Les systèmes de paiement mobile à l'ère de la Covid-19 : sécurité, vie privée et confiance numérique

Mobile payment systems in the Covid-19 era: security, privacy and digital trust

Schallum Pierre[1], Olson Italis[2]

[1] Institut intelligence et données (IID), Université Laval, schallum.pierre@iid.ulaval.ca
[2] LARIM, Polytechnique Montréal / ISTEAH, olson.italis@polymtl.ca

RÉSUMÉ. Les systèmes de paiement mobile se basent sur de nombreuses technologies. L'article s'appuie sur une solide revue de la littérature scientifique portant sur le développement récent des systèmes de paiement mobile. Il présente les principales implémentations et solutions existantes. Cependant, de nombreux problèmes restent encore ouverts dont la sécurité des données à caractère personnel qui soulève des questions éthiques en lien, entre autres, au respect de la vie privée. L'article montre comment, à l'ère de la Covid-19, l'éthique constitue un atout pour l'amélioration de la confiance numérique dans les systèmes de paiement mobile qui sont devenus des outils incontournables dans la vie des citoyens et citoyennes.

ABSTRACT. Mobile payment systems are based on many technologies. This paper builds on a fairly comprehensive review of the scientific literature, relative to the recent development of mobile payment systems. It presents the main current solutions and some implementations. However, many issues remain open, including the security of personal data, which raises ethical concerns related to privacy, among other concerns. The article shows how, in the Covid-19 era, ethics are an asset for improving digital trust in mobile payment systems that have become essential tools in the lives of citizens.

MOTS-CLÉS. Covid-19, système de paiement mobile, sécurité, éthique, confiance numérique, vie privée, Blockchain.
KEYWORDS. Covid-19, mobile payment system, security, ethic, digital trust, privacy, Blockchain.

Introduction

La pandémie de Covid-19 et le confinement qui s'en est suivi ont accéléré l'usage des technologies en ligne comme le paiement numérique sans contact [XIA 20]. Selon la Banque de France, au mois d'avril, prélèvements et virements totalisent 45% des paiements, en France, ce qui représente une augmentation de 12%, comparativement aux mois précédents [BES 20]. Durant ce contexte de pandémie, le marché de la cybersécurité comprenant le délit en ligne, les menaces en ligne et les violations de données, exploite à son avantage la vulnérabilité des individus et la crainte qui s'installent dans les villes [WAN 15]. Des stratégies inédites ont été utilisées en vue de dérober des fonds et de collecter des données privées [CEN 20]. Aux États-Unis, entre février et avril, les cyberattaques visant le secteur financier ont été multipliées par plus de 2 [JON 20]. Devant ce constat, les dépenses mondiales en matière de cybersécurité devront passer, selon Forbes, de 173 milliards de dollars en 2020 à 270 milliards de dollars en 2026 [COL 20].

Le présent article porte sur le problème de la sécurité des données à caractère personnel générées dans des environnements numériques, en mettant en lumière les enjeux éthiques liés aux technologies utilisées dans les systèmes de paiement mobile. Dans le contexte européen, la sécurité des données à caractère personnel considère non seulement l'aspect éthique mais aussi juridique en référence au règlement général sur la protection des données (RGPD) [EUR 18]. Dans le contexte spécifique de la France, elle est encadrée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) [ANS 20] et la Commission Nationale de l'Informatique et des Libertés (CNIL) [COM 20]. L'article propose une synthèse des connaissances sur les technologies adoptées dans les systèmes de paiement mobile. Tenant compte du rôle central de l'éthique, quelle technologie pourrait contribuer à

l'amélioration de la confiance numérique dans la sécurité des systèmes de paiement mobile à l'ère de la Covid-19 ?

L'article se divise en quatre sections qui répertorient les différentes approches technologiques rattachées au déploiement du paiement mobile et à leurs impacts sur la sécurité des données. Dans la première, six technologies des systèmes de paiement mobile sont abordées. Dans la deuxième, les problèmes de sécurité sont considérés sous l'angle des cyberattaques. Dans la troisième, les problèmes de la vie privée (privacité) sont décrits. Enfin, dans la quatrième, la blockchain est étudiée pour ce qui a trait à la protection de la vie privée.

1. Six technologies pour les systèmes de paiement mobile

Dans son livre *Mobile Payment*, Thomas Lerner [LER 13] décrit les principales technologies utilisées dans les systèmes de paiement mobile, lequel renvoie aux transactions faites via un appareil mobile [PAT 17]. Chacune des technologies abordées [LER 13] présente avantages et inconvénients [ITA 18].

1.1. *Le « Short Message Service » (SMS)*

Le « *Short Message Service* » (SMS) est un service de messagerie permettant d'employer jusqu'à 160 caractères. Il a été développé pour être utilisé dans le réseau « *Global System for Mobile Communications* » (GSM). Très simple à utiliser et connu à travers le monde, il est cependant coûteux et peut devenir facilement la cible de cyberattaques à cause de la mise en défaut des techniques de cryptographie.

1.2. *L' « Unstructured Supplementary Service Data » (USSD)*

L'« *Unstructured Supplementary Service Data* » (USSD) utilise généralement le « *Global System for Mobile Communication / Short Message Service* » (GSM/SMS) et sert d'interface pour les clients eux-mêmes et entre ceux-ci et les banques. Son avantage est qu'il est facile à utiliser et compatible avec tous les mobiles. L'inconvénient est que les données ne sont pas assez sécurisées. En effet, les systèmes utilisent en général un numéro d'identification personnel (NIP) pour authentifier l'utilisateur ou l'utilisatrice au niveau de l'application [DIG 20], mais comme dans le cas précédent, les procédures cryptographiques sont mises en défaut.

1.3. *Le « Bluetooth Low Energy » (BLE) ou « Bluetooth Smart »*

Le « *Bluetooth Low Energy* » (BLE) ou « *Bluetooth Smart* » utilise la transmission sans fil. Étant donné son faible besoin en énergie, il trouve une grande application dans le secteur du paiement de proximité, d'où ses limites également. Il a l'avantage de permettre des échanges sécurisés en respectant des recommandations de la *National Institute Standard and Technology* (NIST). Cet organisme a décrit les deux modes et des niveaux de sécurité pour un service entre deux appareils connectés via BLE [GUP 16] [PAD 17]:

- Pour le mode 1, le niveau 1 n'initie ni chiffrement ni authentification, le niveau 2 concerne seulement le chiffrement, mais pas l'authentification, le niveau 3 requiert l'authentification et le chiffrement et le niveau 4 exige l'utilisation de AES-CMAC des clés de la courbe elliptique de 250 bits de longueur.

- Pour le mode 2, la signature des données est considérée à deux niveaux selon que l'authentification n'est pas requise au niveau 1 ou au niveau 2 au début de l'établissement de la connexion.

Pour un service tel le paiement mobile, où la sécurité est nécessaire, NIST recommande le mode 1 et le niveau 4 ou les 2 appareils doivent s'authentifier et les échanges encryptés utilisant AES-CMAC avec p-256 ECC.

De plus, le BLE est compatible avec la plupart des smartphones (téléphones intelligents). Ce qui est un avantage puisqu'un système de paiement mobile avec BLE a donc une grande disponibilité.

