УДК 004.3; 004.7

Б. І. Гаваньо
Національний університет "Львівська політехніка"
кафедра електронних обчислювальних машин

ПРОБЛЕМИ КОНФІДЕНЦІЙНОСТІ ТА БЕЗПЕКИ В КІБЕРФІЗИЧНИХ СИСТЕМАХ ІНТЕЛЕКТУАЛЬНИХ БУДИНКІВ

Розумні будинки стають дедалі популярнішими для продуктів та послуг IoT з великою кількістю обіцянок для покращення якості життя людей. Тим не менше, гетерогенна, динамічна та пов'язана з Інтернетом природа цього середовища додає нових побоювань, оскільки приватні дані стають доступними, часто без відома власників. Ця доступність поряд із зростаючими ризиками захисту даних та порушень конфіденційності робить безпеку інтелектуального будинку важливою темою, яка заслуговує уваги. Наведено огляд проблем конфіденційності та безпеки, спрямованих на кіберфізичні системи розумних будинків. Також визначено обмеження, оцінено рішення та завдання та проблеми, які потребують подальшого дослідження.

Ключові слова: інтелектуальний будинок, кіберфізична система, інтернет речей, конфіденційність, безпека.

B. I. Havano
Lviv Polytechnic National University,
Computer Engineering Department

PROBLEMS OF PRIVACY AND SECURITY IN CYBER PHYSICAL SYSTEMS OF INTELLECTUAL HOUSES

Smart homes have become increasingly popular for IoT products and services with a lot of promises for improving the quality of life of individuals. Nevertheless, the heterogeneous, dynamic, and Internet-connected nature of this environment adds new concerns as private data becomes accessible, often without the householders' awareness. This accessibility alongside with the rising risks of data security and privacy breaches, makes smart home security a critical topic that deserves scrutiny. In current paper, is presented an overview of challenges related to the privacy and security in the smart house cyber physical systems. Also, were realized constraints, evaluated solutions, and a several challenges and research issues where further investigation is strongly required. I have identified issues that need to be solved: risk assessment methods, information flow control accesses, identity management, and security management methods.
Keywords: smart house, cyber physical system, IoT, privacy, security.

Вступ

Серед перших розумних домашніх пристроїв було придбано за 100 фунтів "Кухонний комп'ютер", який запропонував у 1969 році Неман Маркус за 10 тисяч доларів із умовою пройти курс програмування, щоб вводити та читати рецепти. З того часу було розроблено багато версій розумних будинків, таких як MavHome [1], які, як правило, також підключені до Інтернету, щоб

забезпечити можливість віддаленого спостереження та контролю. Ці розумні будинки використовують багато різних сенсорних технологій. Останні інтелектуальні домашні пристрої містять мікрофони для голосової взаємодії та використання хмар для зберігання та обробки. Крім того, вони можуть створювати ознаки програмування, що дозволяють розробити розумні служби для дому, такі як Apple HomeKit, Google Weave / Brillo та Samsung SmartThings. Сьогодні будь-який будинок можна легко модернізувати за допомогою персоналізованих, доступних та потенційно "інтелектуальних" пристроїв.

Розумний будинок можна визначити як місце проживання, яке містить багато датчиків, систем та пристроїв, до яких можна віддалено доступитись, керувати та контролювати через мережу зв'язку [2]. Згідно з недавнім дослідженням [3], глобальний ринок інтелектуальних будинків у 2015 році оцінюється в 9,8 мільярда доларів і, за оцінками, досягне 43 мільярдів доларів у 2020 році. Згідно з іншим дослідженням [4], ринок інтелектуальних будинків, як очікується, подвоїться в США, оскільки безпека сім'ї є найбільшим мотиватором.

