Gestion des données de l'Internet des objets axée sur la qualité

Moez Krichen

Gestion des données de l'Internet des objets axée sur la qualité

Moez Krichen

Laboratoire ReDCAD, Université de Sfax, Tunisie
moez.krichen@redcad.org

Résumé. La prolifération des appareils Internet des objets (IdO) a marqué le début d'une ère de prise de décision basée sur les données dans divers secteurs. Cet article présente un examen complet des avancées récentes dans la gestion des données IdO avec un accent particulier sur la qualité. Nous commençons par donner un aperçu des aspects fondamentaux tels que l'authentification, le chiffrement et les protocoles de communication sécurisés qui sous-tendent le traitement des données IdO. Par la suite, nous approfondissons les défis associés à la gestion des vastes ensembles de données générés par les déploiements IdO. L'article explore l'utilisation de l'informatique de pointe pour le traitement des données en temps réel et l'intégration de données synthétiques pour augmenter des ensembles de données limités. De plus, nous discutons de l'application de techniques d'apprentissage automatique pour une analyse approfondie des flux de données IdO, ainsi que des procédures d'évaluation de la qualité des données et des stratégies de détection des anomalies. Compte tenu de la nature limitée des ressources des écosystèmes IdO, une attention particulière est accordée aux solutions de transfert de données économes en énergie. L'article étudie également les mesures de sécurité complètes destinées à protéger les données sensibles, notamment les réglementations en matière de contrôle d'accès et l'utilisation de la technologie blockchain pour sécuriser l'accès aux données. De plus, nous fournissons un aperçu des tendances émergentes et des problèmes potentiels liés à la gestion des données IdO. Le rapport conclut en soulignant l'importance collective de ces progrès et en proposant de futures opportunités de recherche. Cette enquête approfondie vise à constituer une ressource précieuse pour les universitaires, les praticiens et les parties prenantes intéressés par le paysage évolutif de la gestion des données IdO, avec un accent particulier sur la garantie de la qualité des données.

1 Introduction

La prolifération des dispositifs de l'Internet des objets (IdO) a catalysé un changement transformateur dans la façon dont les données sont acquises, traitées et utilisées

dans divers domaines (65). Cette avancée technologique a inauguré une ère de connectivité sans précédent, facilitant les interactions fluides entre les mondes physique et numérique (91). Par conséquent, les écosystèmes IdO sont devenus des composantes indispensables des entreprises couvrant les secteurs de la santé, du transport, des villes intelligentes et de l'automatisation industrielle (54).

La gestion efficace des vastes ensembles de données dynamiques générés par les déploiements IdO est une condition préalable essentielle à leur efficacité (129). Ces ensembles de données, souvent caractérisés par leur volume, leur vitesse et leur variété, nécessitent des méthodologies complexes de stockage, de traitement et d'analyse (108). De plus, la protection de la sécurité et de l'intégrité des données sensibles au sein de ces systèmes en réseau revêt une importance capitale (82; 66).

Cet article propose une exploration complète des avancées actuelles dans la gestion des données de l'IdO, englobant un large spectre de domaines essentiels. Nous entamons ce voyage avec les principes fondamentaux de la gestion des données de l'IdO, notamment l'authentification robuste, le chiffrement et les protocoles de communication sécurisés, et nous plongeons dans les subtilités de la gestion de l'afflux de données provenant de sources de capteurs diverses.

L'intégration du calcul périphérique émerge en tant qu'innovation cruciale en tandem avec l'explosion des volumes de données (53). Cette décentralisation des ressources de calcul permet un traitement en temps réel au niveau de la source de données, réduisant ainsi considérablement la latence et les besoins en bande passante (129). De plus, la synthèse de données par le biais de modèles génératifs apparaît comme une stratégie potentielle pour améliorer les ensembles de données contraints, ouvrant la voie à une analyse plus précise et plus complète (108).

Les algorithmes d'apprentissage automatique, dotés de la capacité de découvrir des motifs significatifs au sein de flux de données complexes, jouent un rôle essentiel dans l'extraction d'informations précieuses à partir des ensembles de données de l'IdO (49). Le déploiement de techniques d'apprentissage automatique adaptées aux défis uniques présentés par les contextes de l'IdO est un point central de cette recherche (18). Il aborde également des préoccupations essentielles telles que l'évaluation de la qualité et la détection des anomalies, garantissant ainsi la fiabilité et l'intégrité des informations obtenues (19; 25).

Compte tenu des contraintes de ressources qui caractérisent de nombreux déploiements de l'IdO, il est impératif de privilégier des solutions de transmission de données économes en énergie (125). Nous explorons des approches innovantes pour optimiser la transmission des données tout en préservant la fidélité des données et en conservant les ressources (23). De plus, des mesures de sécurité strictes, telles que les politiques de contrôle d'accès et l'adoption de la technologie de la blockchain, font l'objet d'un examen approfondi pour se prémunir contre les accès non autorisés et les violations de données (68; 58; 88; 70; 55; 90; 57; 72; 56; 78; 79; 71; 87; 89; 73; 76; 62; 69).

Dans les sections suivantes, nous allons scruter l'horizon, examiner les tendances à venir et les défis potentiels de la gestion des données de l'IdO. Grâce à la fusion de ces réalisations, nous aspirons à dresser un portrait holistique du paysage actuel de la gestion des données de l'IdO et de ses implications étendues pour de nombreuses industries.

2 Préliminaires sur la gestion des données de l'IdO

L'Internet des objets (IdO) fait référence à un réseau en expansion rapide d'appareils et de capteurs interconnectés qui collectent et échangent des données, facilitant une large gamme d'applications et de services. La gestion efficace de la quantité substantielle de données produites par ces appareils pose une difficulté majeure dans ce domaine (102). Cette section abordera les principes fondamentaux et les complexités liées à la gestion des données dans le contexte de l'IdO.

2.1 Sources de données de l'IdO

Les données sont issues d'une diversité de sources, englobant des capteurs intégrés à une multitude de produits tels que des appareils électroménagers intelligents, des équipements industriels, des capteurs environnementaux et des gadgets portables (105). Les capteurs collectent de manière constante des données liées à plusieurs caractéristiques, notamment la température, l'humidité, la localisation et d'autres facteurs (116). Dans le contexte d'un environnement domestique intelligent, les sources de données comprennent divers appareils tels que des thermostats équipés de capteurs de température, des caméras de sécurité intégrant des capteurs de mouvement et des dispositifs portables dotés de moniteurs de fréquence cardiaque (105). Dans le domaine industriel, la collecte de données peut provenir de plusieurs sources, notamment des capteurs intégrés aux machines de production, des compteurs d'énergie et des traceurs GPS fixés aux véhicules de transport utilisés pour les livraisons. Une compréhension approfondie des différentes catégories et variations des sources de données à l'intérieur de l'IdO est cruciale pour élaborer des stratégies de gestion des données adaptées aux applications de l'IdO. Chaque capteur produit des données possédant des caractéristiques distinctes. Par exemple, les capteurs de température fournissent des données numériques continues, tandis que les capteurs d'image produisent de grands volumes de données d'image (116). L'identification de ces distinctions facilite la sélection de formats de stockage de données appropriés et de techniques de traitement (43).

2.2 Volume et vitesse des données

L'une des caractéristiques distinctives des données de l'IdO est leur ampleur considérable et leur rapidité (34). Les appareils produisent d'importants volumes de données à des intervalles rapides, ce qui pose des défis pour les solutions de gestion de données conventionnelles. La gestion de cet afflux de données nécessite l'utilisation de procédures et d'infrastructures spécifiques. Dans le cadre d'une situation hypothétique, imaginons un environnement urbain intelligent dans lequel le système de gestion du trafic acquiert efficacement des données auprès d'une multitude de capteurs de véhicules, de caméras de surveillance du trafic et de dispositifs GPS en temps voulu. Le volume de données généré a le potentiel de s'accumuler rapidement à l'échelle des téraoctets, voire des pétaoctets, dans un laps de temps relativement court. La gestion de grandes quantités de données implique l'utilisation de systèmes de stockage distribués et de cadres de traitement parallèle. La vitesse des données est également cruciale. Certaines applications de l'IdO nécessitent des réponses immédiates et rapides. Par exemple, les

véhicules autonomes dépendent du traitement des données en temps réel pour prendre des décisions éclairées en matière de conduite. Pour gérer efficacement les données de l'IdO, il est impératif que les systèmes de gestion des données aient la capacité d'analyser les flux de données avec une latence minimale. Les considérations relatives au volume et à la vitesse des données dans le contexte de l'IdO ont une influence significative sur la sélection des systèmes de stockage, des méthodes de compression des données et des pipelines de traitement pour la gestion des données de l'IdO.

2.3 Variété des données

Lesdonnées de l'IdO présentent une grande variété en termes de format, de structure et de représentation. Les capteurs peuvent produire des données de différents types, tels que des données numériques, des données textuelles, des données d'image et même des données audio. Par exemple, les capteurs de température peuvent fournir des données numériques continues, tandis que les caméras de surveillance peuvent générer des flux de données vidéo. En outre, les données de l'IdO peuvent avoir une structure complexe ou non structurée. Les données structurées sont organisées dans un format tabulaire avec des colonnes et des lignes, similaires à une base de données relationnelle (116). Par exemple, les données provenant d'un réseau de capteurs de pollution de l'air peuvent être organisées dans une structure tabulaire avec des colonnes pour les mesures de la qualité de l'air et des lignes pour les différents emplacements de capteurs. D'autre part, les données non structurées n'ont pas de format prédéfini et peuvent inclure des données textuelles, des flux de données en temps réel ou des données d'image et de vidéo brutes. La variété des données de l'IdO nécessite des techniques de gestion de données flexibles et évolutives capables de traiter différents formats et structures de données. Les systèmes de gestion de données de l'IdO doivent être adaptés pour prendre en charge ces différentes variétés de données et permettre leur intégration et leur traitement efficaces.

2.4 Véracité et valeur des données

La véracité des données de l'IdO fait référence à la fiabilité et à la précision des informations collectées. En raison de la nature distribuée et hétérogène de l'IdO, il peut y avoir des problèmes de qualité des données, tels que des erreurs de mesure, des valeurs aberrantes et des données manquantes. Il est essentiel de mettre en place des mécanismes de validation et de vérification des données pour garantir leur exactitude et leur fiabilité. Cela peut inclure des techniques telles que la surveillance de la qualité des données, la détection des valeurs aberrantes et la validation croisée avec d'autres sources de données fiables. La valeur des données de l'IdO réside dans leur capacité à fournir des informations exploitables et à prendre des décisions éclairées (34). Cependant, toutes les données générées par l'IdO ne sont pas nécessairement utiles ou pertinentes. Il est important de mettre en place des mécanismes d'analyse et d'extraction de connaissances pour extraire des informations précieuses à partir des données brutes. Cela peut impliquer l'utilisation de techniques d'apprentissage automatique, de l'intelligence artificielle ou de l'exploration de données pour découvrir des motifs, des tendances ou des anomalies dans les données de l'IdO. La véracité et la valeur des données de l'IdO

sont des aspects critiques de leur gestion. Les systèmes de gestion des données de l'IdO doivent intégrer des mécanismes de vérification et d'assurance de la qualité des données, ainsi que des techniques d'analyse avancées pour extraire des informations précieuses à partir des données collectées (61; 8; 60; 63; 59; 10; 130; 12; 38; 17; 77).

