Solutions Sécurisées et Écoénergétiques pour un Internet des Objets Vert

TOUAHRIA MILIANI Mohamed Yacine, KANDI Mohamed Ali, LARABA Abir, LABORDE Romain
IRIT, Université de Toulouse, CNRS
Toulouse, France
Mohamed.Touahria-Miliani@irit.fr, Mohamed-Ali.Kandi@irit.fr, Abir.Laraba@irit.fr, Romain.Laborde@irit.fr

***Abstract*—D'ici 2030, le nombre de dispositifs IoT atteindra les 125 milliards, selon IHS Markit [1]. Cette expansion rapide entraîne une surconsommation d'énergie préoccupante soulignant l'urgence de développer des solutions IoT énergétiquement efficace. Parallèlement, le fait que les objets connectés soient souvent caractérisés par des ressources limitées constitue un obstacle majeur au développement de solutions de sécurité efficaces. En plus des problématiques déjà complexes de sécurité et d'environnement, s'ajoute un défi supplémentaire majeur : l'interdépendance de ces deux contraintes, où optimiser l'un peut compromettre l'autre. De nombreux travaux ont tenté de développer des mécanismes de sécurité légers, en déléguant les calculs intensifs à des machines plus puissantes. Cependant, ces solutions se limitent à la réduction de la consommation énergétique au niveau des nœuds à ressources limitées, sans prendre en compte l'impact environnemental global. L'objectif de notre recherche est donc de proposer des solutions de sécurité vertes et innovantes, alliant une sécurité accrue et une consommation énergétique réduite.**

***Index Terms*—Internet des objets, Sécurité verte, Efficacité énergétique, Durabilité**

I. Introduction

L'*IoT* est une technologie qui offre des avantages sociaux et économiques [2] et qui se retrouve dans une multitude de secteurs, notamment la santé, les transports, l'agriculture, et bien d'autres. Un des facteurs importants ayant contribué à la popularité des dispositifs IoT est leur fonctionnement sur batteries, ce qui permet une installation facile et une portabilité accrue, en particulier dans des endroits éloignés comme les sous-marins ou les sommets de montagnes. Cependant, cette évolution prodigieuse a engendré deux problèmes majeurs de nature contradictoire, c'est-à-dire qu'il est difficile de privilégier l'un sans sacrifier en partie l'autre. Ces problèmes concernent la sécurité et la consommation énergétique.

D'un côté, les dispositifs consomment d'énormes quantités d'électricité à l'échelle mondiale. Comme l'a indiqué l'Agence Internationale de l'Énergie (IEA) [3], les appareils connectés ont consommé annuellement 500 TWh d'énergie en 2020, soit une quantité comparable à la consommation de la France. Dans ce contexte, de nombreux travaux se sont concentrés sur la collecte d'énergie disponible dans l'environnement où les dispositifs sont installés, afin qu'ils puissent se recharger sans intervention humaine, maintenance ou remplacement [4]. D'autres chercheurs ont étudié comment prolonger la durée de vie des réseaux IoT alimentés par batteries en prenant en compte l'énergie restante dans chaque nœud. Par exemple, les auteurs de [5] ont développé un protocole de routage sensible à l'énergie, qui dirige les paquets à travers les chemins ayant le plus d'énergie résiduelle, et les auteurs de [6] ont proposé un algorithme de Duty Cycling, qui fait partie du schéma de veille/réveil, où un nœud reste en veille pendant sa période d'inactivité. Cette dynamique a donné naissance au concept d'*IoT vert*, visant à minimiser ou éliminer l'impact environnemental de l'Internet des objets en prenant en compte tous ses aspects, depuis la phase de conception jusqu'au recyclage et à la destruction.