1.4. *Le « Wireless Application Protocol » (WAP)*

Le « *Wireless Application Protocol* » (WAP) permet à un appareil mobile d'avoir accès à Internet. Grâce à l'intégration du « *Wireless Transport Layer Security* » (WTLS) chiffrant les échanges, la sécurité de la protection des données des utilisateurs ou utilisatrices et des modes d'authentification du serveur est très élevée. Le WAP est surtout recommandé pour le paiement en ligne. Cependant, son utilisation est encore limitée, même s'il suscite un grand intérêt. De plus, la technologie est dépassée et se révèle inappropriée pour livrer un choix conséquent de services aux terminaux actuels, ce que Samuel Pierre avait prévu de longue date [PIE 11].

1.5. *Le « Quick Response Code » (QRC)*

Le « *Quick Response Code* » (QRC) ou « *black and white matrix barcode* » est un code-barre à deux dimensions aussi appelé code 2D ou code matriciel. Il rend possible la lecture d'une donnée numérique, alphanumérique ou binaire avec un smartphone équipé d'une caméra. Le Secure QRC (SQRC) a été ajouté à l'ensemble afin de renforcer les mesures de chiffrement car il comporte de sérieux problèmes de sécurité, notamment, la redirection de l'utilisateur ou l'utilisatrice vers un site malveillant, lequel est un faux site capable de dérober des données financières [SHE 16]. Il est comparable au BLE en termes d'accessibilité, car disponible sur des téléphones de milieu de gamme.

1.6. *La « Near Field Communication » (NFC)*

La « *Near Field Communication* » (NFC) est utilisée pour le paiement sans contact. Cette technologie de communication radio utilise la fréquence 13.56 MHz dans la bande libre « *Industrial, Scientific and Medical* » (ISM). Elle rend possible l'échange de données et le paiement entre deux dispositifs se trouvant à une distance de 4 à 10 centimètres. Elle est utilisée selon deux configurations : l'une ou un « élément sécurisé » (SE pour « *Secure Element* ») est à l'intérieur du téléphone – notamment au sein d'une carte SIM – et l'autre ou le SE est intégré dans un serveur Cloud dit « *Host Card Emulation* » (HCE). Si le paiement sans contact est rapide et a connu un grand succès, deux inconvénients majeurs sont à considérer : la configuration HCE est vulnérable à une attaque par relais et avec l'élément sécurisé (SE) intégré, le fournisseur de services est très dépendant du fournisseur de matériel et le déploiement peut aussi être coûteux. Dans le cas de l'attaque par rejeu (« *replay attack* »), un ou une pirate peut capter, sur son passage, les données bancaires d'un utilisateur ou d'une utilisatrice et les envoyer à une autre personne qui pourra les utiliser pour procéder à des achats [CAS 15].

Les six technologies qui viennent d'être décrites sont utilisées dans plusieurs systèmes de paiement mobile qui sont présentés dans les sections « sécurité » et « protection de la vie privée ». Un résumé des avantages et limitations respectifs de chacune de ces technologies est donné dans le tableau 1.

Technologies	Avantages	Inconvénients
SMS	▪ Grande accessibilité : disponible sur les réseaux GSM et avec des téléphones bas de gamme.	▪ Service peut être coûteux ; ▪ Failles de sécurité évidentes.
USSD	▪ Disponible sur les réseaux GSM et avec des téléphones bas de gamme;	▪ Failles de sécurité : mise en défaut des propriétés cryptographiques,

	▪ Aucun coût associé à ce service pour un opérateur de téléphonie mobile.	mot de passe de faible entropie (4 ou 6 digits);
BLE	▪ Niveau de sécurité adéquat pour le paiement mobile; ▪ Accessibilité moyenne : disponible sur des téléphones de milieu de gamme; ▪ Facilité pour le déploiement du service.	▪ Paiement de proximité seulement : une autre technologie de communication est nécessaire pour interconnecter des nœuds distants.
WAP	▪ Technologie permettant à des mobiles (n'ayant pas la capacité adéquate) de se connecter à l'Internet; ▪ Utilisation de propriétés cryptographiques.	▪ Technologie dépassée par l'offre actuelle de services : les mobiles se connectent à l'Internet sans avoir besoin d'une autre couche.
QRC	▪ Accessibilité moyenne comme pour le BLE ; ▪ Facilité de déploiement comparable à l'effort fourni pour déployer un système avec BLE.	▪ Paiement de proximité seulement : d'autres technologies de communication nécessaires pour interconnecter les nœuds distants; ▪ Redirection vers des sites malveillants, une menace pour de tels systèmes.
NFC	▪ Architecture avec SE intégré très sécurisé ; ▪ Grande facilité d'utilisation : paiement sans contact.	▪ Déploiement coûteux du service : fournisseur de service de paiement très dépendant du fournisseur de l'élément sécurisé intégré, base de la robustesse en sécurité du système ; ▪ Architecture HCE, système vulnérable aux attaques par relais.

Tableau 1. *Des technologies dans le paiement mobile : avantages et inconvénients*

Les différents problèmes de sécurité ramènent l'éthique au centre des systèmes de paiement mobile. Ils concernent les cyberattaques, l'attaque dite de « l'Homme Du Milieu » (HDM) et l'attaque par relais. Ils sont exposés dans la section « sécurité ».

2. Sécurité

La sécurité de la technologie de tout système de paiement mobile – paiement mobile à un point de vente, paiement mobile en tant que point de vente, plateforme de paiement mobile, système de paiement mobile indépendant et facturation directe par l'opérateur – est essentielle. En effet, les données des utilisateurs et utilisatrices sont au centre de l'économie numérique. Aussi font-elles l'objet de cyberattaques.

2.1 *Cyberattaques et HDM*

Les systèmes de paiement mobile sont exposés à différents types de menaces et de cyberattaques. Parmi celles-ci, il y a le programme malveillant ou maliciel et le domaine malveillant.

2.1.1. *Programme et domaine malveillants*

La menace la plus importante, sur le plan de la sécurité, est le programme malveillant. Les activités qui le génèrent sur un mobile sont le plus souvent l'enregistrement d'appels, les messages instantanés, la localisation via le « *Global Positioning System* » (GPS) et le transfert des journaux d'appels. Il faudra mettre au point une méthode efficace de détection de programme malveillant dédiée à la téléphonie mobile. Les méthodes de détection de programme malveillant, rattachées à l'analyse statique, à l'analyse dynamique et au cadre juridique pour l'environnement mobile, ne sont actuellement pas efficaces pour les appareils mobiles [WAN 16]. En plus des programmes ou logiciels malveillants, sont apparus, durant la covid-19, des domaines malveillants ou faux-sites. Vers la fin du mois de mars 2020, Palo Alto Networks a identifié 40 261 domaines malveillants à risques élevés et 2 022 nouveaux domaines enregistrés malveillants utilisant des mots clés comme "covid-19", "covid19", "coronavirus" et "corona-virus" [INT 20]. Selon Europol, les malfaiteurs en ligne exploitent l'anxiété croissante, la forte demande en équipements de protection et produits pharmaceutiques, la diminution de la mobilité et l'augmentation du télétravail pour mener des campagnes de communications non sollicitées (spams) et obtenir des informations sensibles (numéros de carte bancaire, identifiant) sur des organisations (hôpitaux et organismes internationaux en santé) et des individus [EUR 20]. Des mesures de prévention comme la protection de son identité s'imposent pour mettre à l'abri ses données personnelles des menaces de détournement de sites [GOU 17]. Les données des utilisateurs et utilisatrices peuvent être piratées par l'attaque de l'Homme Du Milieu (HDM) que facilitent les protocoles « *Secure Sockets Layer/ Transport Layer Security* » (SSL/TLS).