Проте зростаюче розгортання пристроїв, підключених до Інтернету, у домашніх умовах ставить під загрозу конфіденційність та безпеку, оскільки особиста інформація стає віддалено доступною новими способами. Зловмисник, наприклад, може підслуховувати бездротові передачі датчиків та виявляти такі дії, як приймання душу, туалет та сон [5]. Крім того, зловмисник може дистанційно перебирати контроль над домашніми пристроями, використовуючи їх, щоб зламати домогосподарство або як платформу для запуску атак на інші домени, наприклад, перевантажити енергосистему. Було проведено успішні атаки на різні комерційні продукти із незавершеного виробництва [6–8]. Ці напади не тільки гіпотетичні: наприклад, у 2014 році було виявлено, що дані з понад 73 000 відеокамер доступні в Інтернеті.

Технологія інтелектуального будинку

Як правило, інтелектуальний будинок містить безліч підключених пристроїв, що належать до різних областей застосування. Зазвичай сфери застосування розбито на чотири групи: розваги, енергетика, безпека та охорона здоров'я [9]. Розваги спрямовані на максимальне покращення комфорту та зручності, надаючи індивідуальний вміст для розваг та послуги соціального спілкування. Енергетичні програми спрямовані на забезпечення ефективного споживання енергії та управління. Домен безпеки пропонує послуги, призначені для виявлення загроз безпеці та контроль за ними. Програми охорони здоров'я зосереджені на наданні мобільних медичних послуг та підтримці фітнесу. Можливо, медична установа має найширший спектр ризиків, починаючи від підслуховування до фатального хакерства. Як приклад на рис.1 показано типову архітектуру системи інтелектуального дому.

А. Пристрої

Розумні домашні пристрої – це апаратні пристрої, що зазвичай містять датчики, виконавчі пристрої, шлюзи та інтелектуальні об'єкти. Окремі типи пристроїв:

1) датчики – вимірюють фізичну властивість середовища або фізичної особи. Датчики можуть варіювати від мобільних (наприклад, браслетів) до датчиків, які не носять (наприклад, IP-камери). Відеокамери вважаються датчиками, які порушують конфіденційність [10] разом із мікрофонами;

2) виконавчі пристрої виконують такі дії, як ввімкнення / вимкнення або затемнення ліхтарів, закриття вікон, спрацьовування сигналів тривоги тощо;

3) шлюз слугує точкою доступу до будинку, що дозволяє користувачеві або іншому об'єкту відстежувати, контролювати та управляти побутовою технікою або датчиками віддалено. Крім того, він слугує точкою агрегації для надсилання вимірюваних даних до зовнішньої мережі;

4) розумні об'єкти – це пристрої, що складаються з датчиків та / або приводів, які підключені до домашньої мережі. Прикладами цього є розумні пристрої, такі як розумні замки, які відповідають на дзвінки і забезпечують контроль за часом.

