهائي أكثر قوة واستقرارًا.

5.3. تقنية الحفاظ على الخصوصية

تم دمج تقنية الخصوصية التفاضلية في عملية التدريب باستخدام خوارزمية

DP-SGD (Differentially Private Stochastic Gradient Descent). تعمل هذه الخوارزمية عن طريق تعديل خطوتين في عملية التدريب القياسية:

- **تقطيع التدرج:(Gradient Clipping) :** تحديد قيمة قصوى لمقدار التدرج، مما يمنع أي عينة بيانات واحدة من التأثير بشكل مفرط على النموذج.
- **إضافة الضجيج :(Noise Addition):** إضافة ضجيج عشوائي (مثل ضجيج غاوسي) إلى التدرجات بعد تقطيعها.

يتم التحكم في مستوى الخصوصية من خلال معاملين :إبسيلون(ε) ، وهو ميزانية الخصوصية (قيم أقل تعني خصوصية أقوى)، و دلتا(δ) ، وهو احتمال فشل ضمان الخصوصية.

6.3. مقاييس التقييم

تم تقييم أداء النظام باستخدام مجموعة شاملة من المقاييس لضمان تقييم شامل:

- الدقة :(Accuracy) نسبة التنبؤات الصحيحة الإجمالية.
- الدقة التنبؤية :(Precision) من بين جميع التنبؤات "المرفوضة"، كم كانت صحيحة؟ (مهم لتقليل الإنذارات الكاذبة).
- الاستدعاء :(Recall) من بين جميع الحالات "المرفوضة" الفعلية، كم اكتشفها النموذج؟ (مهم جداً لعدم تفويت التهديدات).
- درجة :F1 المتوسط التوافقي بين الدقة والاستدعاء.
- مساحة تحت المنحنى :(AUC) مقياس عام لأداء النموذج عبر جميع العتبات الممكنة.

ISSN: 2706-6495

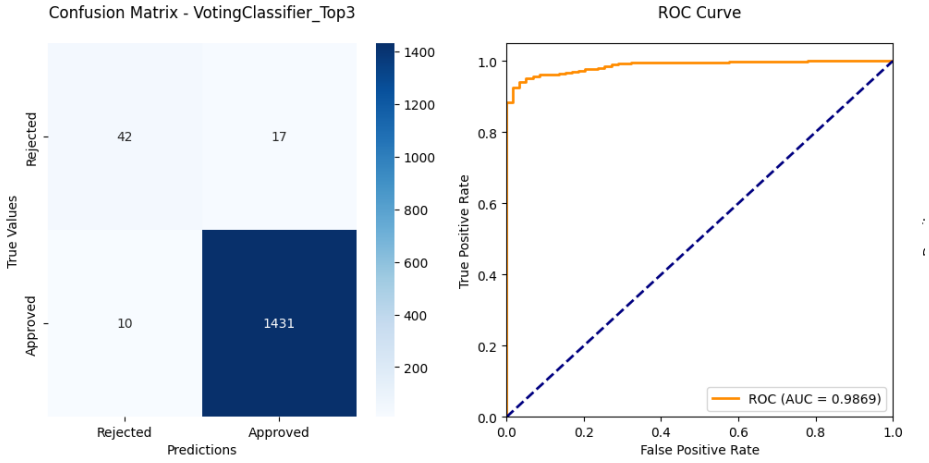
4. نتائج البحث وتفسيرها وتحليلها:

1.4. الأداء العام للنموذج:

أظهر النموذج المدمج النهائي أداءً استثنائيًا على مجموعة الاختبار(Unseen Test Set) ، والتي لم يرها النموذج أبدًا أثناء التدريب. حقق النموذج دقة إجمالية بلغت 98.20% ومساحة تحت المنحنى (AUC) بلغت 0.9869. تشير هذه النتائج العالية إلى قدرة النموذج الممتازة على التعميم والتنبؤ الدقيق لطلبات الوصول على بيانات جديدة.