2.1.2. *Protocoles SSL/TLS et HDM*

Même s'il empêche les pirates d'accéder aux données sensibles en transit grâce à l'algorithme de chiffrement [DIG 20], le protocole SSL (dont une version plus sécurisée est TLS) sur lequel s'appuient beaucoup d'appareils mobiles pour leur sécurité peut avoir des vulnérabilités potentiellement exploitables. C'est le cas de la vulnérabilité Heartbleed Bug qui se trouve dans la bibliothèque cryptographique OpenSSL. Elle peut être exploitée par des agents utilisateurs malveillants pour subtiliser des informations appartenant au propriétaire ou à la propriétaire du mobile. Le protocole SSL (ou TLS pour la nouvelle version) est également vulnérable à une attaque de l'Homme Du Milieu (HDM). L'HDM désigne toute attaque réalisée dans l'objectif d'accéder aux échanges entre deux interlocuteurs ou interlocutrices sur Internet [TOR 18]. L'attaque peut être à l'origine de transactions frauduleuses menant à des détournements d'argent. Afin d'augmenter la confiance numérique des utilisateurs et utilisatrices, il est crucial de mettre en place un système de sécurité de la protection des données sur le backend grâce au certificat valide du serveur. Il faudra élaborer un système de sécurité efficace qui mettra automatiquement fin à toute transaction dont le certificat est invalide [WAN 16].

2.2. *Paiement sans contact et limites (NFC : SE et HCE)*

Une autre technologie est le paiement sans contact, lequel a été récemment déployé, à très grande échelle, dans beaucoup d'institutions bancaires et des commerces de détail, en dépit de quelques limites [QYR 19]. À l'ère de la Covid-19, pour des raisons sanitaires, les échanges de monnaie tendent à être supplantés par le paiement sans contact [BLA 20]. NFC est la technologie permettant ce paiement sans contact.

L'article « Fraud on host card emulation architecture: Is it possible to fraud a payment transaction realized by a mobile phone using an "Host Card Emulation" system of security ? » [PAS 16] traite de deux grandes architectures qui sécurisent ce type de paiement : l'élément sécurisé (SE) qui est intégré dans le mobile et la technologie « *Host Card Emulation* » (HCE) qui est une architecture non intégrée

au mobile mais connectée via un réseau. Le SE se trouve seulement dans la carte « *Subscriber Identity Module* » (SIM). Cela signifie que le système d'exploitation du mobile n'a aucun accès aux données de transaction. C'est là son point fort. Cependant, le SE, étant rattaché à un opérateur mobile, se pose le problème de l'interopérabilité. La technologie HCE facilite le paiement via la technologie NFC qu'on retrouve sur « plus de deux smartphones sur trois » [THA 15]. Proposée par les opérateurs du secteur de la monnaie électronique, la HCE vise à résoudre le problème de l'interopérabilité du SE. Elle procède à la désynchronisation du SE et rend possible le stockage des données bancaires sur l'infonuagique/Cloud Computing [OFF 15]. Elle utilise la tokenisation ou le remplacement des données bancaires par un jeton (élément qui représente les données sensibles seulement à l'intérieur du système). Le but est d'empêcher toute forme de réutilisation de données sensibles. Cependant, deux types de cyberattaques ont été signalés. Premièrement l'attaque des données téléphoniques et secondement l'attaque entre le processeur d'application et le contrôleur NFC sur le téléphone portable [PAS 16]. Avant de choisir les SE et HCE, il faudra résoudre ces deux importants problèmes de sécurité.

2.2.1. *Attaque des données téléphoniques*

Avec le serveur HCE, les données sensibles remontent au système d'exploitation du mobile. Dans le but d'éviter qu'un autre mobile prenne le contrôle du mobile auquel est lié le serveur HCE via un programme malveillant, une reconnaissance du téléphone est effectuée par l'adresse IP et l'adresse MAC. L'adresse IP (pour Internet Protocol) est une chaine de caractères qui identifie de manière unique une entité connectée à internet. Cette chaine a une longueur qui dépend de la version de protocole, IPv4 (version 4) ou IPv6 (version 6); l'adresse « *Media Access Control* » (MAC) ou adresse physique est une chaine de caractères qui identifie une interface réseau, elle est l'adresse d'un sous-réseau dans un réseau plus large [PAE 20]. Lorsque ces adresses correspondent à celles connues du serveur HCE, ce dernier procède à l'envoi des données. Trois éléments peuvent être à l'origine de l'attaque d'un mobile utilisant la technologie HCE : la clé symétrique, l'adresse Mac et l'adresse IP. Un renforcement de ces trois éléments est indispensable pour améliorer la sécurité du serveur HCE [PAS 16]. L'attaque entre le processeur d'application et le contrôleur NFC constitue une autre vulnérabilité du paiement sans contact.

2.2.2. *Attaque entre le processeur d'application et le contrôleur NFC sur MOBILE*

Ce genre d'attaque survient en mode déconnecté, un mode qui autorise l'utilisation permanente du paiement via HCE. L'autorisation est possible parce que le téléchargement des numéros de carte a été effectué en amont sur le réseau. Même si le mobile est déconnecté du réseau, le paiement peut être autorisé. Si un programme malveillant arrive à transférer les données importantes vers un autre téléphone, la transaction pourra être complétée sans que le titulaire authentique ou le serveur HCE en ait été mis au courant. La technologie HCE gagnera à être plus robuste, afin d'éviter des attaques de programmes malveillants [PAS 16] [CAS 15]. Le paiement sans contact est confronté à d'autres contraintes techniques et fonctionnelles d'envergure.

2.3. *NFC et limite de l'exigence de la carte préenregistrée*

Dans « A prototype-based case study of secure mobile payments » [TIL 15], Till Halbach explore les relations entre les interactions des utilisateurs ou utilisatrices, la sécurité et le mécanisme de confidentialité pour un cas de paiement mobile basé sur la technologie NFC. Les connaissances qui en découlent peuvent servir à élaborer des solutions de paiement pour les systèmes d'Apple et de Google, par exemple. Une application Android a été développée comme preuve de concept. Cependant, il y a beaucoup de contraintes techniques et fonctionnelles pour effectuer un paiement, car une carte physique doit être préalablement enregistrée avant l'utilisation de l'application. Il faut tenir compte des exigences de la banque. L'utilisateur ou l'utilisatrice ne peut pas choisir de carte particulière durant sa transaction [TIL 15]. Des solutions doivent être apportées pour éviter les limitations du paiement sans contact qui est, par ailleurs, vulnérable aux attaques par relais.