De l'autre côté, la sécurité des réseaux IoT est un autre sujet préoccupant et complexe en raison de leur nature hétérogène. Cela inclut la diversité des types de dispositifs, des systèmes d'exploitation et des protocoles de communication. De plus, les objets connectés, tels que les microcontrôleurs, sont limités en ressources et possèdent de faibles capacités de calcul et de stockage en termes de CPU, de cache, et de RAM. Cela rend difficile l'exécution et le déploiement de mécanismes de sécurité sophistiqués sur ces réseaux, tels que les programmes anti-malware et les systèmes de détection et de prévention des intrusions. De nombreux articles ont été publiés pour traiter le problème de la sécurité dans les réseaux IoT, en tenant compte des limitations en termes de capacités de traitement et de stockage, notamment [7, 8, 5, 9, 10, 11, 12, 13]. Cependant, ces travaux négligent l'aspect écologique de la sécurité et se concentrent uniquement sur la sécurisation du réseau IoT, ce qui relève du concept de *sécurité pour l'IoT Vert*. Ce manque a engendré l'émergence d'une nouvelle perspective, passant de l'*IoT vert* vers une *sécurité verte* intégrée au sein de l'écosystème IoT.

La *sécurité verte* définit et examine les solutions de sécurité sous un angle sensible à l'énergie, ce qui constitue une proposition plus complexe, car la réduction de la consommation est toujours évaluée par rapport au niveau de sécurité atteint [14]. Des travaux ont cherché à réduire la consommation énergétique de leurs solutions de sécurité, mais se sont concentrés sur les noeuds à ressources limitées et sans prendre en compte l'impact environnemental global au niveau du réseau [15, 16, 17, 18]. Elles délestent souvent les calculs complexes à des machines plus puissantes adoptant des architectures de calcul en périphérie (edge) et en brouillard (fog).

L'objectif de notre thèse est de fournir des outils permettant

aux architectes IoT de proposer des solutions offrant un compromis optimal entre sécurité et consommation énergétique, en fonction du niveau de risque et de la capacité des nœuds. Cela conduit à la conception de solutions de sécurisation écologiques, ayant un impact positif sur la phase d'utilisation du numérique, laquelle représente une part significative de la consommation énergétique globale — à savoir 21% selon une étude menée par l'ADEME et l'Arcep [19]. Pour ce faire, nous nous concentrerons non seulement sur la couche de perception, où les ressources de traitement et de calcul sont les plus limitées, mais aussi sur la couche réseau (Voir la Section II-A pour les détails de l'architecture des réseaux IoT). Dans cet article, nous présentons nos travaux en cours durant cette première année de doctorat, visant à développer une métrique permettant d'estimer de manière quantitative la consommation d'énergie des solutions de sécurité, avant même leur déploiement. Nous présenterons également nos perspectives futures, qui s'appuient sur cette métrique, et visent à établir des lignes directrices pour le développement d'approches de sécurité verte, afin de réduire leur impact écologique dans l'IoT.

II. Contexte

Dans cette section, nous définissons le cadre de notre thèse en présentant tout d'abord l'architecture des réseaux IoT, puis en introduisant un concept clé : l'*IoT vert*. Nous présentons également les défis spécifiques liés à la sécurité dans l'IoT.

A. Architecture de l'IoT

L'IoT possède plusieurs architectures. L'une des plus couramment considérées est l'architecture à trois couches [20], composée de la couche de perception, de la couche réseau et de la couche application (Figure 1). La couche de perception (couche de détection) est responsable de la collecte des données et de leur transmission à la couche supérieure (la couche réseau). Cette dernière, comme son nom l'indique, assure la connexion entre les deux autres couches. Enfin, la couche application est responsable de l'analyse et du traitement des données capturées, ainsi que de la fourniture des services [20].

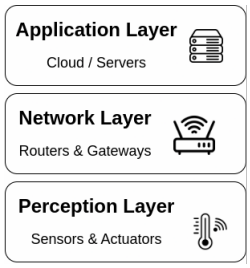

Fig. 1. Architecture IoT à trois couches [20].

B. IoT vert

L'*informatique verte* se réfère à l'étude et à la pratique de la conception, de la fabrication, de l'utilisation et de l'élimination des ordinateurs et des systèmes de manière à minimiser ou éliminer l'impact environnemental. En améliorant l'efficacité énergétique, en réduisant les émissions de gaz à effet de serre, en minimisant l'utilisation de matériaux nocifs et en favorisant la réutilisation et le recyclage, l'*informatique verte* apporte des bénéfices significatifs à l'environnement. La résolution des défis environnementaux posés par l'informatique nécessite une approche holistique qui se concentre sur quatre domaines interconnectés : la conception verte, la production verte, l'utilisation verte et l'élimination verte [21].