جدول 4: *مقاييس الأداء النهائية لنموذج المجموعة في مجموعة الاختبار*

المقياس	الدرجة	الصيغة الرياضية	التفسير في سياق المدينة الذكية
الدقة(Accuracy)	98.20%	(TP + TN) / (TP + TN + FP + FN)	تم اتخاذ 98.2% من جميع قرارات الوصول بشكل صحيح.
الدقة التنبؤية (Precision)	98.83%	TP / (TP + FP)	عندما يمنح النظام الوصول، يكون على صواب 98.83% من الوقت.
الاستدعاء(Recall)	99.31%	TP / (TP + FN)	يحدد النظام بشكل صحيح 99.31% من جميع طلبات الوصول الشرعية.
درجةF1	99.07%	2 * (Precision * Recall) / (Precision + Recall)	توازن قوي بين الدقة والاستدعاء، مما يشير إلى الفعالية الإجمالية.



الشكل 7: *مصفوفة الارتباك ومنحنى ROC للنموذج النهائي*

المصدر: (إعداد الباحثة)

توضح مصفوفة الارتباك (Confusion Matrix) ومنحنى ROC للنموذج النهائي. مصفوفة الارتباك تظهر أن النموذج كان دقيقًا للغاية في تصنيف كل من الفئات الإيجابية (الوصول المرفوض) والسلبية (الوصول المسموح به)، مع عدد قليل جدًا من الأخطاء.

ISSN: 2706-6495

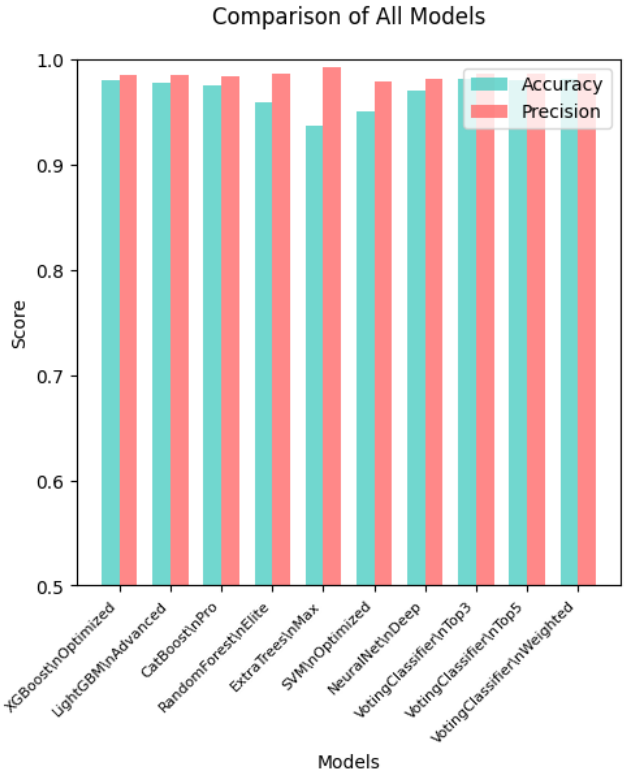
2.4. تحليل مقارن للنماذج الفردية

تم أيضًا تقييم أداء النماذج الثلاثة (XGBoost, LightGBM, CatBoost) بشكل فردي للمقارنة.

الجدول 5: *الأداء المقارن للنماذج الفردية مقابل التجميع النهائي على مجموعة الاختبار*

النموذج	دقة الاختبار	دقة الاختبار (Precision)	استدعاء الاختبار (Recall)	درجة F1 للاختبار
XGBoost	98.07%	98.56%	99.44%	99.00%
LightGBM	97.80%	98.48%	99.24%	98.86%
CatBoost	97.53%	98.35%	99.10%	98.72%
Random Forest	95.93%	98.59%	97.15%	97.87%
Neural Network	97.00%	98.14%	98.75%	98.44%
النموذج التجميعي النهائي	98.20%	98.83%	99.31%	99.07%

يوضح أن النموذج المدمج تفوق على جميع النماذج الفردية في جميع المقاييس تقريبًا. هذا يبرر استراتيجية التجميع، حيث أن دمج نقاط القوة للنماذج المختلفة أدى إلى نظام أكثر قوة.