2.5 Valeur temporelle des données

Dans l'IdO, la valeur des données peut être étroitement liée au facteur temps. Les données de l'IdO peuvent avoir une valeur temporelle, ce qui signifie qu'elles sont plus précieuses et utiles lorsqu'elles sont analysées et traitées rapidement. Par exemple, dans le domaine de la surveillance de la santé, les données en temps réel provenant de capteurs portables surveillant les signes vitaux d'un patient peuvent être utilisées pour détecter rapidement des anomalies et déclencher des interventions médicales immédiates (43). La gestion efficace de la valeur temporelle des données de l'IdO nécessite des capacités de traitement en temps réel et de gestion des flux de données.

3 Gestion des données massives de l'IdO

L'examen des données massives pour l'IdO implique une exploration des dynamiques complexes et des potentialités qui émergent des volumes importants de données produites par les appareils IdO (122; 101). Les appareils en question, qui comprennent des capteurs et des dispositifs intelligents, génèrent une quantité substantielle de données remarquable par sa grande quantité, sa vitesse de production rapide et ses nombreux formats (50; 2). L'analyse et le traitement efficaces de ces données volumineuses sont essentiels pour faire progresser les applications IdO intelligentes et extraire des informations importantes (32; 94). L'examen des données massives pour l'IdO implique de relever plusieurs obstacles liés à la capture, au stockage, au traitement, à l'analyse et à l'affichage des données (24; 16). Ces facteurs sont d'une importance capitale pour gérer efficacement le flux substantiel de données (35; 3). L'examen des données à grande échelle pour l'IdO est un domaine de recherche en constante évolution, nécessitant une créativité continue et la création de nouvelles méthodes et solutions pour faire face aux difficultés qui l'accompagnent et utiliser efficacement les vastes capacités des données de l'IdO (7).

L'un des principaux obstacles rencontrés dans la gestion des données massives de l'IdO concerne :

— La quantité substantielle de données produites par les appareils IdO a le potentiel de submerger les systèmes de gestion de données et l'infrastructure traditionnels.
— La vitesse à laquelle les données sont produites nécessite des capacités de traitement et d'analyse en temps réel ou quasi temps réel.
— La présence de différents types et formats de données, tels que les données structurées, semi-structurées et non structurées, introduit de la complexité dans la gestion et l'analyse des données.

— L'absence de plates-formes accessibles et efficaces de partage et de commercialisation des données entrave la pleine réalisation de la valeur et de l'utilisation des données de l'IdO.
— L'exactitude des données peut être compromise en raison d'erreurs ou d'incohérences, ce qui pose des difficultés pour obtenir des informations précises et prendre des décisions éclairées.
— La nécessité de mettre en œuvre des protocoles de confidentialité et de sécurité pour protéger les informations sensibles contenues dans les données de l'IdO.
— Il existe une demande significative pour une infrastructure évolutive et efficace de stockage, de traitement et d'analyse des données afin de gérer efficacement la quantité et la vitesse substantielles des données générées par l'IdO.
— Il existe une demande croissante pour des approches et des algorithmes analytiques sophistiqués qui peuvent extraire efficacement des informations précieuses des vastes quantités de données générées par l'IdO. Ces méthodes d'analyse avancées sont essentielles pour permettre des actions intelligentes basées sur les données.
— La résolution efficace des difficultés nécessite l'incorporation d'une collaboration interdisciplinaire et de connaissances dans des domaines tels que la gestion des données, l'analytique et les technologies de l'IdO.

Les principales stratégies pour faire face aux difficultés associées à la gestion des Big Data dans le contexte de l'IdO comprennent :

— L'utilisation de technologies de stockage et de traitement de données évolutives et distribuées, telles que les plateformes basées sur le cloud, est essentielle pour gérer efficacement la quantité substantielle et la vitesse rapide des données.
— Tirer parti de méthodologies d'analyse sophistiquées, y compris l'apprentissage automatique et l'intelligence artificielle, pour tirer des informations significatives des données de l'IdO.
— La mise en œuvre de méthodes et de technologies de gestion de la qualité des donnéesest cruciale pour garantir l'exactitude et la cohérence des données de l'IdO. L'objectif est de créer des plateformes robustes et efficaces de partage et de commercialisation des données qui facilitent l'échange et l'exploitation des données de l'IdO.
— La mise en œuvre de mesures rigoureuses de confidentialité et de sécurité, y compris le chiffrement et le contrôle d'accès, est essentielle pour protéger les informations sensibles incluses dans les données de l'IdO. L'objectif est de favoriser la collaboration interdisciplinaire et de faciliter l'échange de connaissances entre les professionnels spécialisés dans la gestion des données, l'analytique et les technologies de l'IdO, afin de relever ensemble les défis qui se posent.
— L'allocation de ressources à la recherche et au développement visant à améliorer les solutions de gestion des données et d'analytique pour les Big Data de l'IdO.
— Veiller au respect des critères réglementaires et de conformité est essentiel pour garantir une utilisation éthique et légale des données de l'IdO.

En résumé, l'IdO présente à la fois des défis et des opportunités dans la gestion efficace et l'interprétation du volume substantiel de données qu'il génère. Les problèmes concernent divers aspects tels que le volume important, la vitesse rapide, la diversité

des données et la qualité requise des données générées par l'IdO. De plus, il est urgent de développer des plates-formes ouvertes de partage de données et de mettre en œuvre des mesures robustes de confidentialité et de sécurité. Néanmoins, diverses solutions existent pour résoudre ce problème, notamment des systèmes évolutifs de stockage et de traitement des données, des méthodologies d'analyse sophistiquées, des protocoles de gestion de la qualité des données et la promotion de la collaboration interdisciplinaire. En abordant efficacement ces difficultés et en adoptant des solutions appropriées, les organisations peuvent exploiter la valeur inhérente des Big Data de l'IdO et prendre des décisions éclairées pour favoriser l'innovation et améliorer plusieurs aspects tant dans les entreprises que dans la société. L'investissement continu dans la recherche et le développement est d'une importance capitale pour faire progresser les solutions de gestion des données et d'analytique pour les Big Data de l'IdO, tout en veillant au respect des exigences réglementaires. En adoptant une méthodologie appropriée, l'utilisation des Big Data de l'IdO a le potentiel de faciliter le développement d'un environnement mondial plus intelligent et interconnecté.

4 Informatique Périphérique pour le Traitement des Données de l'IdO

Le concept d'informatique périphérique concerne un modèle informatique décentralisé dans lequel le traitement et le stockage des données se produisent à proximité du bord du réseau, près de l'origine de la génération des données (27; 29; 4). Contrairement à l'informatique en nuage conventionnelle, qui dépend de centres de données centralisés, l'informatique périphérique implique le déploiement de ressources informatiques et de services plus près des appareils et des capteurs situés au bord du réseau (36). La proximité entre les composants facilite le traitement rapide des données, réduit la latence, améliore l'évolutivité, renforce la confidentialité et permet une prise de décision instantanée (118; 75). L'informatique périphérique permet d'optimiser la bande passante du réseau et facilite l'exécution d'applications sensibles au temps, telles que les appareils IdO, les systèmes autonomes et les analyses en temps réel, en déplaçant les charges de travail de calcul et le stockage des données à proximité du bord du réseau (9; 39). En général, l'informatique périphérique permet aux entreprises de traiter et d'analyser localement les données sur les périphériques, réduisant ainsi la nécessité de transmettre en permanence des données à des infrastructures de cloud éloignées (123; 100).

L'informatique périphérique offre plusieurs avantages pour la gestion des données de l'IdO, notamment une latence réduite, des performances améliorées, une optimisation de la bande passante, une fiabilité accrue, une confidentialité et une sécurité renforcées, une évolutivité et une rentabilité :

— Latence réduite : L'informatique périphérique permet un traitement et une analyse plus rapides des données en rapprochant le calcul de la source de génération des données, réduisant ainsi le temps nécessaire aux données pour se déplacer vers un cloud centralisé ou un centre de données.
— Performances améliorées : En traitant les données au niveau du périphérique, l'informatique périphérique peut fournir des capacités de prise de décision en

temps réel, permettant des temps de réponse plus rapides et des performances globales améliorées des applications IdO.
— Optimisation de la bande passante : L'informatique périphérique contribue à optimiser la bande passante du réseau en réduisant la quantité de données à transmettre au cloud, ce qui permet de réduire la congestion du réseau et les exigences en matière de bande passante.
— Fiabilité accrue : Avec l'informatique périphérique, le traitement et la prise de décision locaux peuvent encore avoir lieu même lorsque la connexion réseau vers le cloud est interrompue, améliorant ainsi la fiabilité et la résilience des applications IdO.
— Confidentialité et sécurité accrues : L'informatique périphérique permet le traitement et l'analyse des données localement, réduisant ainsi la nécessité de transmettre des données sensibles au cloud, ce qui améliore la confidentialité et la sécurité.
— Évolutivité : L'informatique périphérique permet des ressources informatiques distribuées, ce qui permet un déploiement évolutif et flexible des applications IdO, notamment dans des environnements distants ou aux ressources limitées.
— Rentabilité : En réduisant la nécessité d'une transmission extensive des données et des ressources de cloud centralisées, l'informatique périphérique peut contribuer à réduire les coûts associés à la gestion et au traitement des données pour les applications IdO.

Les contraintes liées à l'informatique périphérique dans le contexte de la gestion des données de l'IdO comprennent certaines restrictions dans l'analyse théorique découlant de l'imprévisibilité inhérente à Internet, des pratiques de routage divergentes utilisées par les fournisseurs d'Internet et de cloud, ainsi que des capacités deressources relativement limitées des périphériques par rapport aux serveurs cloud. De plus, il convient de noter que les mécanismes actuels de détection d'erreurs de données dans les schémas d'informatique périphérique basés sur la blockchain présentent une efficacité suboptimale. De plus, par rapport aux solutions basées sur le cloud, l'évolutivité et la réactivité des applications périphériques restent limitées (64; 86; 80; 67). Il est essentiel de prendre en compte les limitations des ressources et les dépenses liées à la consommation d'énergie dans le contexte des appareils IdO. De plus, il est nécessaire de prioriser l'allocation et la gestion efficaces des ressources sur les périphériques afin de garantir un niveau de service satisfaisant pour les applications IdO.

En résumé, l'informatique périphérique présente des avantages notables pour la gestion des données de l'IdO. Ces avantages comprennent une latence réduite, des performances améliorées, une utilisation optimisée de la bande passante, une fiabilité accrue, des mesures renforcées de confidentialité et de sécurité, une évolutivité et une rentabilité. L'informatique périphérique est un paradigme qui utilise des nœuds de calcul situés à la périphérie d'un réseau. Cette approche facilite le traitement des données de l'IdO à proximité de leur source, réduisant ainsi la latence de communication et maximisant l'utilisation des ressources réseau. Néanmoins, il est important de reconnaître certaines contraintes, notamment l'imprévisibilité inhérente à Internet, les variations des protocoles de routage, les capacités de ressources limitées des périphériques et les éventuelles inefficacités dans l'identification et la correction des erreurs de

données. Malgré ces contraintes, l'informatique périphérique offre une solution viable pour aborder les complexités associées à la gestion des données de l'IdO et réaliser les capacités complètes des applications IdO.