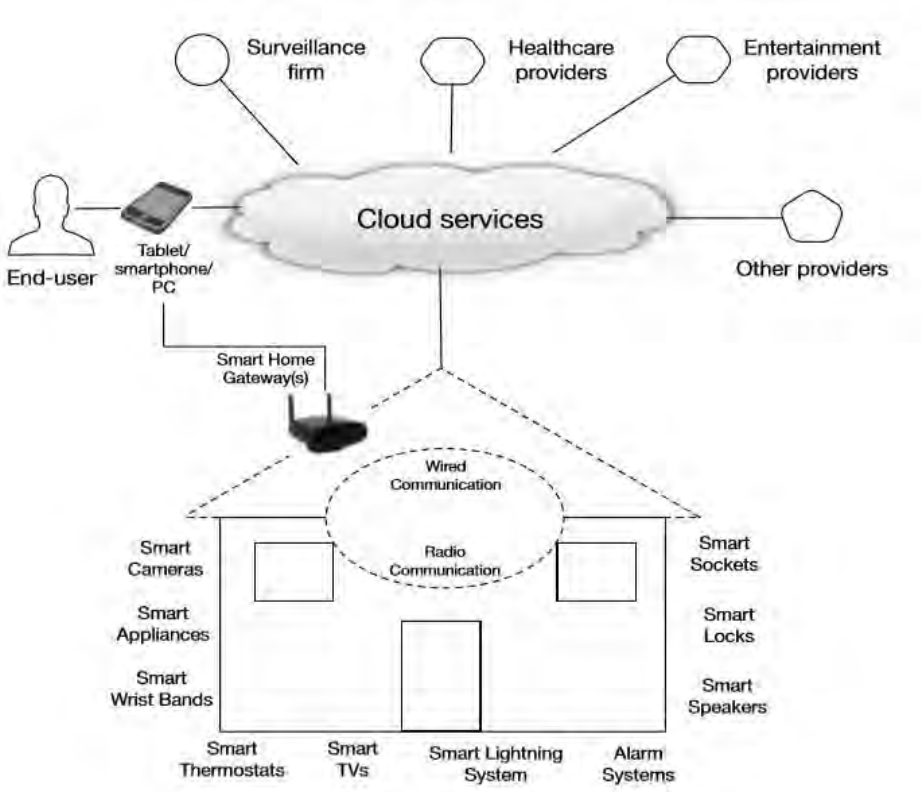

Рис. 1. Типова архітектура системи інтелектуального дому

Б. Зв'язок

Типовий зв'язок інтелектуального будинку використовує різні протоколи зв'язку. Вони варіюють від протоколів дротового зв'язку до радіозв'язку. Як правило, датчики спілкуються з використанням протоколів домашньої автоматизації, таких як KNX, ZigBee, Z-Wave і DASH7, або через протоколи мережевого зв'язку, такі як Wi-Fi, Bluetooth, 6LoWPAN, IEEE 802.15.4 або стільникова технологія. RFID та технології NFC також використовуються для моніторингу та відстеження мешканців, особливо у сфері охорони здоров'я, і зазвичай використовуються в розумних дверних замках.

В. Сервіси

Сервіси – це програмні додатки, розміщені у хмарі або усередині домашнього середовища, які відповідають за впровадження автоматизації, управління пристроєм, прийняття рішень тощо. Спеціальна категорія служб – це контролери, які дозволяють керувати підключеними пристроями. Як правило, домашні господарства запускають таке програмне забезпечення через свої смартфони або планшети, щоб локально або дистанційно взаємодіяти з пристроєм.

Виклики безпеки і конфіденційності

Інтелектуальний будинок може містити конфіденційні дані (наприклад, особисті фотографії, відеоролики та цифрові щоденники), а також такі пристрої, як IP-камери, які можуть бути віддалено активовані та доступні з будь-якого місця. Крім того, в ньому можуть бути мікрофони, які можуть слухати приватні розмови: наприклад, такі акустичні системи, як Amazon Echo та Google Home, мікрофони, які запрограмовані для прослуховування команди "прокинься" та голосової підказки для виконання таких завдань, як затемнення світла та відтворення музики. Це вимагає жорстких вимог до безпеки через важливість приватної інформації. Однак пристосування стандартного контролю безпеки до інтелектуальних будинків є складним завданням, як визначають Лі і співавт. [11]. Нижче розширено згадані проблеми та налаштовано їх на різні архітектурні шари.

А. Питання пристрою

Ресурсні обмеження: розумні пристрої для домашнього використання часто використовуються без вимкнення та використовують малопотужні процесори з низькими тактовими частотами та невеликою пропускною спроможністю. Це робить обчислювально дорогими криптографічні алгоритми, такі як RSA, які важко приєднати до таких низькопродуктивних пристроїв [12]. Це також ускладнює обмеження оперативної пам'яті та флеш-пам'яті.

Безголова природа: типові пристрої IoT не містять клавіатури, миші та екрана. Це може змусити кінцевих користувачів покладатися на смартфони або веб-сайти для введення параметрів. Крім того, це робить такі механізми, як "повідомлення та згоду", складнішими для впровадження в інтелектуальних будинках.

Пакети, що стійко захищені від несанкціонованого доступу: інтелектуальні домашні пристрої більшу частину часу є фізично доступними, що робить їх схильними до фізичних втручань. Іноді домовласники можуть проводити цю атаку, наприклад, втручаючись у розумні лічильники, щоб зменшити витрати на виставлення рахунків. Проте технічне сальдо можуть також проводити інші організації.