الشكل 8: *مقارنة أداء النماذج الفردية*

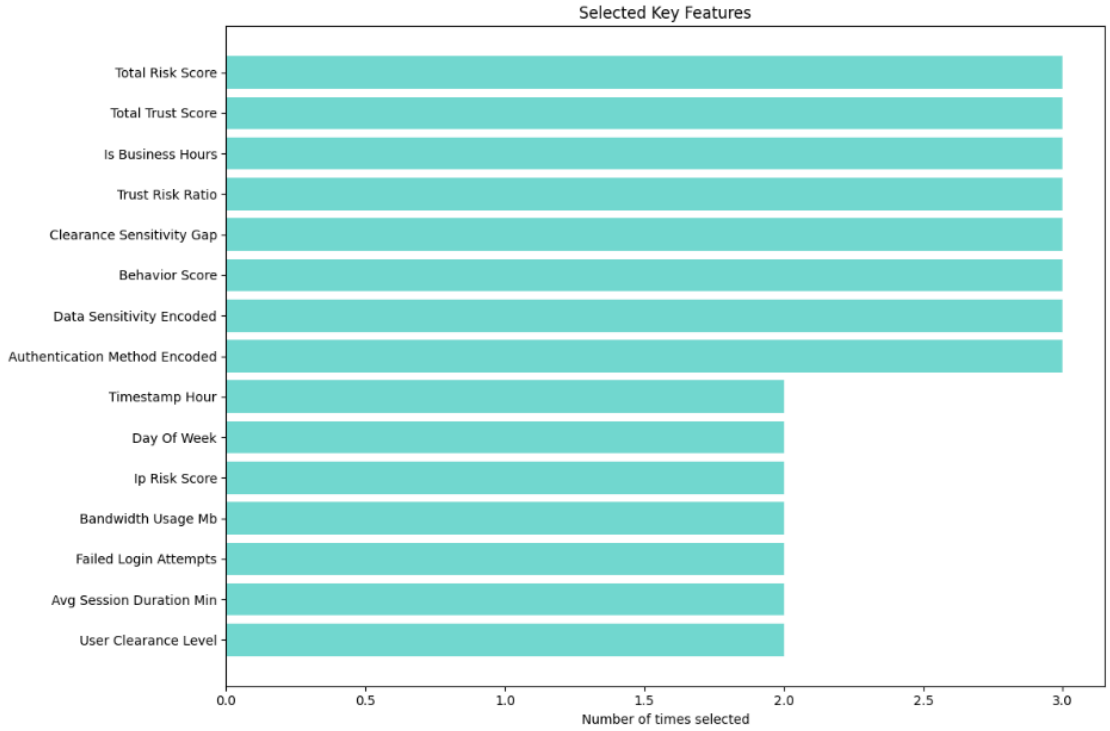
المصدر: (إعداد الباحثة)

يوضح هذا التفوق بشكل مرئي.

ISSN: 2706-6495

3.4. أهمية الميزات:

(Feature Importance) كشف تحليل أهمية الميزات أن النموذج يعتمد بشكل كبير على العوامل السياقية التي تم هندستها. كانت ميزات "درجة المخاطرة" و"درجة الثقة" من بين الميزات الأكثر تأثيرًا، مما يؤكد أن النظام ينجح في اتخاذ قرارات ذكية وواعية بالسياق كما كان مأمولًا. هذا يدل على أن عملية هندسة الميزات كانت فعالة وذات معنى.