5 Qualité dans la gestion des données de l'IdO

Le rôle de la qualité des données dans la gestion des données de l'IdO est d'une importance capitale car elle garantit la fiabilité et l'exactitude des données utilisées pour la prise de décision, le traitement de l'information et les systèmes d'ingénierie (83). La nature hétérogène des données produites par les appareils IdO suscite des appréhensions et peut avoir une influence substantielle sur l'efficacité et la productivité des applications ultérieures (126). Il est donc impératif pour les entreprises d'améliorer leurs systèmes de gestion de la qualité des données afin d'intégrer efficacement l'IdO et d'obtenir des avantages significatifs (47). La reconnaissance de l'importance de la qualité des données dans le contexte de l'IdO est largement acceptée tant par les professionnels que par les chercheurs. Cela souligne la nécessité d'approches et de cadres permettant de développer, d'évaluer et d'améliorer la qualité des données dans les systèmes IdO (46).

Les auteurs de (52) ont proposé un cadre pour améliorer les processus de gestion de la qualité des données (DQM) dans l'IdO. Le cadre comprend un modèle de référence de processus (PRM) pour le DQM de l'IdO et un modèle de maturité appelé IdO DQM3. Validé par des enquêtes et une étude de cas, il offre aux organisations une approche globale pour améliorer leurs processus de DQM dans le domaine de l'IdO. Le travail (104) présente une méthodologie pour gérer efficacement la qualité des données dans les contextes impliquant des "produits intelligents et connectés (SCP)". Cette technique est basée sur l'utilisation de normes internationalement reconnues telles que l'ISO/CEI 25000 et l'ISO 8000. Notre méthodologie propose une collection de stratégies optimales pour évaluer et améliorer la qualité des données dans ces contextes particuliers. Le cadre proposé dans (51) présente une approche globale pour évaluer la qualité des données (DQ) dans le contexte de l'IdO. L'utilisation d'une architecture basée sur les graphes de connaissances facilite l'intégration de l'évaluation de la qualité des données dans une multitude d'applications IdO. Cet outil facilite l'identification et l'intégration des mesures de qualité des données. L'efficacité du cadre dans la résolution de tâches pratiques est illustrée par la présentation d'un cas d'utilisation.

Les auteurs de (48) ont proposé une approche basée sur l'architecture orientée modèle pour la gestion de la qualité des données (DQ) dans l'IdO. Elle aborde la nature subjective de la DQ et les besoins divers des consommateurs de données en permettant aux développeurs d'exprimer les exigences de la DQ à travers des modèles et un éditeur graphique. L'approche génère automatiquement une infrastructure personnalisée pour la gestion de la DQ, adaptée aux spécifications du consommateur de données. Sa flexibilité et son efficacité sont démontrées par la génération de deux infrastructures de gestion de la DQ testées dans un scénario de flux de données IdO réel. L'étude (6) présente le cadre Quality of Data for IdO Devices (QoDID) pour aborder la difficulté des systèmes IdO à collecter et traiter les données brutes des capteurs. Cet article décrit l'architecture de QoDID, les cas d'utilisation et la mise en œuvre. De plus, les auteurs

montrent comment l'architecture de QoDID peut améliorer la collecte des données des appareils et capteurs IdO, offrant des informations utiles.

En conclusion, garantir la qualité des données dans l'IdO présente de nombreux défis. Les systèmes IdO font face à des défis liés à des besoins divers, à une intégration limitée des méthodologies de qualité des données et à la nécessité d'évaluer et de comparer les problèmes de qualité des données. Cependant,ces problèmes peuvent être résolus. Cette étude implique des revues systématiques de la littérature pour identifier les thèmes de recherche, des cadres génériques dérivés des graphes de connaissances, des explorations d'apprentissage approfondi, des modèles de maturité pour la gestion de la qualité des données IdO et des enquêtes sur les cadres et les méthodologies existants. Les entreprises et les praticiens peuvent améliorer les processus et la prise de décision en aval en améliorant la qualité des données dans les applications IdO.

6 ML pour l'analyse des données de l'IdO

L'utilisation de l'apprentissage automatique (ML) est devenue de plus en plus répandue en tant que méthodologie efficace pour analyser les grandes quantités de données produites par les appareils IdO (5; 92). Avec la prolifération croissante des appareils physiques interconnectés, il existe une demande correspondante pour des approches efficaces permettant d'extraire des informations significatives à partir des données qu'ils fournissent (124). Les algorithmes de ML offrent une alternative viable en proposant des méthodologies automatisées et intelligentes pour traiter et tirer des insights significatifs des données de l'IdO (110). En utilisant ces algorithmes, il devient possible d'identifier des tendances, de détecter des anomalies et de faire des prédictions (97). Cette capacité permet aux entreprises d'optimiser leurs opérations, d'améliorer leurs processus de prise de décision et d'améliorer la fonctionnalité globale des appareils IdO (1).

Les principaux avantages de l'utilisation du ML pour la gestion de l'IdO comprennent :

- Les algorithmes de ML ont la capacité de traiter et d'analyser efficacement les vastes volumes de données produits par les appareils IdO, ce qui permet d'obtenir des résultats d'analyse caractérisés par une précision et une fiabilité améliorées.
- Les algorithmes de ML ont la capacité d'identifier et de traiter les attaques réseau sur les appareils IdO grâce à l'analyse des données de trafic réseau. Cette approche analytique améliore la sécurité globale des systèmes IdO.
- Les algorithmes de ML ont la capacité d'analyser des données IdO en temps réel, ce qui permet aux entreprises de prendre des décisions éclairées et rapides en tirant parti des informations acquises.
- Les algorithmes de ML ont le potentiel d'améliorer l'efficacité de l'analyse de grandes quantités de données dans les applications IdO en distribuant le processus d'analyse et en allouant équitablement la charge de travail.
- Les algorithmes de ML peuvent être entraînés à l'aide de données de capteurs IdO pour identifier les anomalies, prévoir les performances futures et améliorer

l'efficacité des systèmes IdO. Cela s'applique notamment aux domaines tels que les tests et l'analyse du béton.
— Les algorithmes de ML peuvent automatiser et optimiser divers processus dans la gestion de l'IdO, réduisant ainsi le besoin d'interventions manuelles et améliorant l'efficacité globale.
— Les algorithmes de ML peuvent identifier des motifs et des tendances dans les données de l'IdO, permettant une maintenance prédictive et une prise de décision proactive.
— Les algorithmes de ML peuvent s'adapter et apprendre à partir de nouvelles données, permettant une amélioration continue et une adaptation aux environnements changeants de l'IdO.
— Les algorithmes de ML peuvent permettre des services personnalisés et adaptés au contexte dans les applications IdO, améliorant ainsi l'expérience utilisateur et la satisfaction.
— Les algorithmes de ML peuvent faciliter la prise de décision basée sur les données dans la gestion de l'IdO, conduisant à une allocation plus efficace des ressources et à une optimisation des coûts.

Il existe un certain nombre de problèmes et de défis importants dans le domaine de l'utilisation du ML pour le traitement des données de l'IdO qui nécessitent une recherche approfondie :

— L'un des principaux défis dans l'utilisation du ML pour l'analyse des données de l'IdO est le traitement des données volumineuses et dynamiques. Les algorithmes traditionnels peuvent avoir du mal à produire des résultats précis et fiables lorsqu'ils traitent de grands volumes de données en constante évolution.
— Un autre défi est la sécurité et la confidentialité des appareils et des données de l'IdO. À mesure que les appareils IdO deviennent de plus en plusinterconnectés, le risque d'attaques réseau et d'accès non autorisés augmente. Les algorithmes de ML peuvent aider à détecter et à atténuer ces attaques, mais garantir la sécurité des systèmes IdO reste un défi.
— La scalabilité des algorithmes de ML pour l'analyse des données de l'IdO est également une limitation. À mesure que le nombre d'appareils IdO et la quantité de données générées continuent de croître, il devient important de développer des algorithmes scalables capables de gérer le volume croissant de données et les exigences computationnelles.
— Les performances et l'exactitude des algorithmes de ML dans l'analyse des données de l'IdO peuvent varier en fonction de l'application spécifique et de l'ensemble de données. Il est important de sélectionner et d'évaluer soigneusement les algorithmes pour s'assurer qu'ils conviennent à la tâche donnée et fournissent des résultats précis.
— Une autre limitation est la nécessité de prétraitement des données et d'extraction des caractéristiques dans l'analyse des données de l'IdO. Des techniques de prétraitement telles que le nettoyage des données, la normalisation et la sélection des caractéristiques sont souvent nécessaires pour améliorer la qualité et la pertinence des données pour les algorithmes de ML.
— La centralisation et la gestion de la charge des données de l'IdO dans la couche

cloud peuvent également poser des défis. Les frameworks distribués qui exploitent le calcul de périphérie (edge computing) et le traitement des données au niveau des appareils peuvent aider à relever ces défis et à améliorer les performances et la fiabilité de l'analyse des données de l'IdO.

En résumé, le domaine des algorithmes de regroupement pilotés par le ML pour l'étude des données de l'IdO offre de nombreuses perspectives ainsi que des obstacles. Les limites posées par l'échelle et la dynamique des données de l'IdO peuvent être efficacement résolues grâce à diverses méthodes. Une stratégie potentielle consiste à développer et déployer des algorithmes de regroupement sophistiqués spécifiquement conçus pour gérer efficacement des ensembles de données volumineux et en constante évolution. L'utilisation de ces algorithmes a le potentiel d'améliorer la précision et la fiabilité des résultats, garantissant ainsi l'évolutivité et l'efficacité de l'analyse des données de l'IdO. De plus, l'intégration de mesures de sécurité et d'approches renforçant la confidentialité lors du développement des systèmes IdO peut réduire efficacement les risques potentiels liés aux attaques réseau et aux intrusions illégales. De plus, l'utilisation de frameworks distribués et du calcul de périphérie (edge computing) a le potentiel d'améliorer les performances et l'efficacité du traitement des données de l'IdO en réduisant la dépendance aux systèmes cloud centralisés. Grâce à l'utilisation de ces stratégies et à l'amélioration continue des algorithmes de ML, il devient possible de surmonter les obstacles et les contraintes associés à l'analyse des données de l'IdO. Cela facilite l'obtention d'une précision, d'une fiabilité et d'une évolutivité accrues dans l'analyse des données de l'IdO dans diverses applications.

7 Détection d'anomalies dans le transfert de données IdO

La détection des anomalies est d'une importance capitale pour garantir la sécurité et la fiabilité du transfert de données au sein de l'IdO. Une anomalie peut être définie comme une déviation ou une irrégularité observée dans les données générées par l'IdO, qui ne correspond pas aux schémas ou comportements attendus (30). Les anomalies peuvent se manifester en raison de diverses circonstances, notamment des défauts des capteurs, des cyberattaques, des défaillances du système, des modifications de l'environnement ou même des erreurs humaines. L'identification des anomalies revêt une importance significative pour garantir l'intégrité, la sécurité et les performances des réseaux et des applications IdO (111). L'identification et la réponse rapides aux anomalies peuvent neutraliser efficacement les menaces ou les problèmes opérationnels potentiels, réduisant ainsi les conséquences graves telles que les violations de données, les dommages matériels ou les interruptions de service.

Les solutions de détection d'anomalies IdO utilisent des techniques sophistiquées d'analyse de données, des algorithmes d'apprentissage automatique et des méthodologies de modélisation statistique pour discerner les schémas et les anomalies dans les données (26). Les méthodes discutées peuvent être catégorisées en trois approches principales : supervisée, non supervisée et semi-supervisée (85). Les approches supervisées dépendent de la disponibilité de données d'entraînement étiquetées afin de construire

des modèles capables de distinguer les événements normaux des événements anormaux. En revanche, les algorithmes non supervisés sont conçus pour détecter les anomalies sans aucune connaissance préalable du comportement normal, ce qui les rend adaptés à l'identification de schémas nouveaux ou inhabituels (15). Les méthodologies semi-supervisées incluent des aspects des procédures supervisées et non supervisées, en utilisant à la fois des données étiquetées et non étiquetées pour améliorer la précision de l'identification des anomalies.