Б. Питання комунікації

Гетерогенні протоколи: різні комунікаційні протоколи, які, можливо, використовуються для з'єднання пристроїв у інтелектуальному домі, вимагають використання мостів, вузлів або шлюзів. Крім того, пристрій може використовувати власний протокол (наприклад, не на базі IP) локально та стандартний для підключення до хмари. Ці фактори, пов'язані з апаратними обмеженнями, можуть призвести до того, що інженери мережі обирають слабші схеми шифрування [13].

Динамічні характеристики: такі пристрої як носії можуть приєднуватися або залишати домашню мережу в будь-який час і, можливо, з будь-якого місця. Це підвищує необхідність розроблення алгоритмів стійкості безпеки і робить відстеження та управління активами складним завданням. Параметри багатопротокольного зв’язку разом з різними можливостями пристрою також роблять традиційні схеми захисту не придатними для домашніх пристроїв [14].

В. Проблеми з сервісом

Очікування довголіття: для пом'якшення вразливостей системи безпеки потрібне віддалене перепрограмування. Однак це може виявитися неможливим для всіх пристроїв, оскільки операційна система, стек протоколу або прошивки не підтримують динамічних виправлень. Більше того, деякі пристрої, наприклад, розумні вимірювачі, розроблено, тож очікують, що вони залишатимуться в мережі протягом багатьох років, не вимагаючи заміни або безпосередньої підтримки компонентів.

Підходи до збереження безпеки та конфіденційності

Технологічні підходи до пом'якшення загроз безпеці та конфіденційності можна поділити на рішення пристроїв та комунікацій (мереж) [8]. У роботі, дотримуючись архітектури, описаної в розділі II, також додано мінімізацію рівня обслуговування. Визначені методи є адаптацією роботи Анвара та співавт. [15] щодо інтегрованої парадигми охорони здоров'я до інтелектуального домашнього домену. Приклади визначаються з останніх наукових та галузевих джерел.

А. Підходи до рівня пристрою

Безпека рівня пристрою зосереджена на гарантіях, які підтримуються на пристроях. Це передбачає такі методи, як апаратне шифрування, дизайн пристроїв із захистом від несанкціонованого доступу та механізми контролю доступу на основі пристроїв. За підходами, які пропонують вбудовувати архітектуру безпеки, включаючи посилення захищеності транспортного рівня Datagram [16] та реалізацію в межах апаратних шифрів, було запропоновано процедури безпеки [17], сумісні з IEEE 802.15.4. Також оптимізовано версії криптографічних алгоритмів, такі як ECDSA, розроблені для обмежених середовищ. Також побудовано різні платформи, які раніше розглядали безпеку та конфіденційність на стадії розроблення. Однією з таких платформ є RERUM [18]. Це покриває безпеку на всіх рівнях стек-мережевого протоколу з наголосом на елементах керування пристроєм. Він реалізує захист пристроїв за допомогою безпечного завантаження, когнітивної радіотехніки та механізмів контролю доступу. З боку індустрії гарантії можуть

передбачати використання апаратного забезпечення та прошивки, сертифіковані за спільними критеріями та EMVCo IC Security Evaluation. Крім того, це може включати використання криптографічних алгоритмів, схвалених, наприклад, Національним інститутом стандартів і технологій. Проблема полягає в тому, що більшість пристроїв мають серйозні ресурсні обмеження, і нові стандарти, в основному, експерименту обмежують їх ширшу придатність та прийнятність у промисловості. Окрім того, це може виявитись неможливим у значних масштабах із потенційно високими додатковими витратами порівняно з вартістю традиційних пристроїв IoT.