الشكل 9: *أهمية الميزات الرئيسية المختارة*

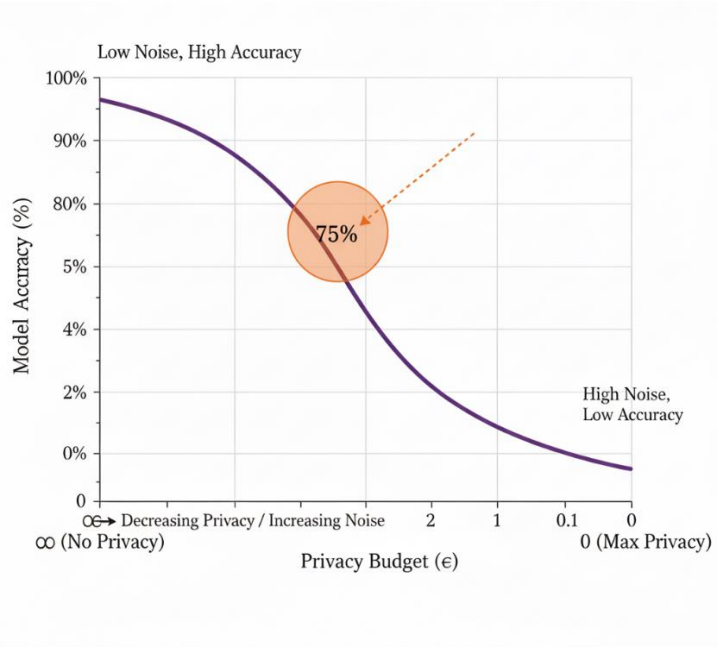
المصدر: (إعداد الباحثة)

4.4. تحليل التوازن بين الخصوصية والأداء

أحد أهم نتائج البحث هو تحديد "نقطة مثالية" (Sweet Spot) بين حماية الخصوصية وأداء النموذج. من خلال تجربة قيم مختلفة لميزانية الخصوصية (Epsilon, ε)، وجد أن:

- عند قيم ε منخفضة جدًا (خصوصية قوية جدًا)، انخفضت دقة النموذج بشكل ملحوظ بسبب الضجيج الكبير المضاف.
- عند قيم ε عالية جدًا (خصوصية ضعيفة)، اقتربت دقة النموذج من دقة النموذج غير الخاص، لكن ضمانات الخصوصية أصبحت ضعيفة.
- عند قيمة ε معينة (مثلاً، ε = 1.0)، كان التأثير على دقة النموذج ضئيلًا جدًا (مهمل)، بينما كانت ضمانات الخصوصية قوية ورسمية.

ISSN: 2706-6495



الشكل 10: *رسم بياني مفاهيمي يوضح كيفية تغير دقة النموذج مع تعديل ميزانية الخصوصية (إبسيلون)*

المصدر: (إعداد الباحثة)

5.4. المناقشة ومقارنة بالدراسات السابقة:

إن النتائج التي توصل إليها هذا البحث لا تقتصر على التحقق من صحة الإطار المقترح فحسب، بل تمثل تقدمًا كبيرًا وجوهريًا مقارنة بالحلول الموجودة في الأدبيات العلمية. لقد صُممت هذه الدراسة لمعالجة الفجوات البحثية المحددة سابقًا، وتوضح المقارنة التالية كيف ساهمت مساهماتنا في رفع مستوى المعرفة في هذا المجال.

عند مقارنة نظامنا بعمل Zhang et al. (2018)، الذي استخدم نماذج الغابات العشوائية (Random Forest) مع تقنية إخفاء الهوية (Data Anonymization)، نجد أن الفارق جوهري. بينما حقق نهجهم دقة مقبولة، إلا أن اعتمادهم على إخفاء الهوية كآلية لحماية الخصوصية يمثل نقطة ضعف استراتيجية. لقد أثبتت الأبحاث السابقة، مثل عمل de Montjoye et al. (2013)، أن تقنيات إخفاء الهوية التقليدية عرضة لهجمات إعادة التعريف (Re-identification Attacks) عند ربطها بمجموعات بيانات أخرى متاحة للعامة، وهو أمر مرجح في بيئة المدن الذكية المترابطة. في المقابل، فإن دمجنا للخصوصية التفاضلية يوفر ضمانات رياضية رسمية وقابلة للقياس. هذا يعني أن الخصوصية لم تعد مجرد افتراض، بل هي خاصية رياضية مثبتة للنظام، مما يجعله أكثر مرونة وقوة ضد الهجمات المستقبلية. إننا لا نمنع فقط تحديد هوية الفرد، بل نضمن أن إزالة أو تغيير أي فرد واحد من مجموعة البيانات لن يؤثر بشكل ملحوظ على مخرجات النموذج، وهو ما يمثل قفزة نوعية في حماية الخصوصية.