Les auteurs de (22) proposent HS-TCN, un réseau de convolution temporelle hiérarchique semi-supervisé, pour la détection d'anomalies dans la communication IdO. Il s'entraîne efficacement sur des données étiquetées et non étiquetées, prend en compte les caractéristiques des données en continu et améliore l'efficacité et les performances de détection des anomalies. Cette approche permet de relever le défi de la disponibilité limitée de données étiquetées et contribue à l'avancement de la détection d'anomalies dans les réseaux de communication IdO. De plus, les chercheurs de l'article (113) proposent un cadre de travail pour la détection des attaques sur les dispositifs IdO en utilisant la méthode DWU-ODBN. Leur approche comprend un prétraitement, une extraction de caractéristiques, une sélection de caractéristiques et une classification pour identifier la source des attaques. Les résultats expérimentaux montrent que leur méthode surpasse les approches existantes, atteignant un temps de détection des attaques de 77 secondes avec un taux de précision de 98,1%.

L'article (84) propose un cadre de travail pour la détection précise des anomalies dans l'Internet industriel des objets (IIdO) en utilisant une approche d'apprentissage fédéré (FL). Ils présentent un modèle de réseau de neurones convolutifs-LSTM (CNN-LSTM) qui capture les caractéristiques fines et utilise des unités LSTM pour la prédiction de données en séries temporelles. Le cadre de travail permet une détection d'anomalies en temps réel et légère grâce à un mécanisme de compression de gradient, réduisant les coûts de communication d'environ 50% par rapport aux schémas traditionnels. Les résultats expérimentaux valident l'efficacité de l'approche proposée pour détecter avec précision les anomalies dans les environnements IIdO.En résumé, la détection d'anomalies dans le transfert de données IdO est cruciale pour assurer la sécurité et la fiabilité des réseaux et des applications IdO. Différentes approches, telles que les méthodes supervisées, non supervisées et semi-supervisées, sont utilisées pour identifier les schémas normaux et les anomalies dans les données. Des techniques avancées d'apprentissage automatique, de modélisation statistique et d'analyse de données sont appliquées pour détecter les anomalies et prendre des mesures appropriées. Les cadres de travail proposés, tels que HS-TCN, DWU-ODBN et FL-CNN-LSTM, ont montré des performances prometteuses dans la détection précise des anomalies dans les réseaux IdO. Ces approches contribuent à améliorer la sécurité, l'intégrité et les performances des systèmes IdO en identifiant rapidement les problèmes potentiels et en permettant une réponse adéquate.

8 Transfert de données économe en énergie dans l'IdO

La question de l'efficacité énergétique dans la communication de données dans le contexte de l'IdO est d'une importance capitale, étant donné la mise en œuvre géné-

ralisée des dispositifs IdO et leurs ressources énergétiques souvent limitées (41). L'optimisation des mécanismes de transfert de données a le potentiel d'avoir une influence substantielle sur la consommation énergétique globale des systèmes IdO, prolongeant ainsi la durée de vie opérationnelle des dispositifs alimentés par batterie. De nombreuses méthodologies ont été examinées afin d'obtenir une meilleure efficacité énergétique dans le domaine du transfert de données dans l'IdO (103). Une stratégie potentielle consiste à utiliser l'agrégation de données, qui implique la consolidation des données obtenues à partir de plusieurs dispositifs IdO en un seul paquet unifié (40). Cette approche permet de réduire la fréquence des transferts et de limiter l'utilisation d'énergie. L'agrégation peut être réalisée à différents niveaux, tels que dans un groupe localisé ou au niveau d'une passerelle centralisée, en fonction du cadre spécifique de l'IdO.

Une autre approche implique l'utilisation de protocoles de communication efficaces. Des protocoles de communication traditionnels tels que MQTT et CoAP sont largement utilisés dans les applications IdO. Cependant, il convient de noter que ces protocoles peuvent ne pas offrir le plus haut niveau d'efficacité énergétique (13). Des protocoles novateurs, tels que les technologies de réseau à faible consommation d'énergie à large portée (LPWAN) (20) comme Narrowband Internet of Things (NB-IdO) (45) et Long Range Wide Area Network (LoRaWAN) (37), ont été développés dans le but principal de répondre aux limitations énergétiques des dispositifs IdO. Ces protocoles offrent une portée étendue et une consommation d'énergie réduite, ce qui les rend adaptés aux dispositifs IdO à contraintes énergétiques.

De plus, les stratégies de gestion de l'alimentation ont un impact substantiel sur l'efficacité énergétique de la communication de données. Les dispositifs IdO ont la capacité d'utiliser des techniques telles que le duty cycling, qui consiste à alterner entre des états actifs et de veille. Cette approche permet de réduire efficacement l'utilisation d'énergie pendant les périodes d'inactivité (107). Le contrôle adaptatif de la puissance de transmission est une technologie qui module la puissance de transmission en fonction de la séparation spatiale entre les dispositifs, dans le but d'optimiser la consommation d'énergie (99). De plus, l'utilisation de l'informatique en périphérie peut être utilisée comme moyen de réduire la quantité de données à transmettre vers le cloud. Des économies d'énergie peuvent être réalisées en minimisant les transmissions de données inutiles et les communications avec le cloud grâce au traitement et à l'analyse des données au niveau du réseau périphérique, à proximité des dispositifs IdO (21; 42**?**). Les méthodologies d'apprentissage automatique peuvent également apporter une contribution précieuse à l'amélioration de l'efficacité énergétique de la communication dans l'IdO. Grâce à l'utilisation de la prédiction de modèles de données locales ou d'événements, les dispositifs IdO ont la capacité de communiquer sélectivement des données, ce qui réduit ainsi le volume global de données transmises et préserve efficacement les ressources énergétiques (11).

Le travail (127) propose un système IdO sans cellules basé sur un réseau de communication sans cellules pour améliorer la fiabilité et la durabilité de l'IdO. En diluant le concept de cellule traditionnel, l'architecture IdO sans cellules améliore la robustesse du système par rapport à l'IdO cellulaire. L'article aborde l'allocation de l'énergie dans les réseaux IdO sans cellules en utilisant des algorithmes d'optimisation pour minimiser la consommation d'énergie des dispositifs IdO. Les résultats expérimentaux montrent

que le système IdO sans cellules peut réduire la consommation d'énergie de manière significative par rapport aux systèmes IdO cellulaires traditionnels.

En résumé, il existe plusieurs approches pour améliorer l'efficacité énergétique dans le transfert de données de l'IdO. L'agrégation de données, l'utilisation de protocoles de communication efficaces, les stratégies de gestion de l'alimentation, l'informatique en périphérie et les techniques d'apprentissage automatique sont autant de méthodologies potentielles pour réduire la consommation d'énergie des dispositifs IdO et prolonger leur durée de vie opérationnelle. L'adoption de ces techniques dépendra du contexte spécifique de déploiement de l'IdO et des exigences du système, mais elles offrent toutes des opportunités prometteuses pour une communication de données économe en énergie dans l'IdO.

9 Sécurité dans la gestion des données de l'IdO

La sécurité est un élément essentiel de la gestion des données de l'IdO qui doit être abordé pour garantir la protection et l'intégrité des données sensibles collectées et traitées par les dispositifs IdO. Il existe plusieurs problématiques essentielles pour assurer une sécurité robuste à mesure que le nombre de dispositifs connectés augmente et que les données circulent entre eux et les plateformes basées sur le cloud :

- Authentification et contrôle d'accès (14) : Il est essentiel de garantir l'authenticité des dispositifs et des utilisateurs interagissant avec les données de l'IdO. Des techniques d'authentification robustes doivent être développées pour vérifier l'identité à la fois des dispositifs et des utilisateurs. De plus, des politiques strictes de contrôle d'accès doivent être mises en œuvre pour prévenir les accès non autorisés à des informations sensibles.
- Chiffrement des données (95; 112) : Afin de se prémunir contre l'interception ou la falsification, il est impératif d'utiliser le chiffrement pour les données de l'IdO, à la fois en transit et au repos. Des technologies telles que Transport Layer Security (TLS) ou Secure Shell (SSH) peuvent être utilisées pour mettre en place des mécanismes de chiffrement robustes, garantissant l'intégrité et la confidentialité des données.
- Protocoles de communication sécurisés (93; 33) : Les dispositifs IdO doivent utiliser des protocoles de communication sécurisés tels que HTTPS ou MQTT avec TLS pour établir des connexions chiffrées et autorisées avec les systèmes backend. Cette pratique empêche l'écoute indiscrète et maintient la confidentialité des données en transit.
- Gestion et mises à jour des dispositifs (31; 114) : Pour faire face aux vulnérabilités potentielles en matière de sécurité et se défendre contre d'éventuelles attaques, les organisations doivent mettre en place des procédures complètes de gestion des dispositifs. Cela inclut le déploiement régulier de mises à jour du micrologiciel (firmware) et de correctifs pour garantir que les dispositifs sont protégés contre les menaces en constante évolution.
- Confidentialité des données (117; 115) : La protection des informations personnelles identifiables (PII) revêt une importance capitale. Les systèmes IdO doivent respecter la législation et les lignes directrices en matière de confiden-

tialité pour protéger les données sensibles des individus. Des techniques telles que l'anonymisation, l'agrégation et la pseudonymisation des données peuvent être utilisées pour réduire les risques pour la vie privée.

— Systèmes de détection et de prévention des intrusions (IDS/IPS) (44; 28) : La mise en œuvre de systèmes IDS/IPS est essentielle pour identifier et atténuer les violations de sécurité ou les activités non autorisées au sein de l'écosystème IdO. Ces systèmes surveillent activement le trafic réseau pour détecter les comportements suspects et prennent des mesures préventives pour se protéger contre les menaces potentielles.

— Infrastructure cloud sécurisée (96; 74) : Les systèmes basés sur le cloud qui stockent et traitent les données de l'IdO doivent être renforcés par des mesures de sécurité robustes. Cela comprend des centres de données sécurisés, des contrôles d'accès stricts et des mécanismes de chiffrement pour empêcher les accès non autorisés et se protéger contre d'éventuelles violations.

— Audits de sécurité réguliers et surveillance (81; 109) : La réalisation d'audits de sécurité réguliers et la surveillance étroite des dispositifs IdO sont des pratiques essentielles. Ces mesures aidentà identifier les vulnérabilités potentielles, à détecter rapidement les activités inhabituelles et à réagir rapidement à tout incident de sécurité pouvant survenir.

Les organisations peuvent améliorer la sécurité des données de l'IdO, conserver la confiance des utilisateurs et réduire les risques liés à l'accès non autorisé, aux violations de données et aux atteintes à la vie privée en abordant ces facteurs de sécurité. Pour surmonter ces problèmes, une approche multi-niveaux de la sécurité est nécessaire, combinant une conception matérielle sûre, des techniques de développement logiciel robustes, des politiques de sécurité efficaces et des mécanismes de surveillance et de réaction continus.