2.4. *Attaque par relais*

L'infrastructure de la plateforme de paiement mobile ouverte « SIMulations des Mobilités » ou MobiSIM – modélisation de simulations quotidienne et résidentielle pour une planification durable des villes françaises et européennes [ANT 10] – est basée sur la technologie HCE [URI 14]. Elle utilise des SE cartes « *Europay Mastercard Visa* » (EMV) hébergés dans l'infonuagique/Cloud Computing [OFF 15] et accessibles à distance via le protocole « *Remote APDU Call Secure* » (RACS). Il est décrit par un projet Internet Engineering Task Force (IETF) dont la sécurité repose sur le protocole Transport Layer Security (TLS) qui applique une authentification mutuelle forte et s'exécute dans le module SIM. Les transactions s'effectuent en moins d'une seconde. Cependant, MobiSIM est confronté à des attaques par relais. En plus de ce problème d'attaque par relais, il faudra résoudre le problème de la limitation de l'utilisation des cartes bancaires sans contact via le réseau. En effet, ces cartes périphériques ne peuvent effectuer qu'un nombre limité de transactions sans contact. Il exige d'entrer un numéro d'identification personnel après quelques dizaines de paiements [URI 14]. Le mobile étant aujourd'hui un outil au travers duquel les utilisateurs et utilisatrices enregistrent plusieurs catégories de données, il importe de faire usage d'une sécurité de communication solide comme le permettent les primitives cryptographiques.

2.5. *Primitives cryptographiques*

L'article « A Secure Transaction Scheme With Certificateless Cryptographic Primitives for IoT-Based Mobile Payments » [YEH 17] introduit pour les paiements mobiles, un schéma de transaction sécurisé avec des « primitives cryptographiques ». Ces dernières sont des modules fournissant des fonctions de hachage cryptographique et de chiffrement permettant de garantir la sécurité de systèmes informatiques. Le schéma proposé profite des mérites d'Android Pay et d'un crypto-système de signature certifié pour assurer simultanément la sécurité des transactions et atteindre l'efficacité du paiement en pratique. Il se révèle à la fois précis et sécurisé via un modèle oracle aléatoire. Il offre une robustesse et une sécurité de communication solides pour les utilisateurs ou utilisatrices mobiles lors des transactions de paiement en ligne. D'autre part, l'évaluation de la performance montre la praticabilité du schéma de transaction proposé car le coût de calcul total est acceptable pour un test basé sur « des objets connectés » (« *Internet of Things* » ou IOT). En raison de l'adoption de la crypto-opération d'appariement bilinéaire, les performances de calcul et l'évolutivité du système sont donc limités. Il faudra améliorer les composants de sécurité adoptés dans le schéma proposé [YEH 17], avant le choix de cette technologie. Parallèlement à la sécurité, il y a la gestion des données dans l'infonuagique/Cloud Computing se rapportant à tout accès à un service informatique via Internet [OFF 15]. Le modèle du cloudlet [WU 15] propose un cadre d'échange de ressources multilatéral à envisager.

2.6. *Infonuagique/Cloud Computing : cloudlet pour l'échange de ressources entre les utilisateurs ou utilisatrices sans le Wi-Fi et limites*

Wu et Ying [WU 15] s'inspirent de la monnaie numérique en pair-à-pair Bitcoin [BIT 20] pour proposer un cadre d'échange de ressources multilatéral basé sur le cloudlet pour les utilisateurs ou utilisatrices mobiles. Il s'agit d'un système de petits centres de données qui permet des transactions sans faille entre les utilisateurs et utilisatrices sur la bande passante Internet en tant que preuve de concept. Le cloudlet est un paradigme de déploiement de cloud plus évolutif et peu coûteux visant l'utilisation de ressources de calcul et de stockage de proximité. Il permet d'exploiter les ressources de serveurs personnels inactifs des utilisateurs individuels ou utilisatrices individuelles, accessibles par Wi-Fi. L'accès aux ressources exige l'authentification 802.1x, à partir d'un serveur et d'un routeur sans fil via Radius. Le 802.1X est un protocole d'authentification permettant de sécuriser l'accès d'un ordinateur à un réseau qui peut être soit cablé (réseau interne câblé ou LAN), soit sans fil (réseau interne sans fil ou WLAN) [GON 13].

Wu et Ying présentent un système d'échange de ressources sur le marché pour les utilisateurs ou utilisatrices mobiles qui tient lieu de système monétaire virtuel. Il est adapté à d'autres systèmes

distribués. Cependant, le service de stockage est inaccessible sans bande passante. Or, selon la cartographie établie par le « *Global Connectivity Index* » (GCI) [GCI 17], l'écart ne cesse de se creuser entre les pays au regard de la connectivité. Cette fracture numérique est aussi visible même au sein des pays dits connectés étant donné que l'accès à l'Internet n'est pas le même selon que l'utilisateur ou l'utilisatrice se trouve en milieu rural ou urbain. Il faudra trouver une solution, dans le cadre du cloudlet, pour l'échange de ressources entre les utilisateurs ou utilisatrices sans le Wi-Fi [WU 15]. Le paiement mobile exige des spécificités en lien à la protection de la vie privée.

Types de système de paiement mobile	Mesures de sécurité à prendre
Système de paiement utilisant NFC avec SE intégré dans le mobile.	• Eviter les limitations liées à la carte pré-enregistrée.
Système de paiement utilisant NFC avec l'architecture HCE.	• Renforcer la clé symétrique pour encrypter les échanges et les adresses IP et MAC du mobile de l'utilisateur. • Protéger l'application mobile contre les attaques de programmes malveillants qui pourraient accéder à des données confidentielles préchargées. • Sécuriser la communication entre le serveur HCE et le mobile utilisateur pour éviter une attaque par relais.
Systèmes utilisant des primitives cryptographiques.	• Adopter des opérations cryptographiques garantissant une bonne performance et l'évolutivité.
Système base sur des plateformes distribuées, particulièrement avec les cloudlet.	• Sécuriser les liens, le risque étant devenu plus grand en environnement distribué, puisque certains nœuds peuvent avoir des brèches. • Surmonter le manque de connectivité dans certaines régions.

Tableau 2. *Des améliorations nécessaires pour la sécurité dans le paiement mobile*

3. Le problème du respect de la vie privée

Le problème du respect de la vie privée devient de plus en plus important quand on considère le grand nombre de participants et participantes dans un système de paiement mobile tel qu'exposé par Wang et al. à la figure 1 [WAN 16]. Les données sont souvent accessibles à des opérateurs de téléphonie mobile, des fournisseurs de matériels, des fournisseurs de services de paiement, des banques, des réseaux de cartes et des personnels marchands. Certains systèmes n'ont pas de mécanisme fiable de protection de ces données en transit ou stockées ; d'autres assurent partiellement cette protection. Nous allons dans cette section décrire brièvement les différentes classes de solutions.