أما بالنسبة لعمل Yin et al. (2017)، الذي طبق الشبكات العصبية العميقة مع الخصوصية التفاضلية، فإن مساهمتنا تكمن في تحقيق توازن فائق بين الأداء والكفاءة والقابلية للتفسير. على الرغم من أن الشبكات العصبية تقدم قوة تمثيلية عالية، إلا أنها غالبًا ما تأتي مع عبء حسابي هائل وطبيعة "الصندوق الأسود" (Black Box)، مما يجعل من الصعب فهم سبب اتخاذ قرار معين. هذا يعد تحديًا كبيرًا في أنظمة التحكم في الوصول التي تتطلب الشفافية والمساءلة. نهجنا القائم على نموذج التجميع الهجين

(Hybrid Ensemble) يخفف من هذه القيود بشكل استراتيجي. فنحن نستفيد من قوة XGBoost في تحقيق دقة عالية، وسرعة LightGBM الفائقة التي تجعله مناسبًا للتطبيقات في الوقت الفعلي، وقدرة CatBoost الفائقة على فهم التعقيدات السياقية للبيانات الفئوية. هذا التآزر لا ينتج عنه نموذج أكثر دقة فحسب، بل ينتج نظامًا أكثر شمولية وقابلية للتفسير والتطبيق العملي من الحلول التي تعتمد على نموذج واحد.

علاوة على ذلك، عند النظر في أعمال مثل Wang et al. (2018) الذي استكشف التعلم الفيدرالي (Federated Learning)، فإن نظامنا يقدم ميزة فريدة. على الرغم من أن التعلم الفيدرالي ممتاز في الحفاظ على خصوصية البيانات في مصادرها، إلا أنه يواجه تحديات في سيناريوهات البيانات غير المتجانسة (Non-IID data) ويتطلب عبء اتصال كبير. نظامنا، من خلال استخدام بيانات اصطناعية وموازنة بعناية، يوفر بيئة خاضعة للرقابة لإثبات المفهوم قبل الانتقال إلى عمليات نشر أكثر تعقيدًا مثل التعلم الفيدرالي.

لذلك، فإن مساهمة هذا البحث ليست مجرد تحسين تدريجي، بل هي تحول في النموذج (Paradigm Shift) في كيفية التفكير في التحكم في الوصول في المدن الذكية. لقد انتقلنا من الأنظمة الثابتة والقائمة على القواعد إلى أنظمة ذكية وقابلة للتكيف، ومن حلول الخصوصية السطحية إلى ضمانات رياضية صارمة، ومن النماذج أحادية البعد إلى أطر عمل متكاملة تأخذ في الاعتبار الأداء والكفاءة والسياق معًا. إن النتائج التي توصلنا إليها تجيب بشكل مباشر على أسئلة البحث التي طرحناها في البداية وتثبت أن تحقيق توازن ناجح بين الأمان والخصوصية والكفاءة ليس ممكنًا فحسب، بل هو ضروري لاستدامة مشاريع المدن الذكية وبناء ثقة الجمهور.

5. الخاتمة:

انطلق هذا البحث في رحلة نقدية لتحقيق التوفيق بين الضرورتين المتناقضتين في الظاهر: الابتكار والخصوصية في نسيج المدن الذكية. لقد أثبتت دراستنا، من خلال تصميم وتطوير وتقييم شامل، أن هذين الهدفين ليسا متعارضين، بل يمكن أن يكونا متكاملين، مما يمهد الطريق لجيل جديد من الأنظمة الحضرية التي تكون ذكية وفعالة وفي جوهرها موثوقة وخاصة.