10 Blockchain pour l'accès aux données de l'IdO

La technologie de la blockchain a suscité beaucoup d'attention en raison de sa promesse d'améliorer la sécurité, la transparence et la confiance dans divers secteurs. Lorsqu'elle est appliquée à l'accès aux données de l'IdO, la blockchain peut offrir divers avantages et résoudre des problèmes tels que l'intégrité des données, l'authentification et le contrôle décentralisé. Voici un aperçu de la façon dont la technologie de la blockchain peut être utilisée pour accéder aux données de l'IdO (121; 119; 106) :

— Contrôle décentralisé de l'accès aux données : La blockchain offre un registre décentralisé et inviolable qui peut être utilisé pour gérer le contrôle d'accès aux données de l'IdO. Sur la blockchain, des contrats intelligents peuvent être utilisés pour définir et appliquer les autorisations d'accès aux données, garantissant que seules les entités autorisées peuvent accéder aux données et interagir avec elles.

— Intégrité et traçabilité des données : L'immutabilité et le hachage cryptographique de la blockchain en font un outil idéal pour vérifier l'intégrité des données de l'IdO. Chaque transaction ou mise à jour des données peut être enregistrée sur la blockchain, créant ainsi une piste auditable que toutes les parties peuvent

vérifier. Cela contribue à éviter les modifications non autorisées et offre un enregistrement clair des opérations sur les données.
— Sécurité et authentification renforcées : En fournissant un système de gestion d'identité décentralisé, la blockchain peut améliorer la sécurité de l'accès aux données de l'IdO. Les dispositifs de l'IdO peuvent vérifier et interagir de manière sécurisée les uns avec les autres en utilisant l'authentification basée sur la blockchain et les signatures numériques, réduisant ainsi les risques d'accès illégal ou de contrefaçon.
— Monétisation et propriété des données : La technologie de la blockchain peut permettre la monétisation sécurisée et transparente des données de l'IdO. Les producteurs de données peuvent conserver les droits de propriété et le contrôle sur la manière dont leurs données sont consultées et diffusées en enregistrant les transactions de données sur la blockchain. Les contrats intelligents peuvent fournir des méthodes de compensation automatiques et équitables pour le partage des données.
— Partage et collaboration des données : La technologie de la blockchain permet le partage sécurisé et efficace des données entre plusieurs parties. Les dispositifs de l'IdO peuvent contribuer des données à un réseau basé sur la blockchain, et les utilisateurs autorisés peuvent accéder et utiliser les données à des fins diverses, telles que la recherche, l'analyse et l'amélioration des services, tout en protégeant la confidentialité et le contrôle des données.

Cependant, certaines préoccupations doivent être abordées lors de l'utilisation de la technologie de la blockchain pour l'accès aux données de l'IdO (98; 120; 128) :

— Scalabilité : La scalabilité de la blockchain reste un défi majeur, en particulier lorsqu'elle est appliquée à l'accès aux données de l'IdO. Le volume important de données générées par les dispositifs de l'IdO peut surcharger les réseaux blockchain et entraver le traitement efficace des transactions. Il est essentiel de développer des solutions blockchain évolutives capables de gérer l'ampleur et la vélocité des données générées par l'IdO.
— Débit et latence : Les applications de l'IdO nécessitent fréquemment un accès et un traitement des données en temps réel ou quasi temps réel. Les algorithmes de consensus intrinsèques et les processus de validation des transactions de la blockchain peuvent entraîner une latence et limiter le débit. L'amélioration des performances du réseau blockchain pour fournir un accès aux données à faible latence et un débit élevé des transactionsest un problème constant.
— Efficacité énergétique : Le minage de la blockchain et les méthodes de consensus peuvent être intensifs en termes de calcul et consommer beaucoup d'énergie. L'efficacité énergétique est cruciale dans les contextes de l'IdO avec des dispositifs aux ressources limitées. Ce défi peut être atténué en développant des algorithmes de consensus écoénergétiques ou en explorant des méthodes de consensus alternatives telles que la preuve d'enjeu.
— Interopérabilité et normes : L'absence d'interopérabilité et de normes communes entre différentes implémentations de la blockchain et les plateformes de l'IdO entrave l'intégration et l'échange de données. Il est crucial, pour une adoption généralisée, d'établir des cadres d'interopérabilité, des formats de données et des

protocoles de communication qui permettent la compatibilité entre différents réseaux blockchain et dispositifs de l'IdO.
— Confidentialité et sécurité : Bien que la blockchain offre l'ouverture et l'immutabilité, la protection de la confidentialité et de la sécurité des données sensibles de l'IdO reste un défi. Pour sécuriser les informations sensibles, il est important de trouver un équilibre entre la transparence des données et la confidentialité, par exemple en utilisant des mécanismes préservant la vie privée tels que les preuves de connaissance nulle ou des solutions de stockage de données hors chaîne.
— Gouvernance et réglementation : En raison de la nature décentralisée de la blockchain, des questions de gouvernance et de réglementation se posent. Pour garantir la conformité à la législation existante et résoudre tout problème juridique et éthique lié à l'accès aux données de l'IdO sur les réseaux blockchain, il est nécessaire de déterminer les cadres juridiques, les modèles de gouvernance et les questions de responsabilité.
— Sécurité et résilience : Bien que la technologie de la blockchain améliore la sécurité de plusieurs façons, elle n'est pas à l'abri des menaces cybernétiques. Les failles des contrats intelligents, les attaques contre le consensus et la possibilité d'une attaque à 51% sont tous des risques de sécurité qui doivent être traités. Pour maintenir la stabilité des systèmes d'accès aux données de l'IdO basés sur la blockchain, des mécanismes de sécurité robustes, des audits de code et une surveillance régulière sont nécessaires.
— Coût et complexité : La mise en œuvre des technologies de la blockchain peut être coûteuse en termes d'infrastructure et de dépenses opérationnelles. Il est important de déterminer l'efficacité économique et d'effectuer une analyse coûts-avantages de l'utilisation de la blockchain pour l'accès aux données de l'IdO. De plus, réduire la complexité de la technologie de la blockchain et créer des interfaces conviviales et des cadres de développement facilitera son adoption plus large.

Résoudre ces problèmes en suspens est essentiel pour l'application réussie de la technologie de la blockchain pour l'accès aux données de l'IdO. Pour surmonter ces problèmes et réaliser pleinement le potentiel de la blockchain pour améliorer l'accès et la sécurité des données de l'IdO, les chercheurs, les acteurs de l'industrie et les organismes de normalisation doivent travailler ensemble.

11 Orientations et défis futurs

L'évolution rapide de la gestion des données de l'IdO va se poursuivre selon plusieurs voies intrigantes. En regardant vers l'avenir, de nombreux thèmes majeurs et défis se dégagent qui façonneront le paysage futur des écosystèmes de données de l'IdO.

11.1 Intelligence artificielle au service des insights de données

L'intégration de l'intelligence artificielle (IA) et de la gestion des données de l'IdO représente un moment décisif dans le domaine. Les algorithmes d'apprentissage automatique et les modèles d'apprentissage profond devraient jouer un rôle essentiel dans

l'obtention d'insights complexes à partir de quantités massives de données de l'IdO. Ces algorithmes sont capables de détecter des motifs subtils, des corrélations et des anomalies que les méthodes analytiques standard peuvent ignorer. À mesure que les modèles d'IA se développent, ils fourniront aux décideurs des informations plus précises et conscientes du contexte. De plus, les avancées de l'IA embarquée, qui effectue des calculs d'apprentissage automatique directement sur les appareils IdO, promettent de placer la prise de décision en temps réel et localisée au premier plan.

11.2 Maturité de l'informatique en périphérie

Le développement de l'informatique en périphérie marque un changement fondamental dans le traitement des données de l'IdO. Les appareils en périphérie deviennent de plus en plus sophistiqués en termes de capacités de calcul. Grâce à ces progrès, ils peuvent désormais effectuer des calculs complexes localement, réduisant ainsi la nécessité de transmettre continuellement des données aux serveurs cloud centralisés. Par conséquent, la latence est considérablement réduite, ce qui permet des temps de réaction plus rapides pour les applications cruciales. Cette tendance améliore non seulement la prise de décision en temps réel, mais réduit également la charge sur l'infrastructure cloud centralisée, ce qui se traduit par des installations IdO plus efficaces et réactives.

11.3 Interopérabilité et normalisation

L'interopérabilité transparente des différents appareils et plateformes de l'IdO est essentielle pour maximiser le potentiel des écosystèmes de l'IdO. Il est crucial de déployer des efforts pour normaliser les protocoles de communication et les formats de données. La normalisation permet non seulement une intégration simple, mais encourage également une atmosphère de collaboration dans laquelle les développeurs peuvent construire des applications compatibles entre elles. À mesure que l'écosystème de l'IdO se développe, la demande d'interopérabilité augmentera, ce qui nécessitera un travail continu de normalisation et de compatibilité.

11.4 Sécurité à l'ère de la connectivité omniprésente

La croissance des dispositifs connectés augmente la surface d'attaque, ce qui fait de la sécurité une priorité absolue. Pour protéger les systèmes IdO contre les nouvelles menaces en matière de cybersécurité, des mesures de sécurité solides sont nécessaires. Cela inclut la mise en place d'algorithmes de chiffrement avancés, d'une gestion décentralisée des identités et de systèmes de détection des intrusions. De plus, l'intégration de processus de démarrage sécurisé et de fonctionnalités de sécurité basées sur le matériel sera cruciale pour renforcer la posture de sécurité des installations IdO, garantissant ainsi l'intégrité et la confidentialité des données.

11.5 Scalabilité et optimisation des ressources

À mesure que le nombre d'appareils connectés augmente rapidement, garantir la scalabilité devient crucial. Concevoir des systèmes capables de gérer en douceur un nombre

croissant d'appareils tout en améliorant l'efficacité des ressources est un défi majeur. Des recherches et développements continus dans des domaines tels que la conception matérielle efficace, les protocoles de communication légers et les architectures informatiques distribuées sont nécessaires. Les innovations dans ces domaines seront essentielles pour permettre une mise en œuvre harmonieuse et durable de l'IdO.

11.6 Considérationséthiques et gouvernance des données

À mesure que les applications de l'IdO touchent de plus en plus de aspects de la vie quotidienne, les préoccupations éthiques liées à la protection, à l'autorisation et à la propriété des données deviennent de plus en plus importantes. Il est essentiel d'établir des règles claires de gouvernance des données et de respecter les réglementations sur la vie privée. Des systèmes de consentement solides, des réglementations transparentes sur l'utilisation des données et des outils permettant aux individus de contrôler leurs propres données font partie de cela. Il est crucial de trouver un équilibre entre l'innovation et la protection des droits individuels afin d'assurer une utilisation responsable et éthique des technologies de l'IdO.

11.7 Durabilité environnementale

L'impact environnemental de l'adoption extensive de l'IdO suscite de plus en plus d'inquiétudes. Des efforts doivent être déployés pour réduire la consommation d'énergie et la génération de déchets électroniques. Cela implique des travaux sur la conception matérielle économe en énergie, les technologies de communication à faible consommation d'énergie et les techniques de production respectueuses de l'environnement. De plus, l'élaboration de normes pour la gestion des appareils en fin de vie et le recyclage sera essentielle pour réduire l'impact environnemental des installations de l'IdO.

Naviguer dans ces orientations futures et surmonter les obstacles qui y sont associés sera essentiel pour réaliser pleinement le potentiel de la gestion des données de l'IdO. À mesure que le paysage de l'IdO évolue, la collaboration interdisciplinaire et de nouvelles solutions seront essentielles pour concevoir un monde connecté efficace et sécurisé.