Б. Підходи до рівня комунікації

Рішення рівня зв'язку є ефективними, коли дані передаються між пристроями, службами та кінцевими користувачами. Популярні схеми передбачають використання віртуальних приватних мереж (VPN), міжмережевих екранів та систем виявлення вторгнень (IDS) або систем захисту від вторгнення (IPS). Цей підхід, як правило, реалізується в центральному шлюзі / проксі і у хмарі. Придатність міжмережевих екранів, IDS та IPS у межах інтелектуального домашнього контексту обговорюється Mantasetal [19]. Замість того, щоб використовувати брандмауери та підхід IDS / IPS, Нгуєн та ін. [20] використовують анонімну систему на основі TOR, яка допомагає захистити конфіденційність користувачів та підвищує безпеку інтелектуальної побутової техніки. Нещодавно на ринку з'явилися спеціалізовані інтелектуальні домашні пристрої, які підключаються до домашнього маршрутизатора, який виконує роль мережевих притулків. Наприклад, Cujo, Dojo та Keezel є прикладами цього. Cujo та Dojo працюють як пристрої брандмауера, які контролюють, аналізують та блокують загрози в режимі реального часу. Keezel створює тунель VPN для шифрування пристроїв і з'єднань. Організації безпеки, такі як Європейське агентство з інформаційної безпеки мережі та Cloud Security Alliance складають великі обсяги документації, розробляючи гарантії мережі на рівні мережі. Проте на практиці залишається проблемою те, що деякі пристрої можуть переміщуватися мережею та спілкуватися за допомогою зашифрованих каналів. Це ускладнює аналіз трафіку, якщо не підтримується технологія глибокого пакетного огляду. Крім того, пристрої все ще можуть бути схильні до локальних атак, наприклад, шкідливий код, встановлений через скомпрометовану пам'ять.

В. Підходи службового рівня

Підходи до рівня обслуговування зосереджені на програмних ресурсах високого рівня. Типові підходи містять безпечні процеси розроблення, такі як тестування безпеки, принципи безпечного проектування та маскування даних. Останнє може містити використання методів збереження конфіденційності, таких як k-анонімність та криптографічні схеми, як атрибут шифрування. З погляду галузі, організації, такі як проект відкритої веб-застосунок безпеки, беруть участь у наданні безпечних посібників з розроблення, таких, як системи оцінювання та посібники з тестування для розроблення пристроїв IoT. Інші організації, такі як Builditsecure.ly, надають поради щодо створення процесів інженерної безпеки. Є також такі сайти, як BugCrowd, які дозволяють розробникам аналітики безпеки перевіряти код. На практиці, однак, немає офіційного керівного органу чи організації, яка забезпечує кінцевим споживачам гарантовану репутацію, яку надає конкретний постачальник послуг. Крім того, певні методики, що підвищують конфіденційність чи безпеку, можуть мати побічні ефекти. Наприклад, вони можуть призвести до втрати інформації та можуть впливати на функції персоналізації, необхідні для певних домашніх пристроїв.

Напрямки досліджень у галузі кіберфізичних систем інтелектуальних будинків

Деякі критичні питання безпеки та конфіденційності можуть залишатися непоміченими або недостатньо вивченими дослідниками, оскільки комерційна сторона цієї парадигми розвивається високими темпами. У цьому розділі обговорено деякі сфери, які потребують подальшого дослідження.

Управління ідентифікацією: пристрої, особливо під час підключення до Інтернету та забезпечення операцій та керування третіми сторонами, потребують контролю автентичності та авторизації. Розроблення ефективного рішення для управління ідентифікацією передбачає розроблення

захищених протоколів управління ключами. Однак це важко реалізувати для налаштування бездротових сенсорних мереж [11], і це ускладнюється наявністю різних, іноді несумісних технологій і відсутністю глобальних ідентифікаційних схем [21]. Інший складний аспект полягає в тому, що процедури автентифікації можуть бути складні для окремих осіб і можуть викликати додаткові проблеми конфіденційності.

Методи оцінювання ризику: власнику будинку важко оцінити фінансову вартість своїх особистих даних. Оскільки він може не знати, які особисті дані зібрано, і чи ці дані розголошено сторонам, про які він не знає. Крім того, не завжди зрозуміло, наскільки легко отримати таку інформацію та використовувати її для негативних дій. Необхідність емпіричних методів оцінювання ризику для використання в інтелектуальних будинках визначено як важливу умову безпеки та конфіденційності [22].