L'*Internet des Objets vert* est un sous-domaine de l'*informatique verte* qui se concentre uniquement sur les objets intelligents et connectés. Il vise à améliorer l'efficacité énergétique tant du logiciel que du matériel afin de réduire l'empreinte carbone des applications et services existants ou de réduire l'impact de l'IoT lui-même [22].

C. Sécurité de l'IoT

La sécurité de l'IoT et la sécurité conventionnelle partagent des similitudes et des différences, chacune ayant ses caractéristiques influencées par l'environnement et les matériaux utilisés. La sécurité conventionnelle est mise en œuvre sur des dispositifs riches en ressources, avec des algorithmes complexes et un haut niveau de sécurité, reposant sur une technologie homogène. En revanche, la sécurité de l'IoT repose sur des dispositifs à matériel limité qui privilégient des algorithmes légers et une technologie hétérogène [23]. L'hétérogénéité est justifiée par le fait que l'architecture de l'IoT est divisée en plusieurs couches composées de technologies différentes, comme expliqué précédemment, ce qui élargit la zone des menaces et des vulnérabilités du système [23]. Dans ce cadre, le NIST (National Institute of Standards and Technology) a animé plusieurs ateliers entre 2015 et 2023 dans le processus de sélection d'algorithmes de cryptographie légère qui a fini par choisir de standardiser la famille d'algorithmes de chiffrement et d'hachage ASCON en 2023[24]. Cependant, ce domaine de recherche nécessite davantage d'efforts pour atteindre un niveau de sécurité décent autre que la cryptographie légère.

III. Travaux en cours

Le premier objectif de la thèse est d'établir une métrique d'estimation de l'énergie consommée par les mécanismes de sécurité sur les deux premières couches des réseaux IoT, notamment la couche de perception et la couche réseau (Voir les détails dans la Section II-A). Cela permettra aux architectes de solutions de sécurité pour les réseaux IoT d'intégrer l'aspect énergétique dans leurs contraintes de conception, en optimisant leurs travaux jusqu'à ce qu'ils satisfassent aux exigences environnementales [25, 26].

L'optimisation de la consommation énergétique d'un système commence par une évaluation précise de l'énergie consommée par ses composants, suivie par des efforts de réduction de la consommation des composants les plus énergivores. Dans la littérature, les techniques de mesure de l'énergie consommée par un logiciel peuvent être classées en trois catégories : mesure matérielle, mesure logicielle, et modèles de consommation d'énergie [27].

La mesure matérielle repose sur des wattmètres ou compteurs de puissance externes, qui offrent une grande précision mais à un niveau grossier. En d'autres termes, il est difficile de distinguer entre la consommation du matériel et celle du logiciel, d'autant plus qu'ils ne donnent pas la consommation de chaque processus exécuté. De plus, ils sont difficiles à mettre à l'échelle et peuvent être coûteux [27]. La mesure logicielle est connue pour le profilage énergétique des applications et des processus en temps réel. Elle utilise les statistiques fournies par le système d'exploitation, telles que l'utilisation du CPU et l'espace mémoire DRAM occupé. Par exemple, dans les systèmes d'exploitation Linux, ces statistiques sont stockées dans le répertoire virtuel */proc* et organisées par le PID de chaque processus en cours d'exécution. La mesure logicielle exploite également les mesures fournies par les interfaces matérielles, comme l'interface RAPL d'Intel, qui utilise le MSR (Model-Specific Register) pour suivre la consommation énergétique du CPU pour chaque processus en cours d'exécution sur le système, ainsi que la bibliothèque NVML (Nvidia Management Library) de Nvidia pour les charges de travail des GPU [28]. La catégorie des modèles de consommation d'énergie regroupe les modèles qui estiment la consommation avant l'exécution du logiciel.

Dans le cadre de ce projet, nous cherchons à développer une métrique capable d'estimer la consommation des algorithmes de sécurité dès la phase de conception. Cette métrique aidera à la prise de décision concernant les solutions à adopter avant leur déploiement. Elle sert principalement à comparer, d'un point de vue énergétique, différents algorithmes et protocoles, tels que les algorithmes de chiffrement, les mécanismes d'authentification et de vérification.