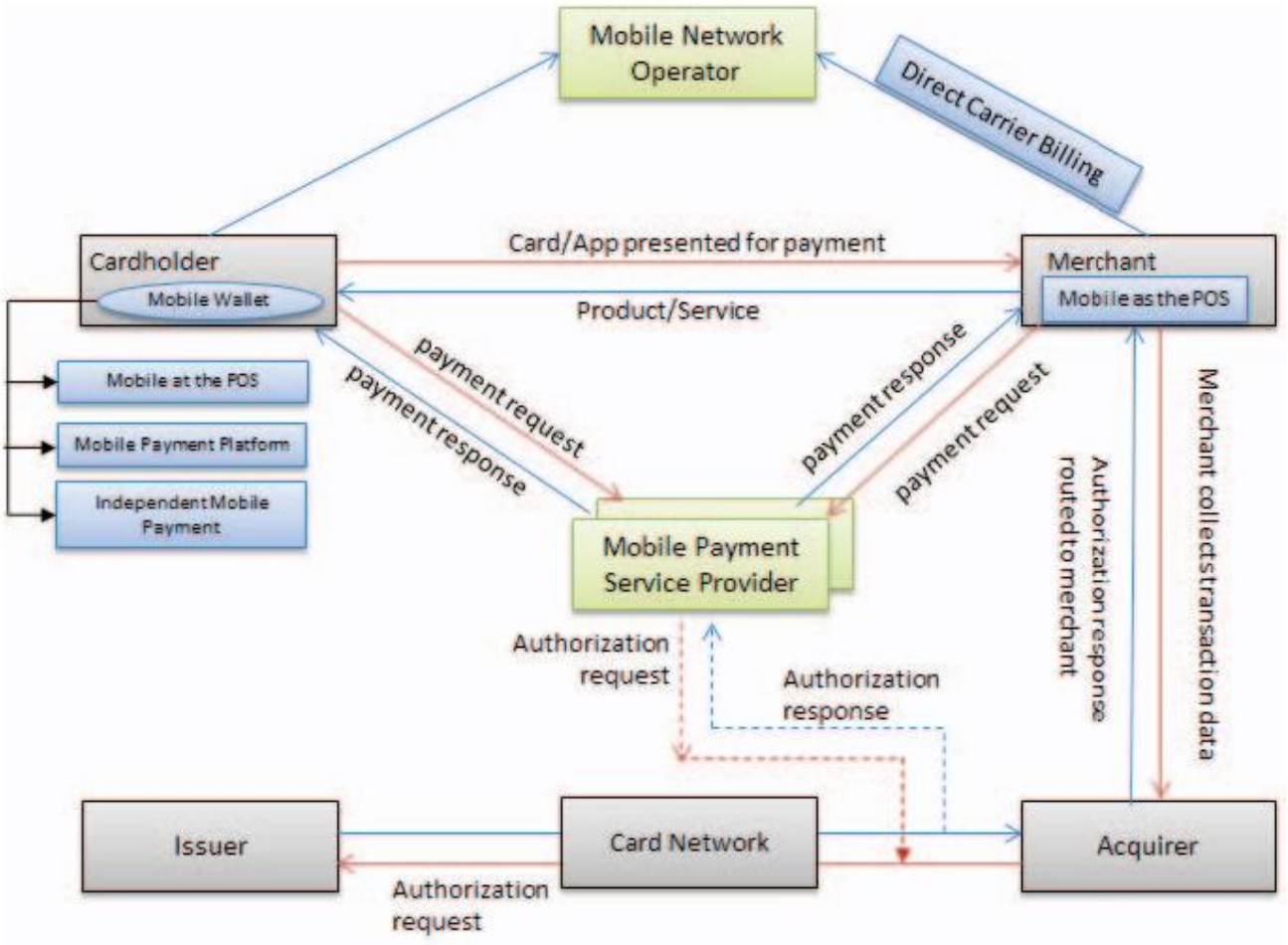

Figure 1. *Le processus de paiement dans un système de paiement mobile [WAN 16]*

3.1. *Le respect de la vie privée avec les technologies considérées*

Dans l'article, "USSD—Architecture analysis, security threats, issues and enhancements" est exprimée une menace d'exposition des données confidentielles de l'utilisateur [LAK 17] : elles sont affichées telles durant la transaction. De plus, pour certains systèmes de paiement mobiles basés sur SMS et USSD, les données sont chiffrées avec des algorithmes ayant déjà subi le processus de rétro-ingénierie [NYA 13] avec risque de clonage de la SIM qui héberge la clé de chiffrement. Enfin, il faut mentionner que le chiffrement de bout-en-bout n'est pas garantie et que l'opérateur de téléphonie mobile aura accès aux données avant d'atteindre le fournisseur de service quand les deux entités sont différentes.

Pour BLE et SQRC, la cryptographie est utilisée pour protéger les échanges [SHE 16]. Ce qui empêche à un grand nombre d'intermédiaires d'avoir accès aux données sensibles, mais dans ce cas, les marchands accèdent toujours à des numéros de cartes de paiement. Certains systèmes avec NFC sont plus efficaces en utilisant la tokenisation. Ainsi, le marchand ou la marchande a droit à un jeton. Toutefois, dans tous les cas, le fournisseur de services ou la banque a accès à un ensemble d'informations faisant partie de l'identité numérique du client ou de la cliente.

3.2. *Le respect de la vie privée avec l'authentification biométrique*

Certains systèmes, dont Apple Pay, utilisent l'authentification biométrique [MAR 16]. En effet, des caractéristiques biologiques de l'utilisateur ou de l'utilisatrice sont enregistrées avec d'autres informations personnelles pour constituer son identifiant. Ainsi, il ou elle peut utiliser ses caractéristiques biométriques pour s'authentifier au moment d'accéder au service. Le fournisseur de service a de son côté accès aux données biométriques du client ou de la cliente. Il est vrai que dans le cas d'Apple Pay, ces informations sont dans une enclave, mais il n'en est pas ainsi de tous les systèmes

où ces données peuvent être moins sécurisées. Pour avoir des systèmes d'authentification biométriques plus robustes (notamment avec des méthodes d'apprentissage machine profond), davantage de caractéristiques biométriques nécessitent d'être stockées [OSA 19]. Ce qui augmente clairement le risque d'exposer des données privées.

4. Protection de la vie privée et amélioration de la confiance numérique

Les systèmes informatiques qui se rapportent à la vie privée doivent être fiables pour éviter des brèches de sécurité, une des sources de méfiance envers la technologie. Cette section décrit quatre prototypes de systèmes de paiement mobile très sécurisés qui sont capables d'améliorer la confiance numérique des utilisateurs et utilisatrices dans les systèmes de paiement mobile. Le premier prototype est associé à TrustZone [ZEN 16].

4.1. *Système informatique sécurisé et TrustZone*

Les auteurs Zheng, Yang, Shi et Meng [ZEN 16] proposent un cadre de plateforme utilisant un système informatique sécurisé pour la protection de la vie privée en matière de paiement grâce aux plateformes activées sur TrustZone. La technologie TrustZone garantit la confidentialité des données sensibles face aux logiciels malveillants. Les auteurs Zheng, Yang, Shi et Meng utilisent une plateforme de paiement mobile qui est un prototype de système sur un environnement de simulation. Ils se basent sur les architectures ARM et la virtualisation et développent un système avec les FastModels qui sont des modèles précis et flexibles d'ARM IP [ARM 20]. Une implémentation est présentée sur un plan de développement réel utilisant ARM CoreTile Express A9x4. La plateforme peut assurer la sécurité des transactions de paiement, réaliser un paiement bienveillant concernant la protection de la vie privée et fournir des services informatiques fiables. Elle peut aussi empêcher les attaques des « *Robot Operating System* » (ROS) malveillants et peut sécuriser l'affichage et l'entrée pour empêcher la lecture de données sensibles du périphérique d'affichage et des périphériques d'entrée par des agents hostiles.

Afin d'améliorer la praticabilité du paiement mobile, il faudra créer un écran tactile, une reconnaissance d'empreintes digitales sûres. En outre, il faudra améliorer la sécurité des mécanismes de paiement dans un environnement réel [ZEN 16]. Tout système de paiement mobile a besoin, pour être solide, de sécuriser les données générées par les transactions. C'est ce que propose le deuxième prototype développé par Kang et Nyang [KAN 17].