12 Conclusion

L'évolution rapide de la gestion des données de l'IdO démontre l'interaction dynamique entre la technologie et les attentes d'un monde connecté. Les avancées mises en évidence dans cet article témoignent des progrès extraordinaires réalisés dans l'exploitation du potentiel des données de l'IdO pour une large gamme d'applications.

L'évolution de la gestion des données de l'IdO s'est distinguée par la créativité et l'ingéniosité, des concepts fondamentaux d'authentification et de chiffrement aux applications de pointe basées sur les insights de l'IA. L'intégration de l'informatique en périphérie a entraîné un changement fondamental dans le traitement des données, offrant des avantages remarquables en termes d'efficacité et de réactivité. Les efforts d'interopérabilité et de normalisation sont essentiels pour garantir l'intégration transparente de dispositifs disparates, permettant l'émergence de solutions interdomaines.

Face à une connectivité omniprésente, la sécurité reste une priorité absolue. Les approches avancées de chiffrement et la gestion décentralisée des identités sont des avancées cruciales pour sécuriser les environnements de l'IdO. De plus, les considérations éthiques, la gouvernance des données et la durabilité environnementale sont essentielles pour assurer le déploiement responsable et durable des technologies de l'IdO.

En regardant vers l'avenir, l'avenir de la gestion des données de l'IdO promet une intégration encore plus poussée de l'IA, une maturation des capacités de l'informatique en périphérie et une volonté déterminée de favoriser l'interopérabilité. Ces développements, combinés aux travaux continus sur la sécurité et la scalabilité, sont la clé pour réaliser pleinement le potentiel des déploiements de l'IdO.

Enfin, le parcours de la gestion des données de l'IdO montre l'esprit collaboratif de la recherche et de l'innovation interdisciplinaires. Le pouvoir révolutionnaire de la technologie de l'IdO a été observé grâce aux efforts de collaboration des chercheurs, des praticiens et des parties prenantes. Poursuivons notre travail pour repousser les limites de la connaissance alors que nous naviguons dans les eaux inexplorées de demain, guidés par la vision d'un monde connecté à la fois efficace et sécurisé.

Références

[1] Erwin Adi, Adnan Anwar, Zubair Baig, and Sherali Zeadally. Machine learning and data analytics for the iot. *Neural computing and applications*, 32 :16205–16233, 2020.

[2] Abu Fuad Ahmad, Md. Shohel Sayeed, Choo Peng Tan, Kim Geok Tan, Md Ahsanul Bari, and Ferdous Hossain. A review on iot with big data analytics. In *2021 9th International Conference on Information and Communication Technology (ICoICT)*, pages 160–164, 2021.

[3] Ejaz Ahmed, Ibrar Yaqoob, Ibrahim Abaker Targio Hashem, Imran Khan, Abdelmuttlib Ibrahim Abdalla Ahmed, Muhammad Imran, and Athanasios V Vasilakos. The role of big data analytics in internet of things. *Computer Networks*, 129 :459–471, 2017.

[4] Mehreen Ahmed, Rafia Mumtaz, Syed Mohammad Hassan Zaidi, Maryam Hafeez, Syed Ali Raza Zaidi, and Muneer Ahmad. Distributed fog computing for internet of things (iot) based ambient data processing and analysis. *Electronics*, 9(11) :1756, 2020.

[5] Redhwan Al-amri, Raja Kumar Murugesan, Mustafa Man, Alaa Fareed Abdulateef, Mohammed A Al-Sharafi, and Ammar Ahmed Alkahtani. A review of machine learning and deep learning techniques for anomaly detection in iot data. *Applied Sciences*, 11(12) :5320, 2021.

[6] Eyhab Al-Masri Al-Masri and Yan Bai. Invited paper : A service-oriented approach for assessing the quality of data for the internet of things. In *2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)*, pages 9–97, 2019.

[7] Zainab Alansari, Nor Badrul Anuar, Amirrudin Kamsin, Safeeullah Soomro, Mohammad Riyaz Belgaum, Mahdi H Miraz, and Jawdat Alshaer. Challenges of internet of things and big data integration. In *Emerging Technologies in Computing : First International Conference, iCETiC 2018, London, UK, August 23–24, 2018, Proceedings 1*, pages 47–55. Springer, 2018.

[8] Omar Azib Alkhudaydi, Moez Krichen, and Ans D Alghamdi. A deep learning methodology for predicting cybersecurity attacks on the internet of things. *Information*, 14(10) :550, 2023.

[9] Mohammed Alrowaily and Zhuo Lu. Secure edge computing in iot systems : Review and case studies. In *2018 IEEE/ACM symposium on edge computing (SEC)*, pages 440–444. IEEE, 2018.

[10] Hamoud Alshammari, Karim Gasmi, Ibtihel Ben Ltaifa, Moez Krichen, Lassaad Ben Ammar, and Mahmood A Mahmood. Olive disease classification based on vision transformer and cnn models. *Computational Intelligence and Neuroscience*, 2022, 2022.

[11] Akm Ashiquzzaman, Hyunmin Lee, Tai-Won Um, and Jinsul Kim. Energy-efficient iot sensor calibration with deep reinforcement learning. *IEEE Access*, 8 :97045–97055, 2020.

[12] Rubby Aworka, Lontsi Saadio Cedric, Wilfried Yves Hamilton Adoni, Jérémie Thouakesseh Zoueu, Franck Kalala Mutombo, Charles Lebon Mberi Kimpolo, Tarik Nahhal, and Moez Krichen. Agricultural decision system based on advanced machine learning models for yield prediction : Case of east african countries. *Smart Agricultural Technology*, 2 :100048, 2022.

[13] Malti Bansal and Priya. Performance comparison of mqtt and coap protocols in different simulation environments. *Inventive Communication and Computational Technologies : Proceedings of ICICCT 2020*, pages 549–560, 2021.

[14] Shanay Behrad, Emmanuel Bertin, Stéphane Tuffin, and Noel Crespi. A new scalable authentication and access control mechanism for 5g-based iot. *Future Generation Computer Systems*, 108 :46–61, 2020.

[15] Randeep Bhatia, Steven Benno, Jairo Esteban, TV Lakshman, and John Grogan. Unsupervised machine learning for network-centric anomaly detection in iot. In *Proceedings of the 3rd acm conext workshop on big data, machine learning and artificial intelligence for data communication networks*, pages 42–48, 2019.

[16] Zhuming Bi, Yan Jin, Paul Maropoulos, Wen-Jun Zhang, and Lihui Wang. Internet of things (iot) and big data analytics (bda) for digital manufacturing (dm). *International Journal of Production Research*, 61(12) :4004–4021, 2023.

[17] Wadii Boulila, Maha Driss, Eman Alshanqiti, Mohamed Al-Sarem, Faisal Saeed, and Moez Krichen. Weight initialization techniques for deep learning algorithms in remote sensing : Recent trends and future perspectives. *Advances on Smart and Soft Computing : Proceedings of ICACIn 2021*, pages 477–484, 2022.

[18] Jamal Bzai, Furqan Alam, Arwa Dhafer, Miroslav Bojović, Saleh M Altowaijri, Imran Khan Niazi, and Rashid Mehmood. Machine learning-enabled internet of things (iot) : Data, applications, and industry perspective. *Electronics*,

11(17) :2676, 2022.

[19] Ayan Chatterjee and Bestoun S Ahmed. Iot anomaly detection methods and applications : A survey. *Internet of Things*, 19 :100568, 2022.

[20] Bharat S Chaudhari, Marco Zennaro, and Suresh Borkar. Lpwan technologies : Emerging application characteristics, requirements, and design considerations. *Future Internet*, 12(3) :46, 2020.

[21] Ying Chen, Ning Zhang, Yongchao Zhang, Xin Chen, Wen Wu, and Xuemin Shen. Energy efficient dynamic offloading in mobile edge computing for internet of things. *IEEE Transactions on Cloud Computing*, 9(3) :1050–1060, 2019.

[22] Yongliang Cheng, Yan Xu, Hong Zhong, and Yi Liu. Leveraging semisupervised hierarchical stacking temporal convolutional network for anomaly detection in iot communication. *IEEE Internet of Things Journal*, 8(1) :144–155, 2021.

[23] Premkumar Chithaluru, Thompson Stephan, Manoj Kumar, and Anand Nayyar. An enhanced energy-efficient fuzzy-based cognitive radio scheme for iot. *Neural Computing and Applications*, 34(21) :19193–19215, 2022.

[24] Fabián Constante Nicolalde, Fernando Silva, Boris Herrera, and António Pereira. Big data analytics in iot : challenges, open research issues and tools. *Trends and Advances in Information Systems and Technologies : Volume 2 6*, pages 775–788, 2018.

[25] Andrew A Cook, Göksel Mısırlı, and Zhong Fan. Anomaly detection for iot time-series data : A survey. *IEEE Internet of Things Journal*, 7(7) :6481–6494, 2019.

[26] Andrew A. Cook, Göksel Mısırlı, and Zhong Fan. Anomaly detection for iot time-series data : A survey. *IEEE Internet of Things Journal*, 7(7) :6481–6494, 2020.

[27] Soumya Kanti Datta and Christian Bonnet. An edge computing architecture integrating virtual iot devices. In *2017 IEEE 6th Global Conference on Consumer Electronics (GCCE)*, pages 1–3. IEEE, 2017.

[28] Cristiano Antonio de Souza, Carlos Becker Westphall, Renato Bobsin Machado, Leandro Loffi, Carla Merkle Westphall, and Guilherme Arthur Geronimo. Intrusion detection and prevention in fog based iot environments : A systematic literature review. *Computer Networks*, 214 :109154, 2022.

[29] Olivier Debauche, Saïd Mahmoudi, and Adriano Guttadauria. A new edge computing architecture for iot and multimedia data management. *Information*, 13(2) :89, 2022.

[30] Abebe Diro, Naveen Chilamkurti, Van-Doan Nguyen, and Will Heyne. A comprehensive study of anomaly detection schemes in iot networks using machine learning algorithms. *Sensors*, 21(24) :8320, 2021.

[31] Nilima Dongre, Mohammad Atique, Zeba A Shaik, and Atul D Raut. A survey on security issues and secure frameworks in internet of things (iot). In *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pages 173–181. IEEE, 2022.

[32] Anastasius Gavras. Factoring big data into the business case for iot. *Designing, Developing, and Facilitating Smart Cities : Urban Design to IoT Solutions*, pages 49–59, 2017.

[33] Apostolos Gerodimos, Leandros Maglaras, Mohamed Amine Ferrag, Nick Ayres, and Ioanna Kantzavelou. Iot : Communication protocols and security threats. *Internet of Things and Cyber-Physical Systems*, 2023.

[34] Isaias Gonzalez, Antonio José Calderón, and Francisco Javier Folgado. Iot real time system for monitoring lithium-ion battery long-term operation in microgrids. *Journal of Energy Storage*, 51 :104596, 2022.

[35] Yosra Hajjaji, Wadii Boulila, Imed Riadh Farah, Imed Romdhani, and Amir Hussain. Big data and iot-based applications in smart environments : A systematic review. *Computer Science Review*, 39 :100318, 2021.

[36] Najmul Hassan, Saira Gillani, Ejaz Ahmed, Ibrar Yaqoob, and Muhammad Imran. The role of edge computing in internet of things. *IEEE communications magazine*, 56(11) :110–115, 2018.

[37] Jetmir Haxhibeqiri, Eli De Poorter, Ingrid Moerman, and Jeroen Hoebeke. A survey of lorawan for iot : From technology to application. *Sensors*, 18(11) :3995, 2018.