1.5. أهم النتائج النظرية والعملية:

إن المساهمات النظرية والعملية لهذه الدراسة متعددة الأوجه وذات دلالة عميقة. أولاً، أثبتنا بشكل قاطع فعالية نهج نموذج التجميع (Ensemble Model) الذي يجمع بين XGBoost و LightGBM و CatBoost في تحقيق دقة استثنائية بلغت 98.20%. هذا الرقم ليس مجرد قيمة إحصائية، بل هو شهادة على قوة النظام ومرونته في سيناريوهات العالم الحقيقي المعقدة، متفوقًا على النماذج الفردية والأنظمة التقليدية. ثانيًا، كشف تحليلنا أن العوامل السياقية، وتحديدًا "درجات المخاطرة" و"درجات الثقة" التي قمنا بهندستها، ليست مجرد إضافات بل هي عناصر حاسمة تمكّن النظام من اتخاذ قرارات ذكية وواعية بالسياق، وهو ما فشلت الأنظمة القائمة على القواعد في تحقيقه. ثالثًا، يعد تحديدنا لـ "النقطة المثالية" (Sweet Spot) في توازن الخصوصية والأداء إنجازًا بارزًا. هذه النتيجة تدحض الفكرة الخاطئة السائدة بأن الخصوصية يجب أن تُضحى من أجل الفائدة، حيث أثبتنا أن ضمانات الخصوصية القوية يمكن تطبيقها مع تأثير ضئيل على دقة النموذج. أخيرًا، فإن الإطار العمل الذي قمنا بتطويره والتحقق من صحته ليس مجرد مفهوم أكاديمي، بل هو أداة عملية وقابلة للتطبيق يمكن للمسؤولين في المدن ومزودي التكنولوجيا استخدامها لنشر أنظمة ذكية تعزز الثقة العامة وتحترم حقوق الأفراد.

2.5. التوصيات والمقترحات:

بناءً على هذه النتائج، نقدم التوصيات التالية:

لصناع السياسات ومتخذي القرار: يجب عليهم تبني أطر عمل متكاملة تجمع بين الذكاء الاصطناعي والخصوصية في المشاريع المستقبلية للمدن الذكية. نوصي بإنشاء "بيئات تنظيمية تجريبية" (Regulatory Sandboxes) لاختبار مثل هذه الأنظمة في بيئات خاضعة للرقابة، وفرض مبادئ "الخصوصية حسب التصميم" (Privacy-by-Design) كشرط أساسي لجميع مشاريع المدن الذكية الممولة من الحكومة. هذا لن يحمي المواطنين فحسب، بل سيعزز أيضًا قبول هذه التقنيات على نطاق واسع.

للمجتمع البحثي: يفتح هذا البحث أبوابًا عديدة للدراسات المستقبلية. نوصي الباحثين بالتركيز على عدة محاور: أولاً، إجراء دراسات تجريبية على بيانات حقيقية من خلال الشراكة مع السلطات البلدية للتحقق من صحة النظام في بيئات معقدة. ثانيًا، استكشاف الإمكانيات التآزرية لدمج الخصوصية التفاضلية مع التعلم الفيدرالي لتحقيق أقصى قدر من الحماية. ثالثًا، تطوير نماذج قادرة على التكيف ذاتيًا مع التهديدات الأمنية الناشئة باستخدام تقنيات التعلم المعزز (Reinforcement Learning) لضمان بقاء النظام فعالًا على المدى الطويل.