Étant donné que la consommation d'énergie est avant tout une mesure matérielle et non logicielle, il devient possible d'évaluer les solutions de sécurité existantes à l'aide des mêmes équations. Cela se fait en modulant la consommation d'énergie des composants matériels sous une certaine charge pendant une période déterminée. Dans ce projet, nous nous limitons aux composants les plus énergivores lors de l'utilisation des appareils IoT, à savoir le processeur (CPU), la mémoire vive (RAM), l'émetteur radio, et l'interface réseau câblé.

A. Estimation de l'énergie consommée par le CPU

Pour estimer la puissance nécessaire à l'exécution d'un programme, de nombreux chercheurs ont modélisé l'énergie consommée par le processeur (CPU) à l'aide de l'apprentissage automatique. Cela se fait en capturant les statistiques fournies par le système d'exploitation, principalement le pourcentage d'utilisation du CPU, et en mesurant la consommation réelle d'énergie à l'aide d'un wattmètre externe. Un modèle est ensuite entraîné sur ces données. Par exemple, des régressions linéaires et polynomiales ont été appliquées dans [29] et les auteurs de [30] ont proposé un ensemble de modèles pour toutes les versions du Raspberry Pi. Ils ont même proposé une architecture qui automatise le processus de création d'un nouveau modèle, depuis la collecte des données jusqu'à la validation du modèle.

Une autre approche prometteuse de modélisation de l'énergie consommée par les processus dans le CPU existe. Elle consiste à utiliser une équation standard [31, 32] qui correspond à l'énergie consommée par les commutations des transistors (switching). Elle est applicable à tous les processeurs basés sur la technologie CMOS (Complementary Metal-Oxide-Semiconductor) et qui correspondent à la majorité des processeurs modernes, quel que soit l'équipement (PC, microcontrôleur, routeur, commutateur, etc.). L'équation est la suivante :

$$E = CNV^2 \tag{1}$$

où C est la capacité moyenne, une constante dépendant du matériel [33], V est la tension, et N est le nombre de cycles nécessaires à l'exécution du programme. En utilisant cette équation, nous pouvons estimer la consommation d'énergie des opérations de traitement effectuées sur le réseau, y compris, par exemple, les contrôles de sécurité supplémentaires au niveau du routeur lors de la mise en œuvre d'une solution SDN (Software Defined Networking).

B. Estimation de l'énergie consommée par la RAM

Pour estimer l'énergie consommée par la mémoire vive (RAM) lors de l'exécution d'un programme, une équation similaire à celle du CPU a été proposée dans [34]. Cette équation repose sur le fait que les DRAMs utilisent également la technologie CMOS. Les auteurs de [35] sont partis du principe que les deux principales opérations consommatrices d'énergie sont l'écriture d'un 1 dans une cellule et le rafraîchissement périodique (réécriture) du 1 pour éviter sa disparition. Ils ont développé un circuit équivalent de la cellule DRAM et ont ensuite déduit une équation pour l'énergie consommée par la RAM lors d'une seule opération (écriture ou rafraîchissement). L'énergie totale consommée par la RAM pour un programme est obtenue en multipliant l'énergie dépensée pour une seule opération par le nombre total de bits 1. Pour estimer ce nombre, ils ont proposé un modèle probabiliste prédisant le nombre de bits 1 écrits sur une période donnée.

Il existe des modèles d'estimation de l'énergie plus précis pour les DRAMs, en particulier ceux développés par les fabricants. Par exemple, Micron Technology fournit un ensemble de calculateurs de puissance pour plusieurs versions et architectures de RAM, notamment DDR4, LPDDR4, et d'autres [36]. Ces calculateurs de puissance sont essentiellement des fichiers XLSM où différentes spécifications peuvent être configurées.

C. Estimation de l'énergie consommée par l'émetteur radio

Pour estimer l'énergie consommée par les émetteurs radio, l'équation proposée dans [31] repose uniquement sur l'électronique de l'émetteur. Cela signifie que l'estimation est indépendante du protocole de communication utilisé (Bluetooth, LoRa, Zigbee, etc.). Le modèle est le suivant :

$$E = bE_{elec} + bd_{ij}^{n}E_{amp} \tag{2}$$

où E_{elec} est l'énergie dissipée pour transmettre ou recevoir des paquets, E_{amp} est l'énergie utilisée pour amplifier le signal, d_{ij} est la distance entre le nœud i et le nœud j, et n est un paramètre égal à 2 pour les courtes distances et à 4 sinon. Comme on peut le voir, le modèle est paramétré par le nombre de bits à envoyer ou à recevoir b, ce qui nous permet de ne prendre en compte que les bits liés à la sécurité.