[38] Olfa Hrizi, Karim Gasmi, Ibtihel Ben Ltaifa, Hamoud Alshammari, Hanen Karamti, Moez Krichen, Lassaad Ben Ammar, and Mahmood A Mahmood. Tuberculosis disease diagnosis based on an optimized machine learning model. *Journal of Healthcare Engineering*, 2022, 2022.

[39] Waleed Noori Hussein, Haider Noori Hussain, Hisham Noori Hussain, and Amer Q Mallah. A deployment model for iot devices based on fog computing for data management and analysis. *Wireless Personal Communications*, pages 1–13, 2023.

[40] Ali Kadhum Idrees and Ali Kadhum M Al-Qurabat. Energy-efficient data transmission and aggregation protocol in periodic sensor networks based fog computing. *Journal of Network and Systems Management*, 29(1) :4, 2021.

[41] Alireza Izaddoost and Matthew Siewierski. Energy efficient data transmission in iot platforms. *Procedia Computer Science*, 175 :387–394, 2020.

[42] Rateb Jabbar, Mohammed Shinoy, Mohamed Kharbeche, Khalifa Al-Khalifa, Moez Krichen, and Kamel Barkaoui. Urban traffic monitoring and modeling system : An iot solution for enhancing road safety. In *2019 international conference on internet of things, embedded systems and communications (iintec)*, pages 13–18. IEEE, 2019.

[43] Jaejin Jang, Im Y Jung, and Jong Hyuk Park. An effective handling of secure data stream in iot. *Applied Soft Computing*, 68 :811–820, 2018.

[44] Amir Javadpour, Pedro Pinto, Forough Ja'fari, and Weizhe Zhang. Dmaidps : a distributed multi-agent intrusion detection and prevention system for cloud iot environments. *Cluster Computing*, 26(1) :367–384, 2023.

[45] Matthieu Kanj, Vincent Savaux, and Mathieu Le Guen. A tutorial on nb-iot

physical layer design. *IEEE Communications Surveys & Tutorials*, 22(4) :2408–2446, 2020.

[46] Aimad Karkouch, Hassan Al Moatassime, Hajar Mousannif, and Thomas Noel. Data quality enhancement in internet of things environment. In *2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA)*, pages 1–8. IEEE, 2015.

[47] Aimad Karkouch, Hajar Mousannif, Hassan Al Moatassime, and Thomas Noel. Data quality in internet of things : A state-of-the-art survey. *Journal of Network and Computer Applications*, 73 :57–81, 2016.

[48] Aimad Karkouch, Hajar Mousannif, Hassan Al Moatassime, and Thomas Noel. A model-driven framework for data quality management in the internet of things. *Journal of Ambient Intelligence and Humanized Computing*, 9 :977–998, 2018.

[49] MM Kashid, KJ Karande, and AO Mulani. Iot-based environmental parameter monitoring using machine learning approach. In *Proceedings of the International Conference on Cognitive and Intelligent Computing : ICCIC 2021, Volume 1*, pages 43–51. Springer, 2022.

[50] Shivanjali Khare and Michael Totaro. Big data in iot. In *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pages 1–7, 2019.

[51] Igor Khokhlov and Leon Reznik. Knowledge graph in data quality evaluation for iot applications. In *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, pages 1–6, 2020.

[52] Sunho Kim, Ricardo Pérez-Castillo, Ismael Caballero, and Downgwoo Lee. Organizational process maturity model for iot data quality management. *Journal of Industrial Information Integration*, 26 :100256, 2022.

[53] Linghe Kong, Jinlin Tan, Junqin Huang, Guihai Chen, Shuaitian Wang, Xi Jin, Peng Zeng, Muhammad Khan, and Sajal K Das. Edge-computing-driven internet of things : A survey. *ACM Computing Surveys*, 55(8) :1–41, 2022.

[54] Hermann Kopetz and Wilfried Steiner. Internet of things. In *Real-time systems : design principles for distributed embedded applications*, pages 325–341. Springer, 2022.

[55] Moez Krichen. *Model-based testing for real-time systems.* PhD thesis, PhD thesis, PhD thesis, Universit Joseph Fourier (December 2007), 2007.

[56] Moez Krichen. A formal framework for conformance testing of distributed real-time systems. In *International Conference On Principles Of Distributed Systems*, pages 139–142. Springer, 2010.

[57] Moez Krichen. A formal framework for black-box conformance testing of distributed real-time systems. *International Journal of Critical Computer-Based Systems*, 3(1-2) :26–43, 2012.

[58] Moez Krichen. *Contributions to model-based testing of dynamic and distributed real-time systems.* PhD thesis, École Nationale d'Ingénieurs de Sfax (Tunisie), 2018.

[59] Moez Krichen. How artificial intelligence can revolutionize software testing techniques. In *International Conference on Innovations in Bio-Inspired Computing and Applications*, pages 189–198. Springer Nature Switzerland Cham, 2022.

[60] Moez Krichen. Convolutional neural networks : A survey. *Computers*, 12(8) :151, 2023.

[61] Moez Krichen. Deep reinforcement learning. In *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, pages 1–7. IEEE, 2023.

[62] Moez Krichen. Formal methods and validation techniques for ensuring automotive systems security. *Information*, 14(12) :666, 2023.

[63] Moez Krichen. Generative adversarial networks. In *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, pages 1–7. IEEE, 2023.

[64] Moez Krichen. Strengthening the security of smart contracts through the power of artificial intelligence. *Computers*, 12(5) :107, 2023.

[65] Moez Krichen. A survey on formal verification and validation techniques for internet of things. *Applied Sciences*, 13(14) :8122, 2023.

[66] Moez Krichen, Wilfried Yves Hamilton Adoni, Alaeddine Mihoub, Mohammed Y Alzahrani, and Tarik Nahhal. Security challenges for drone communications : Possible threats, attacks and countermeasures. In *2022 2nd International Conference of Smart Systems and Emerging Technologies (SMARTTECH)*, pages 184–189. IEEE, 2022.

[67] Moez Krichen, Meryem Ammi, Alaeddine Mihoub, and Qasem Abu Al-Haija. Short survey on using blockchain technology in modern wireless networks, iot and smart grids. In *International Conference on Cybersecurity, Cybercrimes, and Smart Emerging Technologies*, pages 163–173. Springer International Publishing Cham, 2022.

[68] Moez Krichen, Omar Cheikhrouhou, Mariam Lahami, Roobaea Alroobaea, and Afef Jmal Maâlej. Towards a model-based testing framework for the security of internet of things for smart city applications. In *Smart Societies, Infrastructure, Technologies and Applications : First International Conference, SCITA 2017, Jeddah, Saudi Arabia, November 27–29, 2017, Proceedings 1*, pages 360–365. Springer International Publishing, 2018.

[69] Moez Krichen, Mariam Lahami, and Qasem Abu Al-Haija. Formal methods for the verification of smart contracts : A review. In *2022 15th International Conference on Security of Information and Networks (SIN)*, pages 01–08. IEEE, 2022.

[70] Moez Krichen, Seifeddine Mechti, Roobaea Alroobaea, Elyes Said, Parminder Singh, Osamah Ibrahim Khalaf, and Mehedi Masud. A formal testing model for operating room control system using internet of things. *Computers, Materials & Continua*, 66(3) :2997–3011, 2021.

[71] Moez Krichen and Stavros Tripakis. Real-time testing with timed automata

testers and coverage criteria. In *Formal Techniques, Modelling and Analysis of Timed and Fault-Tolerant Systems*, pages 134–151. Springer, Berlin, Heidelberg, 2004.

[72] Moez Krichen and Stavros Tripakis. State identification problems for timed automata. In *Testing of Communicating Systems : 17th IFIP TC6/WG 6.1 International Conference, TestCom 2005, Montreal, Canada, May 31-June, 2005. Proceedings 17*, pages 175–191. Springer Berlin Heidelberg, 2005.

[73] Moez Krichen and Stavros Tripakis. Interesting properties of the real-time conformance relation tioco. In *International Colloquium on Theoretical Aspects of Computing*, pages 317–331. Springer Berlin Heidelberg Berlin, Heidelberg, 2006.

[74] Anuj Kumar, Vinod Jain, and Anupam Yadav. A new approach for security in cloud data storage for iot applications using hybrid cryptography technique. In *2020 international conference on power electronics & IoT applications in renewable energy and its control (PARC)*, pages 514–517. IEEE, 2020.

[75] Umesh Kumar, Parul Verma, and Syed Qamar Abbas. Bringing edge computing into iot architecture to improve iot network performance. In *2021 International Conference on Computer Communication and Informatics (ICCCI)*, pages 1–5. IEEE, 2021.

[76] Mariam Lahami, Fairouz Fakhfakh, Moez Krichen, and Mohamed Jmaiel. Towards a ttcn-3 test system for runtime testing of adaptable and distributed systems. In *Testing Software and Systems : 24th IFIP WG 6.1 International Conference, ICTSS 2012, Aalborg, Denmark, November 19-21, 2012. Proceedings 24*, pages 71–86. Springer Berlin Heidelberg, 2012.

[77] Mariam Lahami and Moez Krichen. A survey on runtime testing of dynamically adaptable and distributed systems. *Software Quality Journal*, 29(2) :555–593, 2021.

[78] Mariam Lahami, Moez Krichen, Hajer Barhoumi, and Mohamed Jmaiel. Selective test generation approach for testing dynamic behavioral adaptations. In *Testing Software and Systems : 27th IFIP WG 6.1 International Conference, ICTSS 2015, Sharjah and Dubai, United Arab Emirates, November 23-25, 2015, Proceedings 27*, pages 224–239. Springer International Publishing, 2015.

[79] Mariam Lahami, Moez Krichen, and Mohamed Jmaïel. Runtime testing approach of structural adaptations for dynamic and distributed systems. *International Journal of Computer Applications in Technology*, 51(4) :259–272, 2015.

[80] Mariam Lahami, Afef Jmal Maâlej, Moez Krichen, and Mohamed Amin Hammami. A comprehensive review of testing blockchain oriented software. *ENASE*, 182 :355–62, 2022.

[81] Fangyu Li, Yang Shi, Aditya Shinde, Jin Ye, and Wenzhan Song. Enhanced cyber-physical security in internet of things through energy auditing. *IEEE Internet of Things Journal*, 6(3) :5224–5231, 2019.

[82] Xiaoming Li, Hao Liu, Weixi Wang, Ye Zheng, Haibin Lv, and Zhihan Lv. Big data analysis of the internet of things in the digital twins of smart city based on deep learning. *Future Generation Computer Systems*, 128 :167–177, 2022.

[83] Caihua Liu, Patrick Nitschke, Susan P Williams, and Didar Zowghi. Data quality and the internet of things. *Computing*, 102(2) :573–599, 2020.

[84] Yi Liu, Neeraj Kumar, Zehui Xiong, Wei Yang Bryan Lim, Jiawen Kang, and Dusit Niyato. Communication-efficient federated learning for anomaly detection in industrial internet of things. In *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, pages 1–6, 2020.

[85] Zhipeng Liu, Niraj Thapa, Addison Shaver, Kaushik Roy, Xiaohong Yuan, and Sajad Khorsandroo. Anomaly detection on iot network intrusion using machine learning. In *2020 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD)*, pages 1–5, 2020.

[86] Elio Jordan Lopes, Shaolin Kataria, Shashank Keshav, Sumaiya Thaseen Ikram, Muhammad Rukunuddin Ghalib, Achyut Shankar, and Moez Krichen. Live video streaming service with pay-as-you-use model on ethereum blockchain and interplanetary file system. *Wireless Networks*, 28(7) :3111–3125, 2022.