4.2. *Système de paiement en transit et protection de la vie privée*

Kang et Nyang [KAN 17] proposent un prototype de paiement en transit de protection de la vie privée. La protection est basée sur des signatures traçables, sur l'identité et sur des signatures anonymes. En plus de la confidentialité, le système facilite le blocage proactif des passagers ou passagères qui se conduisent mal. Il prend en charge les services de transfert gratuit avec des programmes post-payés permettant des paiements mobiles à l'aide de smartphone.

Dans le système proposé, les organismes de transport en commun ne peuvent pas obtenir l'identité des passagers ou passagères et les demandeurs ou demandeuses de paiement ne peuvent pas obtenir des itinéraires de passagers ou passagères. Les passagers ou passagères peuvent terminer leurs procédures d'entrée et de sortie dans environ 0,3-0,4 secondes, y compris la vérification de la révocation, qui prend approximativement 0,1 seconde. Bien que le système proposé soit conçu pour les services de transport en commun tels que les systèmes de métro, il peut être appliqué aux systèmes de paiement mobile hors ligne [KAN 17]. Le système de paiement en transit devra être testé dans différents environnements réels pour s'assurer de son efficacité. Un troisième prototype de système de paiement mobile particulièrement bien sécurisé est présenté dans les lignes qui suivent. Il utilise le cryptage asymétrique.

4.3. *Cryptage asymétrique et code QR chiffré*

Purnomo, Gondokaryono et Kim [PUR 16] proposent une technique d'authentification mutuelle entre le client ou la cliente et le commerçant ou la commerçante utilisant le code « *Quick Response* » (QR) chiffré. Le code QR chiffré permet de partager rapidement des données, de manière sécurisée [AHA 19]. La transmission sécurisée de la transaction de données peut s'effectuer par l'utilisation d'un code QR chiffré. L'application de paiement mobile nécessite un système sécurisé pour gagner la confiance numérique du client ou de la cliente. La sécurité dans le système de paiement est fondamentale car elle concerne les données de compte bancaire personnel. Pour protéger l'acheteur ou l'acheteuse et le vendeur ou la vendeuse, il faut un niveau de sécurité plus élevé utilisant l'authentification mutuelle pour assurer la sécurité de la transaction. L'authentification mutuelle passe par un « système d'infrastructure à clé publique » (« *Public Key Infrastructure* » ou PKI). L'utilisation de cette infrastructure à clé publique assurera la sécurité de la distribution des clés. Ce système de cryptage utilise l'algorithme RSA (en référence aux initiales de ses trois inventeurs Ron Rivest, Adi Shamir et Leonard Adleman) qui est considéré comme le système de protection de messages le plus puissant [ASA 15]. Ce système de sécurité est également renforcé avec l'ajout du code QR chiffré comme support de paiement. L'utilisation du code QR chiffré assurera l'intégrité, la lisibilité et la confidentialité de l'information. Il constitue également une base importante pour la sécurité du système. Cependant, si un intrus parvient à dérober la clé secrète ou privée, il sera en mesure d'avoir accès à l'information [PUR 16].

Le cryptage asymétrique pourra servir de modèle pour une application dans l'environnement de la Blockchain qui est une technologie sécurisée et décentralisée de stockage et de partage de données. Il est actuellement au cœur de l'économie des services électroniques de l'Estonie. Il contribue à y sécuriser l'identité numérique, laquelle est fondée sur la technologie mobile ou l'utilisation des smartphones pour l'authentification et la signature électronique. Quatre principes [MUR 13] définissent cette identité numérique ou mobile et peuvent être utilisés par des organismes publics ou privés en vue d'une gestion éthique des données :

- la décentralisation, à la place d'une base de données centralisée, chaque membre d'un réseau peut créer sa propre base de données;

- l'interconnexion, une harmonisation concernant l'ensemble des membres est réalisée grâce à une couche de liaison de données libre et open source qu'est X-Road (https://x-road.global/);

- l'ouverture de la plateforme, le système d'infrastructure à clé publique est utilisé, et;

- l'ouverture des processus, le projet est développé et amélioré de façon continue.

Ces quatre principes peuvent être considérés comme le fondement de la gestion de l'éthique des données massives. Ils se réfèrent à la collaboration d'une communauté inclusive (de membres, par exemple), l'ouverture du code source et la transparence de l'historique (et non du contenu) des échanges. En ce sens, il faut souligner, à l'échelle mondiale, les projets de la fondation Linux [LIN 2020] et du « *World Wide Web Consortium* » (W3C) [W3C 20] qui soutiennent les systèmes d'open source et le développement de la standardisation ouverte. À l'échelle nationale, les pays peuvent aussi promouvoir ces principes éthiques, à l'instar de l'Estonie, en particulier et de l'Europe, en général, via son RGPD. Considérant le cas de Bitcoin – qui est une monnaie numérique en pair-à-pair, libre et ouverte, sans autorité centrale [BIT 20]–, la blockchain semble être la technologie qui met en oeuvre ces spécifications éthiques. Il reste certes des questions de recherches à approfondir pour Bitcoin mais ce dernier offre une solution de transparence sans contrevenir à la sécurité des données générées par les utilisateurs et utilisatrices [KHA 19].

Si l'utilisation de la blockchain exige, le plus souvent, une connexion à Internet, le « Paiement sans contact » (NFC) peut s'effectuer hors ligne, tout en étant sécurisé. C'est ce que propose le quatrième prototype développé par A. M. San et C. Sathitwiriyawong [SAN 16].

4.4. *Paiement sans contact et confidentialité*

L'article « Privacy-Preserving Offline Mobile Payment Protocol based on NFC » [SAN 16] considère un nouveau protocole de paiement mobile hors ligne basé sur la technologie NFC. Dans le système, une signature de groupe est utilisée pour assurer la non-capacité des transactions. Étant donné qu'il y a moins de calculs à la phase de paiement, l'efficacité de la signature du groupe se trouve améliorée. Le système est pertinemment conçu pour répondre à toutes les exigences en matière de sécurité et de confidentialité, notamment l'anonymat, la non-mobilité, l'aléas et la prévention des attaques à répétition. Il se concentre sur la protection de la vie privée des clients ou clientes pour le paiement mobile. Tout d'abord, le client ou la cliente demande un identifiant anonyme à sa banque. Ensuite, le client ou la cliente utilise cet identifiant pour s'inscrire au Trusted Service Manager (TSM). Le TSM sait seulement que le client ou la cliente est autorisé(e) par la banque, mais ne connaît pas l'identité réelle du client ou de la cliente. Lorsque le client ou la cliente génère une signature de groupe pour le message de transaction, seul le TSM connaît l'identité anonyme du client ou de la cliente. Par conséquent, le système protège la confidentialité du client ou de la cliente. Le protocole de paiement mobile hors ligne, basé sur la NFC de San et Sathitwiriyawong [SAN 16] pourra être implémenté là où le problème de la fracture numérique se pose encore.

Les différents cas qui ont été présentés précédemment démontrent clairement que la sécurité reste un enjeu majeur du paiement mobile. Lorsque la vulnérabilité d'un système déjà implémenté est connue, la réputation de l'entreprise qui utilise la technologie en pâtit. La sécurité est un élément essentiel dans la valorisation de la confiance numérique numérique. Elle peut être renforcée tant par l'utilisation du cryptage asymétrique, avec une connexion Internet, que par le paiement sans contact, dans le cas du paiement mobile hors ligne. Différentes propositions de résolution de problème de sécurité proposées sont reportées dans le tableau 3.