D. Estimation de l'énergie consommée par l'interface réseau

Enfin, pour l'interface réseau câblé (Ethernet), les auteurs de [33] se sont basés sur la documentation des fabricants pour obtenir les valeurs de consommation énergétique pour la transmission de données sur une certaine durée souvent égale à 1 seconde, en fonction du mode de débit de la carte réseau (eg. 10Mbs, 100Mbs). Ils ont formulé la puissance consommée par l'interface réseau pour la communication d'un processus comme suit :

$$P = \frac{\sum_{i \in states} t_i P_i d}{t_{total}} \tag{3}$$

où P_{state} représente la consommation d'énergie de la carte réseau dans l'état i (spécifié par le fabricant), t_i sa durée, d est la durée du cycle de surveillance, et t_{total} correspond à la durée totale passée à transmettre des données.

Pour valider ces équations, un wattmètre externe est mis en œuvre à travers une série de scénarios variés où différents mécanismes de sécurité sont employés. Ces équations sont indépendantes du nature de matériel utilisé (Routeur, micro-contrôleur, passerelle,..), ce qui permet l'évaluation d'un large éventail de solutions. Certes, d'autres paramètres entrent en jeu pour certains équipements, comme les routeurs et les commutateurs, où le châssis et les lignes de cartes sont pris en compte [37]. Cependant, dans le cadre de cette thèse, nous nous focalisons sur le coût de la sécurité et non sur le coût global. Il est possible de formuler des problèmes d'optimisation avec ces équations pour extraire les meilleures valeurs des paramètres offrant une résilience et une durabilité optimales.

Cette métrique d'estimation de l'énergie donnerait une idée claire de la performance énergétique non seulement au niveau du nœud, mais aussi au niveau du réseau. Ainsi, elle permettrait de considérer la mise en œuvre des solutions gourmandes en énergie au niveau des nœuds finaux si celles-ci présentent de meilleurs résultats au niveau du réseau. D'autant plus que, dans les réseaux IoT, la communication est plus énergivore que le traitement.

IV. Travaux futurs

Dans cette section, nous présentons un aperçu des pistes que nous explorons dans le cadre de la *sécurité verte* dans l'IoT, une fois l'étape en cours achevée. Nous les avons organisées en deux sections comme suit:

A. Framework pour la sécurité verte dans l'IoT

La première piste à explorer est de fournir des lignes directrices et des spécifications claires sur la manière dont une solution de sécurité déployée dans un réseau IoT devrait être mise en œuvre et structurée afin d'atteindre à la fois un renforcement de la sécurité et la durabilité. Ainsi, nous étudions la possibilité de développer un framework qui couvre tous les aspects, en mettant davantage l'accent sur la partie technique en donnant des recommandations sur la manière de configurer certains algorithmes, quels mécanismes devraient être utilisés et quelles combinaisons fonctionnent ensemble. Grâce à ces directives, nous encourageons une culture de prise en compte de l'environnement lors de la conception de solutions pour les réseaux d'objets connectés. La stratégie que nous envisageons de suivre pour accomplir ce projet commence par une revue de la littérature et l'analyse des approches existantes, écologiques et sensibles à l'énergie, afin d'extraire les meilleures caractéristiques de chaque solution pour élaborer les lignes directrices. Bien que des lignes directrices existantes, telles que celles proposées par [38], abordent la sécurité et la confidentialité des données IoT au repos, elles ne prennent pas en compte l'aspect environnemental.