[87] Afef Jmal Maâlej, Manel Hamza, Moez Krichen, and Mohamed Jmaiel. Automated significant load testing for ws-bpel compositions. In *2013 IEEE sixth international conference on software testing, verification and validation workshops*, pages 144–153. IEEE, 2013.

[88] Afef Jmal Maâlej and Moez Krichen. A model based approach to combine load and functional tests for service oriented architectures. In *VECoS*, pages 123–140, 2016.

[89] Afef Jmal Maâlej, Moez Krichen, and Mohamed Jmaiel. Conformance testing of ws-bpel compositions under various load conditions. In *2012 IEEE 36th annual computer software and applications conference*, pages 371–371. IEEE, 2012.

[90] Afef Jmal Maâlej, Mariam Lahami, Moez Krichen, and Mohamed Jmaïel. Distributed and resource-aware load testing of ws-bpel compositions. In *ICEIS (2)*, pages 29–38, 2018.

[91] Praveen Kumar Reddy Maddikunta, Quoc-Viet Pham, Dinh C Nguyen, Thien Huynh-The, Ons Aouedi, Gokul Yenduri, Sweta Bhattacharya, and Thippa Reddy Gadekallu. Incentive techniques for the internet of things : a survey. *Journal of Network and Computer Applications*, 206 :103464, 2022.

[92] Mohammad Saeid Mahdavinejad, Mohammadreza Rezvan, Mohammadamin Barekatain, Peyman Adibi, Payam Barnaghi, and Amit P Sheth. Machine learning for internet of things data analysis : A survey. *Digital Communications and Networks*, 4(3) :161–175, 2018.

[93] Priyanka Mall, Md Zakirul Alam Bhuiyan, and Ruhul Amin. A lightweight secure communication protocol for iot devices using physically unclonable function. In *Security, Privacy, and Anonymity in Computation, Communication, and Storage : 12th International Conference, SpaCCS 2019, Atlanta, GA, USA, July 14–17, 2019, Proceedings 12*, pages 26–35. Springer, 2019.

[94] Mohsen Marjani, Fariza Nasaruddin, Abdullah Gani, Ahmad Karim, Ibrahim Abaker Targio Hashem, Aisha Siddiqa, and Ibrar Yaqoob. Big iot data analytics : Architecture, opportunities, and open research challenges. *IEEE Access*, 5 :5247–

5261, 2017.

[95] Muhammad Sheraz Mehmood, Muhammad Rehman Shahid, Abid Jamil, Rehan Ashraf, Toqeer Mahmood, and Aatif Mehmood. A comprehensive literature review of data encryption techniques in cloud computing and iot environment. In *2019 8th International Conference on Information and Communication Technologies (ICICT)*, pages 54–59. IEEE, 2019.

[96] Yuqing Mo. A data security storage method for iot under hadoop cloud computing platform. *International Journal of Wireless Information Networks*, 26(3) :152–157, 2019.

[97] Mehdi Mohammadi, Ala Al-Fuqaha, Sameh Sorour, and Mohsen Guizani. Deep learning for iot big data and streaming analytics : A survey. *IEEE Communications Surveys & Tutorials*, 20(4) :2923–2960, 2018.

[98] Ahmed Afif Monrat, Olov Schelén, and Karl Andersson. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access*, 7 :117134–117151, 2019.

[99] Di Mu, Yunpeng Ge, Mo Sha, Steve Paul, Niranjan Ravichandra, and Souma Chowdhury. Adaptive radio and transmission power selection for internet of things. In *2017 IEEE/ACM 25th International Symposium on Quality of Service (IWQoS)*, pages 1–10. IEEE, 2017.

[100] Manoj Muniswamaiah, Tilak Agerwala, and Charles C Tappert. Fog computing and the internet of things (iot) : a review. In *2021 8th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2021 7th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, pages 10–12. IEEE, 2021.

[101] Fabián Constante Nicolalde, Fernando Silva, Boris Herrera, and Antonio Pereira. Big data analysis tools in iot and their challenges in open researches. In *2018 13th Iberian Conference on Information Systems and Technologies (CISTI)*, pages 1–6, 2018.

[102] Abiodun Esther Omolara, Abdullah Alabdulatif, Oludare Isaac Abiodun, Moatsum Alawida, Abdulatif Alabdulatif, Humaira Arshad, et al. The internet of things security : A survey encompassing unexplored areas and new insights. *Computers & Security*, 112 :102494, 2022.

[103] Antonino Orsino, Giuseppe Araniti, Leonardo Militano, Jesus Alonso-Zarate, Antonella Molinaro, and Antonio Iera. Energy efficient iot data collection in smart cities exploiting d2d communications. *Sensors*, 16(6) :836, 2016.

[104] Ricardo Perez-Castillo, Ana G. Carretero, Moises Rodriguez, Ismael Caballero, Mario Piattini, Alejandro Mate, Sunho Kim, and Dongwoo Lee. Data quality best practices in iot environments. In *2018 11th International Conference on the Quality of Information and Communications Technology (QUATIC)*, pages 272–275, 2018.

[105] Antonis Protopsaltis, Panagiotis Sarigiannidis, Dimitrios Margounakis, and Anastasios Lytos. Data visualization in internet of things : tools, methodologies, and challenges. In *Proceedings of the 15th international conference on availability,*

reliability and security, pages 1–11, 2020.

[106] Mohammad Saidur Rahman, MAP Chamikara, Ibrahim Khalil, and Abdelaziz Bouras. Blockchain-of-blockchains : An interoperable blockchain platform for ensuring iot data integrity in smart city. *Journal of Industrial Information Integration*, 30 :100408, 2022.

[107] Bharti Rana and Yashwant Singh. Duty-cycling techniques in iot : Energy-efficiency perspective. In *Recent Innovations in Computing : Proceedings of ICRIC 2021, Volume 1*, pages 505–512. Springer, 2022.

[108] Abderahman Rejeb, Karim Rejeb, Steve Simske, Horst Treiblmaier, and Suhaiza Zailani. The big picture on the internet of things and the smart city : a review of what we know and what we need to know. *Internet of Things*, 19 :100565, 2022.

[109] Syed Rizvi, Tatiana Zwerling, Benjamin Thompson, Shawn Faiola, Shakir Campbell, Stephen Fisanick, and Codi Hutnick. A modular framework for auditing iot devices and networks. *Computers & Security*, page 103327, 2023.

[110] Tausifa Jan Saleem and Mohammad Ahsan Chishti. Deep learning for internet of things data analytics. *Procedia computer science*, 163 :381–390, 2019.

[111] K Sakthidasan Sankaran and Bong-Hyun Kim. Deep learning based energy efficient optimal rmc-cnn model for secured data transmission and anomaly detection in industrial iot. *Sustainable Energy Technologies and Assessments*, 56 :102983, 2023.

[112] Muzafer H Saračević, Saša Z Adamović, Vladislav A Miškovic, Mohamed Elhoseny, Nemanja D Maček, Mahmoud Mohamed Selim, and K Shankar. Data encryption for internet of things applications based on catalan objects and two combinatorial structures. *IEEE Transactions on Reliability*, 70(2) :819–830, 2020.

[113] M Sathya, M Jeyaselvi, Lalitha Krishnasamy, Mohammad Mazyad Hazzazi, Prashant Kumar Shukla, Piyush Kumar Shukla, and Stephen Jeswinde Nuagah. A novel, efficient, and secure anomaly detection technique using dwu-odbn for iot-enabled multimedia communication systems. *Wireless Communications and Mobile Computing*, 2021 :1–12, 2021.

[114] Eryk Schiller, Andy Aidoo, Jara Fuhrer, Jonathan Stahl, Michael Ziörjen, and Burkhard Stiller. Landscape of iot security. *Computer Science Review*, 44 :100467, 2022.

[115] Jahanzeb Shahid, Rizwan Ahmad, Adnan K Kiani, Tahir Ahmad, Saqib Saeed, and Abdullah M Almuhaideb. Data protection and privacy of the internet of healthcare things (iohts). *Applied Sciences*, 12(4) :1927, 2022.

[116] Cuili Shao, Yonggang Yang, Sapna Juneja, and Tamizharasi GSeetharam. Iot data visualization for business intelligence in corporate finance. *Information Processing & Management*, 59(1) :102736, 2022.

[117] Shuaiyong Shen, Yang Yang, and Ximeng Liu. Toward data privacy preservation with ciphertext update and key rotation for iot. *Concurrency and Computation : Practice and Experience*, 35(20) :e6729, 2023.

[118] Simar Preet Singh, Anand Nayyar, Rajesh Kumar, and Anju Sharma. Fog compu-

ting : from architecture to edge computing and big data processing. *The Journal of Supercomputing*, 75 :2070–2105, 2019.

[119] Michael Sober, Giulia Scaffino, Stefan Schulte, and Salil S Kanhere. A blockchain-based iot data marketplace. *Cluster Computing*, pages 1–23, 2022.

[120] Pinyaphat Tasatanattakool and Chian Techapanupreeda. Blockchain : Challenges and applications. In *2018 International Conference on Information Networking (ICOIN)*, pages 473–475. IEEE, 2018.

[121] Aurelle Tchagna Kouanou, Christian Tchito Tchapga, Michael Sone Ekonde, Valery Monthe, Brice Anicet Mezatio, Josépha Manga, Gael R Simo, and Yves Muhozam. Securing data in an internet of things network using blockchain technology : smart home case. *SN Computer Science*, 3(2) :167, 2022.

[122] Priyanka Vashisht, Vijay Kumar, and Meghna Sharma. Iot, big data, and analytics : Challenges and opportunities. *Predictive Analytics*, pages 151–177, 2021.

[123] Shuo Wan, Jiaxun Lu, Pingyi Fan, and Khaled B Letaief. Toward big data processing in iot : Path planning and resource management of uav base stations in mobile-edge computing system. *IEEE Internet of Things Journal*, 7(7) :5995–6009, 2019.

[124] Li Yang and Abdallah Shami. Iot data analytics in dynamic environments : From an automated machine learning perspective. *Engineering Applications of Artificial Intelligence*, 116 :105366, 2022.

[125] Eljona Zanaj, Giuseppe Caso, Luca De Nardis, Alireza Mohammadpour, Özgü Alay, and Maria-Gabriella Di Benedetto. Energy efficiency in short and wide-area iot technologies—a survey. *Technologies*, 9(1) :22, 2021.

[126] Lina Zhang, Dongwon Jeong, and Sukhoon Lee. Data quality management in the internet of things. *Sensors*, 21(17) :5834, 2021.

[127] Xiu Zhang, Hao Qi, Xin Zhang, and Liang Han. Energy-efficient resource allocation and data transmission of cell-free internet of things. *IEEE Internet of Things Journal*, 8(20) :15107–15116, 2021.

[128] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. Blockchain challenges and opportunities : A survey. *International journal of web and grid services*, 14(4) :352–375, 2018.

[129] Yong Zhong, Liang Chen, Changlin Dan, and Amin Rezaeipanah. A systematic survey of data mining and big data analysis in internet of things. *The Journal of Supercomputing*, 78(17) :18405–18453, 2022.

[130] Salah Zidi, Alaeddine Mihoub, Saeed Mian Qaisar, Moez Krichen, and Qasem Abu Al-Haija. Theft detection dataset for benchmarking and machine learning based classification in a smart grid environment. *Journal of King Saud University-Computer and Information Sciences*, 35(1) :13–25, 2023.