Types de système et références	Mécanismes et modèles pour la protection de la vie privée et l'amélioration de la confiance numérique
Paiement mobile sécurisé avec des plateformes tierces [ZEN 16].	Un environnement dit de confiance numérique (TrustZone) est dédié au système à sécuriser, le séparant de l'environnement extérieur où sont présentes l'ensemble des applications.
Système de paiement dans le transport en commun avec protection de la vie privée [KAN 17].	L'identité du client ou de la cliente est conservée par le système. Toutefois, un participant (institution financière et compagnie de transport) a accès seulement aux informations qu'il a lui-même fourni. Pour y parvenir, les signatures traçables et anonymes sont utilisées.
Système de paiement utilisant QRC avec chiffrement des échanges [PUR 16].	Le système proposé dans la référence utilise le QRC pour la communication entre le système du vendeur ou de la vendeuse et celui de l'acheteur ou l'acheteuse. Il se base sur la cryptographie à clé publique avec une authentification mutuelle des interlocuteurs.
Paiement sans contact garantissant la confidentialité [SAN 16].	Le système utilise la signature de groupe : l'autorisation pour un client ou cliente vient de son institution et est transmise à un ou une gestionnaire de service de confiance numérique.

Tableau 3. *Des mécanismes de sécurité dans le paiement mobile*

5. Conclusion

Cette revue de la littérature présente quelques caractéristiques des technologies et des systèmes du paiement mobile. L'USSD, le BLE, le SMS, le WAP, le QRC et la NFC/RFID sont les modèles décrits dans l'article. La plupart des systèmes de paiement mobile implémentés à travers le monde utilisent

une ou plusieurs de ces technologies. Beaucoup d'entre elles soulèvent des problèmes éthiques qui concernent le respect des données personnelles. Le mobile, s'étant établi en outil accessible, il devient plus facile d'accéder aux données de la vie privée et de suivre l'activité en ligne des utilisateurs et utilisatrices. Voilà pourquoi la sécurité s'impose comme une priorité majeure dans le domaine du paiement mobile. En ce sens, le cryptage asymétrique constitue un excellent vecteur. Il répond à un besoin de sécurité des données, en particulier en cette période de pandémie où l'usage du paiement mobile connaît une forte croissance. Devant l'ampleur des problèmes qui ont été décrits dans les sections précédentes, il constitue un choix éthique qui peut s'allier à la blockchain pour le développement de systèmes de paiement mobile très sécurisés.

6. Bibliographie

[LER 13] LERNER T., « Mobile Technology and Security », dans T. LERNER (dir.), *Mobile payment*, Springer Vieweg, Mainz, 2013.

[PAT 17] PATHIRANA P. A., AZAN S. M. F., « Factors influencing the use of mobile payments — A conceptual model », dans *2017 National Information Technology Conference (NITC)*, Colombo, Sri Lanka, 2017.

[WAN 16] WANG Y., HAHN C., SUTRAVE K., « Mobile Payment Security, Threats, and Challenges », dans *2016 Second International Conference on Mobile and Secure Services (MobiSecServ)*, Gainesville, FL, 2016.

[PAS 16] PASQUET M., GERBAIX S., « Fraud on host card emulation architecture: Is it possible to fraud a payment transaction realized by a mobile phone using an "Host Card Emulation" system of security? », dans 2016 Second International Conference on Mobile and Secure Services (MobiSecServ), Gainesville, FL, 2016.

[CAS 15] CASTÉRAN S., « Le paiement sans contact n'est pas sans risque » *https://lejournal.cnrs.fr/articles/le-paiement-sans-contact-nest-pas-sans-risque*. 2015

[TIL 15] TILL HALBACH T., « A prototype-based case study of secure mobile payments », dans *eChallenges e-2015 Conference: IEEE,* Vilnius, Lithuania, 2015.

[URI 14] URIEN P., « Innovative mobile payments in the cloud for connected citizen: The MobiSIM project », dans *18th Mediterranean Electrotechnical Conference (MELECON): IEEE*, Lemesos, Cyprus, 2016.

[YEH 17] YEH, K. H., « A Secure Transaction Scheme With Certificateless Cryptographic Primitives for IoT-Based Mobile Payments », *IEEE Systems Journal* 12, n° 2, p. 2027-2038, 2018.

[WU 15] WU Y., YING, L., « A Cloudlet-based Multi-lateral Resource Exchange Framework for Mobile Users », dans *2015 IEEE Conference on Computer Communications (INFOCOM)*, Kowloon, 2015.

[GCI 17] Global Connectivity Index (GCI), « Harnessing the Power of Connectivity: Mapping your transformation into a digital economy with GCI 2017 » *https://www.huawei.com/minisite/gci/assets/files/gci_2017_whitepaper_en.pdf?v=20191217v2*. 2017.

[ZEN 16] ZHENG X., YANG L., SHI G., MENG D., « Secure Mobile Payment Employing Trusted Computing on TrustZone Enabled Platforms », dans 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, 2016.

[KAN 17] KANG J., NYANG D., A Privacy-Preserving Mobile Payment System for Mass Transit », *IEEE Transactions on Intelligent Transportation Systems* 18, n° 8, p. 2192-2205, 2017.

[PUR 16] PURMONO A.T., GONDOKARYONO Y.S. and KIM C.S., « Mutual authentication in securing mobile payment system using encrypted QR code based on public key infrastructure », dans *2016 6th International Conference on System Engineering and Technology (ICSET)*, Bandung, 2016.

[SAN 16] SAN, A. M., SATHITWIRIYAWONG C., « Privacy-Preserving Offline Mobile Payment Protocol based on NFC », dans 2016 International Computer Science and Engineering Conference (ICSEC), Chiang Mai, 2016.

[DIG 20] Digicel Haïti, « Comment puis-je ouvrir un portefeuille mini ou complet? » *https://support-ht.digicelgroup.com/hc/fr/articles/115014825127-Comment-puis-je-ouvrir-un-portefeuille-mini-ou-complet-*. 2020.

[PIE 11] PIERRE S., « Introduction à la mobilité et aux systèmes cellulaires » dans S. PIERRE (dir.), *Réseaux et Systèmes Informatiques Mobiles : Fondements, Architectures et Applications*, Presses internationales Polytechnique, Montréal, 2011.

[SHE 16] SHERIF M. T., « Mobile Payment » dans M. T. SHERIF (dir.), *Protocols for secure electronic commerce*, CRC press, Boca Raton, 2016.

[LAK 17] LAKSHMI K. K., GUPTA H., RANJAN J., « USSD—Architecture analysis, security threats, issues and enhancements », dans *2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS)*, Dubai, 2017.

[NYA 13] NYAMTIGA B. W., ANAEL S., LOSERIAN S. L. « Security Perspectives for USSD versus SMS in conducting mobile transactions: A case study of Tanzania », *international journal of technology enhancements and emerging engineering research* 1, n° 3, p. 38-43, 2013.

[MAR 16] MARGRAF M., LANGE S., OTTERBEIN F., « Security evaluation of apple pay at point-of-sale terminals », dans *2016 10th International Conference on Next Generation Mobile Applications, Security and Technologies (NGMAST)*, Cardiff, 2016.

[OSA 19] OSADCHY M., DUNKELMAN O., « It is All in the System's Parameters: Privacy and Security Issues in Transforming Biometric Raw Data into Binary Strings », *IEEE Transactions on Dependable and Secure Computing* 16, n° 5, p. 796-804, 2019.