B. Solution de sécurité verte modulaire pour les réseaux IoT

En établissant des lignes directrices rigoureuses et une métrique d'estimation de la consommation énergétique, nous cherchons à proposer une solution de sécurité innovante pour les réseaux IoT qui optimise efficacement la consommation globale d'énergie d'un réseau et assure ainsi la durabilité et la pérennité en se focalisant sur les sujets de sécurité les plus émetteurs de GES identifiés par Wavestone [39]. Nous souhaitons adopter un mécanisme de niveau de sécurité adaptatif où nous priorisons la préservation de l'écosystème dans des environnements sûrs et sains ; à l'inverse, dans des environnements incertains et peu sécurisés, nous construisons des boucliers solides. Bien que les auteurs de [11] aient proposé une solution où le niveau de sécurité est ajusté en fonction du niveau de menace et de la sensibilité des données, en variant la longueur des clés de chiffrement et le niveau de confiance entre les nœuds, ils n'ont pas pris en compte ni la puissance de calcul des nœuds ni leur mobilité dans leur solution.

V. Conclusion

Le nombre de dispositifs IoT est en augmentation de jour en jour, ce qui a créé deux problèmes majeurs de consommation énergétique et de sécurité. Ces deux enjeux, de nature contradictoire, signifient que l'amélioration de la sécurité des appareils entraîne une hausse de la consommation d'électricité. Cela a conduit à l'émergence de la *sécurité verte*, qui consiste à prendre en considération la sécurité et l'environnement dès la conception des solutions informatiques. Dans cet article, nous avons présenté nos travaux en cours et travaux futurs visant à combler les lacunes en matière de *sécurité verte* dans l'IoT. Ceux-ci incluent un indicateur d'estimation de la consommation d'énergie, un framework pour soutenir le développement de solutions efficaces et vertes, et enfin, une solution modulaire verte. À travers ces initiatives, nous visons à apporter une contribution significative à l'avancement de ce domaine de recherche.

References

[1] Bharat S. Chaudhari and Marco Zennaro. "1 - Introduction to low-power wide-area networks". In: *LPWAN Technologies for IoT and M2M Applications*. Ed. by Bharat S. Chaudhari and Marco Zennaro. Academic Press, 2020, pp. 1–13. ISBN: 978-0-12-818880-4. DOI: https://doi.org/10.1016/B978-0-12-818880-4.00001-6.

[2] Shancang Li, Li Da Xu, and Shanshan Zhao. "The internet of things: a survey". en. In: *Information Systems Frontiers* 17.2 (Apr. 2015), pp. 243–259. ISSN: 1387-3326, 1572-9419. DOI: 10.1007/s10796-014-9492-7.

[3] *With the Internet of Things set to near 30 billion devices by 2025, tech giants are facing pressure to address the growing environmental impact their products pose*. URL: https://www.zerocarbonacademy.com/posts/with-the-internet-of-things-set-to-near-30-billion-devices-by-2025-tech-giants-are-facing-pressure-to-address-the-growing-environmental-impact-their-products-pose.

[4] Sana Benhamaid, Abdelmadjid Bouabdallah, and Hicham Lakhlef. "Recent advances in energy management for Green-IoT: An up-to-date and comprehensive survey". In: *Journal of Network and Computer Applications* 198 (2022). Publisher: Elsevier, p. 103257. DOI: https://doi.org/10.1016/j.jnca.2021.103257.

[5] Abbas Yazdinejad et al. "An energy-efficient SDN controller architecture for IoT networks with blockchain-based security". In: *IEEE Transactions on Services Computing* 13.4 (2020). Publisher: IEEE, pp. 625–638. DOI: 10.1109/TSC.2020.2966970.

[6] Daniyal Munir et al. "Duty Cycle Optimizing for WiFi-based IoT Networks with Energy Harvesting". en. In: *Proceedings of the 12th International Conference on Ubiquitous Information Management and Communication*. Langkawi Malaysia: ACM, Jan. 2018, pp. 1–6. ISBN: 978-1-4503-6385-3. DOI: 10.1145/3164541.3164571.

[7] Muhammad Rana, Quazi Mamun, and Rafiqul Islam. "Lightweight cryptography in IoT networks: A survey". In: *Future Generation Computer Systems* 129 (2022). Publisher: Elsevier, pp. 77–89. DOI: https://doi.org/10.1016/j.future.2021.11.011.

[8] Yan Naung Soe et al. "Towards a lightweight detection system for cyber attacks in the IoT environment using corresponding features". In: *Electronics* 9.1 (2020). Publisher: MDPI, p. 144. DOI: https://doi.org/10.3390/electronics9010144.