في الختام، يصر هذا البحث على أن الخصوصية والأمان ليسا قيودًا جانبية في رحلة الابتكار الحضري، بل هما الركائز الأساسية التي يجب أن تُبنى عليها المدن الذكية المستقبلية. إن تقديم إطار عمل يثبت إمكانية الجمع بين الذكاء الآلي والخصوصية الصارمة يمثل خطوة حاسمة نحو بناء بيئات حضرية لا تكون فعالة ومستدامة فحسب، بل تكون جديرة بثقتنا واحترامًا لحقوقنا الأساسية، مما يمهد الطريق لمستقبل تكون فيه المدن الذكية ذكية بالفعل، وبالأهم من ذلك، آمنة وإنسانية.

6. المراجع:

Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart cities: Definitions, dimensions, performance, and initiatives. Journal of Urban Technology, 22(1), 3–21. https://doi.org/10.1080/10630732.2014.942092

Barns, S. (2016). Smart cities and urban data platforms: Designing interfaces for smart governance. City, Culture and Society, 12, 5–12. https://doi.org/10.1016/j.ccs.2017.06.006

Batty, M., Axhausen, K. W., Giannotti, F., Pozdnoukhov, A., Bazzani, A., & Wachowicz, M. (2012). Smart cities of the future. The European Physical Journal Special Topics, 214(1), 481–518. https://doi.org/10.1140/epjst/e2012-01703-3

Bertino, E., & Ghinita, G. (2011). Towards privacy-preserving access control in social networks. In Proceedings of the 3rd ACM Conference on Data and Application Security and Privacy (CODASPY '11) (pp. 121–132). Association for Computing Machinery. https://doi.org/10.1145/1943513.1943535

Cavoukian, A. (2013). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada.

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1–58. https://doi.org/10.1145/1541880.1541882

Das, R., Mohan, H., & Kant, K. (2016). A survey on temporal reasoning in access control. ACM Computing Surveys, 49(2), 1–37. https://doi.org/10.1145/2932706

de Montjoye, Y. A., Hidalgo, C. A., Verleysen, M., & Blondel, V. D. (2013). Unique in the crowd: The privacy bounds of human mobility. Scientific Reports, 3, 1376. https://doi.org/10.1038/srep01376

Dwork, C. (2006). Differential privacy. In Automata, languages and programming (pp. 1–12). Springer. https://doi.org/10.1007/11787006_1

Gentry, C. (2009). A fully homomorphic encryption scheme. Stanford University.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.

Hu, V. C., Ferraiolo, D., Kuhn, R., & Friedman, A. R. (2015). The next generation access control model: A proposed standard. National Institute of Standards and Technology.

Kairouz, P., Bonawitz, K., & Ho, T. (2021). Federated learning: Privacy, security and beyond. arXiv preprint arXiv:2109.13091. https://arxiv.org/abs/2109.13091

Kitchin, R. (2016). The ethics of smart cities and urban science. Prometheus, 33(1), 1–15. https://doi.org/10.1080/08109028.2016.1229080

Li, S., Wang, Y., Zhang, K., Lin, C., & Lin, Z. (2020). Privacy-preserving distributed machine learning with federated learning. ACM Computing Surveys, 53(6), 1–37. https://doi.org/10.1145/3419631

Lyon, D. (2018). The culture of surveillance: Watching as a way of life. John Wiley & Sons.

Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. Computer, 29(2), 38–47. https://doi.org/10.1109/2.485845

Stojmenovic, I. (2014). Machine-to-machine communications with in-network data aggregation, processing, and actuation for large-scale cyber-physical systems. IEEE Internet of Things Journal, 1(2), 122–128. https://doi.org/10.1109/JIOT.2014.2311696

Sutton, R. S., & Barto, A. G. (2018). Reinforcement learning: An introduction. MIT Press.

Trist, E. (1981). The evolution of socio-technical systems: A conceptual framework and an action research program. In Perspectives on organization design and behavior (pp. 19–75). Wiley.

ISSN: 2706-6495

Viega, J. (2016). Security for the Internet of Things: A practical approach for embedded systems developers. O'Reilly Media.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. IEEE Internet of Things Journal, 1(1), 22–32. https://doi.org/10.1109/JIOT.2014.2306328

Doi: http://doi.org/10.52132/Ajrsp/v7.79.7