[CEN 20] Centre canadien pour la cybersécurité, « Assurer sa sécurité en ligne pendant la période d'isolement liée à la COVID-19 » *https://cyber.gc.ca/fr/nouvelles/assurer-sa-securite-en-ligne-pendant-la-periode-disolement-liee-la-covid-19*. 2020.

[XIA 20] XIAO Y., FAN Z., « 10 tendances technologiques à surveiller pendant la pandémie de COVID-19 » *https://fr.weforum.org/agenda/2020/05/10-tendances-technologiques-a-surveiller-pendant-la-pandemie-de-covid-19/*. 2020.

[COL 20] COLUMBUS L., « 2020 Roundup Of Cybersecurity Forecasts And Market Estimates » Forbes, Editors' Pick, https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/#39fc8ba6381d. 2020.

[JON 20] JONES D., « Cyber fraud surges as COVID-19 changes banking, e-commerce » *https://www.mobilepaymentstoday.com/articles/cyber-fraud-surges-as-covid-19-changes-banking-e-commerce*. 2020.

[INT 20] Interpol, « COVID-19 cyberthreats » *https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats*. 2020.

[GOU 17] Gouvernement du Canada, « Menaces courantes à connaître, Pensez cybersécurité » https://www.pensezcybersecurite.gc.ca/cnt/rsks/cmmn-thrts-fr.aspx. 2017.

[BES 20] BEST I., « Paiements: les chiffres précis de la Banque de France sur l'effet du confinement » *https://point-banque.fr/2020/06/26/paiements-les-chiffres-precis-de-la-banque-de-france-sur-leffet-du-confinement/*. 2020.

[QYR 19] QYR- 13533967, « Global near field communication market size, status and forecast 2019-2025 » 360 Market Uptodates, *https://www.360marketupdates.com/global-near-field-communication-market-13533967*. 2019.

[BLA 20] BLACK T., « Votre chèque est à la poste? Vivement que cette phrase disparaisse! Paiements Canada » *https://www.paiements.ca/%C3%A0-propos/nouvelles/votre-ch%C3%A8que-est-%C3%A0-la-poste-vivement-que-cette-phrase-disparaisse?_ga=2.80804949.373599260.1589202732-1337160026.1586962600*. 2020.

[ITA 18] ITALIS O., Étude comparative des plateformes de paiement mobile, mémoire de maîtrise, Institut des sciences, des technologies et des études avancées d'Haïti, 2018.

[GUP 16] GUPTA N. K., *Inside Bluetooth Low Energy*, *second Edition*, Artech House Publishers, Boston, 2016.

[PAD 17] PADGETTE J., BAHR J., BATRA M., HOLTMANN M., SMITHBEY R., CHEN L. SCARFONE K., « Guide to Bluetooth Security » *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf*. 2017

[WAN 15] WANG P., ALI A., KELLY W., « Data security and threat modeling for smart city infrastructure », dans *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, Shanghai, 2015.

[EUR 18] Eur-Lex, « Règlement général sur la protection des données », Journal officiel de l'Union européenne *https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679*. 2019.

[ANS 20] *https://www.ssi.gouv.fr/*. 2020.

[EUR 20] Europol, « Rapport: Pandemic profiteering: how criminals exploit the COVID-19 crisis », *https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis*. 2020.

[DIG 20] Digicert, « Qu'est-ce qu'un certificat SSL ? » *https://www.websecurity.digicert.com/fr/ca/security-topics/what-is-ssl-tls-https*. 2020.

[THA 15] Thales, « Sécurité des paiements sans contact : la technologie HCE trace la voie », *https://www.thalesgroup.com/fr/systemes-dinformation-critiques-et-cybersecurite/event/securite-des-paiements-sans-contact-la*. 2015.

[ANT 10] ANTONI J.-P., VUIDEL G., « MobiSim: un modèle multi-agents et multi-scalaire pour simuler les mobilités urbaines », dans J.-P. ANTONI, *Modéliser la ville. Forme urbaine et politiques de transport*, Economica, coll. Méthodes et approches, 2010.

[OFF 15] Office québécois de la langue française, « Infonuagique » *http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26501384*. 2015.

[GON 13] GONZALES L., « Qu'est-ce que le 802.1X ? » https://blog.devensys.com/introduction-authentification-reseau-802-1x/. 2013.

[ARM 20] ARM Developer, « Fast Models » https://developer.arm.com/tools-and-software/simulation-models/fast-models/. 2020.

[AHA 19] AHAMED M. S., MUSTAFA H. A., « A Secure QR Code System for Sharing Personal Confidential Information », dans *2019 International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2)*, Rajshahi, 2019.

[ASA 15] ASADUZZAMAN A., GUMMADI D., WAICHAL P., « A promising parallel algorithm to manage the RSA decryption complexity », dans *SoutheastCon 2015*, Fort Lauderdale, 2015.

[TOR 18] TORRES G., « Attaques de l'homme du milieu : qu'est-ce que c'est et comment les éviter » *https://www.avg.com/fr/signal/man-in-the-middle-attack/*. 2018.

[MUR 13] MURPHY A., « Estonia's Mobile-ID: Driving Today's e-Services Economy », *https://www.gsma.com/identity/wp-content/uploads/2013/07/GSMA-Mobile-Identity_Estonia_Case_Study_June-2013.pdf*. 2013.

[KHA 19] KHAN B., SYED T., « Recent Progress in Blockchain in Public Finance and Taxation », dans *2019 8th International Conference on Information and Communication Technologies (ICICT)*, Karachi, 2019.

[LIN 2020] The Linux Foundation *https://www.linuxfoundation.org/*. 2020.

[W3C 20] World Wide Web Consortium *https://www.w3.org/*. 2020.

[BIT 20] bitcoin.org *https://bitcoin.org*. 2020.

[PAE 20] Paessler, « Qu'est-ce qu'une adresse IP *?* » *https://www.fr.paessler.com/it-explained/ip-address*. 2020.

[COM 20] Commission Nationale de l'Informatique et des Libertés (CNIL) https://www.cnil.fr/, 2020.

Biographies

Schallum PIERRE est chargé scientifique et éthique à l'Institut intelligence et données (IID) de l'Université Laval et professeur à temps partiel à l'Université Saint-Paul. Chercheur en éthique des données massives, il s'intéresse à la question de l'identité dans ses dimensions technologiques, numériques, anthropologiques, idéologiques et historiques. Il a effectué un stage postdoctoral à Polytechnique Montréal, au Laboratoire de recherche en réseautique et en informatique mobile (LARIM), dans le cadre du projet "*Recherche et développement d'une plateforme de paiement mobile*". Il est détenteur d'un doctorat en philosophie de l'Université Laval et a été membre du comité d'éthique de la même université.

Olson ITALIS a obtenu un diplôme d'ingénieur électronicien à la faculté des sciences de l'Université d'État d'Haïti en 2011, puis une maîtrise en Génie informatique et technologies de l'information à l'institut des sciences, des technologies et des études avancées d'Haïti (ISTEAH), en 2018. Il est actuellement doctorant à Polytechnique Montréal, attaché au Laboratoire de recherche en réseautique et en informatique mobile (LARIM). Son champ de recherche inclut la sécurité dans les systèmes informatiques mobiles, la conception de services en environnement informatique distribué, notamment la Blockchain. Il est également maitre d'enseignement à l'ISTEAH.