[9] Abbas Yazdinejad et al. "Energy efficient decentralized authentication in internet of underwater things using blockchain". In: *2019 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2019, pp. 1–6. DOI: 10.1109/GCWkshps45667.2019.9024475.

[10] Peixiong He, Yi Zhou, and Xiao Qin. "A Survey on Energy-Aware Security Mechanisms for the Internet of Things". In: *Future Internet* 16.4 (2024). Publisher: MDPI, p. 128. DOI: https://doi.org/10.3390/fi16040128.

[11] Malak Barari and Ramzi Saifan. "Energy–Aware security protocol for IoT devices". In: *Pervasive and Mobile Computing* (2023). Publisher: Elsevier, p. 101847. DOI: https://doi.org/10.1016/j.pmcj.2023.101847.

[12] Alessio Merlo, Mauro Migliardi, and Luca Caviglione. "A survey on energy-aware security mechanisms". In: *Pervasive and Mobile Computing* 24 (2015). Publisher: Elsevier, pp. 77–90. DOI: https://doi.org/10.1016/j.pmcj.2015.05.005.

[13] Omar Abdulkader et al. "A lightweight blockchain based cybersecurity for IoT environments". In: *2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*. IEEE, 2019, pp. 139–144. DOI: 10.1109/CSCloud/EdgeCom.2019.000-5.

[14] Luca Caviglione, Alessio Merlo, and Mauro Migliardi. "What is green security?" In: *2011 7th international conference on information assurance and security (IAS)*. IEEE, 2011, pp. 366–371. DOI: 10.1109/ISIAS.2011.6122781.

[15] N Premkumar and B Santhosh Kumar. "Lightweight Secure Authentication Scheme to thwart Unauthorized Edge Datacenters in Fog Computing". In: *Wireless Personal Communications* 139.1 (2024), pp. 167–181.

[16] Aulia Arif Wardana, Grzegorz Kołaczek, and Parman Sukarno. "Lightweight, trust-managing, and privacy-preserving collaborative intrusion detection for internet of things". In: *Applied Sciences* 14.10 (2024), p. 4109.

[17] Mohamed Ali Kandi et al. "A decentralized blockchain-based key management protocol for heterogeneous and dynamic IoT devices". In: *Computer communications* 191 (2022), pp. 11–25.

[18] Elahe Fazeldehkordi and Tor-Morten Grønli. "A Survey of Security Architectures for Edge Computing-Based IoT". In: *IoT* 3.3 (2022), pp. 332–365. ISSN: 2624-831X. DOI: 10.3390/iot3030019.

[19] *Etude ADEME – Arcep sur l'empreinte environnementale du numérique en 2020, 2030 et 2050*. URL: https://www.arcep.fr/la-regulation/grands-dossiers-thematiques-transverses/lempreinte-environnementale-du-numerique/etude-ademe-arcep-empreinte-environnemental-numerique-2020-2030-2050.html.

[20] Sarah A. Al-Qaseemi et al. "IoT architecture challenges and issues: Lack of standardization". In: *2016 Future technologies conference (FTC)*. IEEE, 2016, pp. 731–738. DOI: 10.1109/FTC.2016.7821686.

[21] San Murugesan. "Harnessing green IT: Principles and practices". In: *IT professional* 10.1 (2008). Publisher: IEEE, pp. 24–33. DOI: 10.1109/MITP.2008.10.

[22] Faisal Karim Shaikh, Sherali Zeadally, and Ernesto Exposito. "Enabling technologies for green internet of things". In: *IEEE Systems Journal* 11.2 (2015). Pub-

lisher: IEEE, pp. 983–994. DOI: 10.1109/JSYST.2015.2415194.

[23] Vikas Hassija et al. “A survey on IoT security: application areas, security threats, and solution architectures”. In: *IEEe Access* 7 (2019). Publisher: IEEE, pp. 82721–82743. DOI: 10.1109/ACCESS.2019.2924045.

[24] *Lightweight Cryptography Standardization Process: NIST Selects Ascon*. URL: https://csrc.nist.gov/News/2023/lightweight-cryptography-nist-selects-ascon.

[25] *Le numérique responsable*. URL: https://www.ecologie.gouv.fr/politiques-publiques/numerique-responsable.

[26] *Les actions de l’UE contre le changement climatique*. URL: https://www.europarl.europa.eu/topics/fr/article/20180703STO07129/les-actions-de-l-ue-contre-le-changement-climatique.

[27] Adel Noureddine, Romain Rouvoy, and Lionel Seinturier. “A review of energy measurement approaches”. en. In: *ACM SIGOPS Operating Systems Review* 47.3 (Nov. 2013), pp. 42–49. ISSN: 0163-5980. DOI: 10.1145/2553070.2553077. (Visited on 03/18/2025).

[28] Mathilde Jay et al. “An experimental comparison of software-based power meters: focus on CPU and GPU”. In: *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing (CCGrid)*. IEEE, 2023, pp. 106–118. DOI: 10.1109/CCGrid57682.2023.00020. (Visited on 03/18/2025).

[29] Kamar Kesrouani, Houssam Kanso, and Adel Noureddine. “A preliminary study of the energy impact of software in raspberry pi devices”. In: *2020 IEEE 29th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*. IEEE, 2020, pp. 231–234. DOI: 10.1109/WETICE49692.2020.00052. (Visited on 03/18/2025).

[30] Houssam Kanso, Adel Noureddine, and Ernesto Exposito. “Automated power modeling of computing devices: Implementation and use case for Raspberry Pis”. In: *Sustainable Computing: Informatics and Systems* 37 (2023). Publisher: Elsevier, p. 100837. DOI: https://doi.org/10.1016/j.suscom.2022.100837. (Visited on 03/18/2025).

[31] Malka Nisha Halgamuge et al. “An estimation of sensor energy consumption”. In: *Progress In Electromagnetics Research B* 12 (2009). Publisher: Electromagnetics Academy, pp. 259–295. DOI: 10.2528/PIERB08122303.

[32] Johan Pouwelse, Koen Langendoen, and Henk Sips. “Dynamic voltage scaling on a low-power microprocessor”. In: *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*. MobiCom ’01. Rome, Italy: Association for Computing Machinery, 2001, pp. 251–259. ISBN: 1581134223. DOI: 10.1145/381677.381701.

[33] Adel Noureddine, Romain Rouvoy, and Lionel Seinturier. “Monitoring energy hotspots in software: Energy profiling of software code”. en. In: *Automated Software Engineering* 22.3 (Sept. 2015), pp. 291–332. ISSN: 0928-8910, 1573-7535. DOI: 10.1007/s10515-014-0171-1. (Visited on 03/19/2025).

[34] Thomas Vogelsang. “Understanding the energy consumption of dynamic random access memories”. In: *2010 43rd Annual IEEE/ACM International Symposium on Microarchitecture*. IEEE, 2010, pp. 363–374. DOI: 10.1109/MICRO.2010.42. (Visited on 03/19/2025).

[35] D. A. Maevsky, E. J. Maevskaya, and E. D. Stetsuyk. “Evaluating the RAM Energy Consumption at the Stage of Software Development”. In: *Green IT Engineering: Concepts, Models, Complex Systems Architectures*. Ed. by Vyacheslav Kharchenko, Yuriy Kondratenko, and Janusz Kacprzyk. Vol. 74. Series Title: Studies in Systems, Decision and Control. Cham: Springer International Publishing, 2017, pp. 101–121. ISBN: 978-3-319-44161-0. DOI: 10.1007/978-3-319-44162-7_6. (Visited on 03/19/2025).

[36] *DRAM power calculator*. URL: https://www.micron.com/sales-support/design-tools/dram-power-calculator.

[37] Jaewon Ahn and Hong-Shik Park. “Measurement and modeling the power consumption of router interface”. In: *16th International Conference on Advanced Communication Technology*. 2014, pp. 860–863. DOI: 10.1109/ICACT.2014.6779082.

[38] Hezam Akram Abdulghani et al. “A study on security and privacy guidelines, countermeasures, threats: IoT data at rest perspective”. In: *Symmetry* 11.6 (2019). Publisher: MDPI, p. 774. DOI: https://doi.org/10.3390/sym11060774.

[39] *Sustainability: Cybersecurity has a role to play*. URL: https://www.wavestone.com/en/insight/cyber-sustainability-solutions.