Підходи до управління потоком інформації: агрегація реальних даних може надати приватні дані про поведінку та діяльність мешканців. Зрозуміліші користувацькі інтерфейси, які допомагають інтуїтивно відображати конфіденційність і водночас пропонують настроювані функції для керування подальшим використанням та розповсюдженням таких даних [23]. Це також є складною вимогою для задоволення, оскільки пристрої IoT можна розробити так, щоб вони діяли автономно, без будь-яких інструкцій з боку користувачів. Також існує необхідність у розробленні ефективних заходів, які дозволяють безпечно видаляти збережені дані, особливо для задоволення регуляторних вимог.

Методи управління безпекою: відсутні методи управління інформаційної безпеки, зокрема, кращі підходи до виправлення, оновлення та надання інформації домашнім господарствам [24]. Зазначено у [22], що необхідність інтеграції безпеки в дизайні та безпечних процесів керування безпекою, як правило, не є завданням розроблення інтелектуальних будинків.

Висновки

Порівняно з традиційними цифровими системами більшість інтелектуальних домашніх пристроїв мають обмеження в обчислювальній потужності, пам'яті та енергії. Це призводить до того, що впроваджувати ефективні заходи безпеки та конфіденційності в розумному домашньому середовищі стає дедалі важче. Крім того, конфіденційність є складною і не завжди очевидною. Тим не менш, забезпечення конфіденційності та безпеки в будинках необхідно розглядати як пріоритетне завдання. Описано найбільш актуальні проблеми безпеки та конфіденційності, пов'язані з інтелектуальними будинками. Крім того, визначено підходи до подолання проблем на різних рівнях архітектури та запропоновано області, де потрібні подальші дослідження. Як загальне спостереження: сьогодні формуються деякі ініціативи для забезпечення безпеки та зміцнення конфіденційності користувачів. Незважаючи на це, виявлено чотири суттєві виклики, які необхідно вирішити: управління ідентифікацією, методи оцінювання ризиків, підходи до управління інформаційними потоками та методи управління безпекою. Такі виклики посилюються в області інтелектуальних будинків, але також є загальними для інших кіберфізичних систем, де застосовуються пристрої IoT.

1. D. J. Cook et al., "MavHome: An agent-based smart home", IEEE International Conference on Pervasive Computing and Communications, San Diego, CA, USA, pp. 521–524, 2003. 2. N. King, "Smart home – A Definition", Milton Keynes: Intertek Research and Testing Centre, 2003. 3. Statista, 2015 [Online]. Available: https://goo.gl/89rRIa. 4. August and Xfinity, "The Safe and Smart Home: Security in the Smart Home Era," 2016 [Online]. Available: http://goo.gl/UGWb5Z. 5. V. Srinivasan et al., "Protecting your daily in-home activity information from a wireless snooping attack," 10th international conference on Ubiquitous computing, pp. 202–211, 2008. 6. B. Ur et al., "The current state of access control for smart devices in homes," Workshop on Home Usable Privacy and Security, 2013. 7. S. Notra et al., "An experimental study of security and privacy risks with emerging household appliances", IEEE Conference on Communications and Network Security, pp. 79–84, 2014. 8. V. Sivaraman et al., "Network-level security and privacy control for smart-home IoT devices," Wireless and Mobile Computing,

Networking and Communications, pp. 163–167, 2015. 9. T. D. P. Mendes et al., "Smart home communication technologies and applications: Wireless protocol assessment for home area network resources", Energies, vol. 8, no. 7, pp. 7279–7311, 2015. 10. C. Debes et al., "Monitoring Activities of Daily Living in Smart Homes: Understanding human behavior", IEEE Signal Processing Magazine, vol. 33, no. 2, pp. 81-94, 2016. 11. C. Lee et al., "Securing smart home: Technologies, security challenges, and security requirements", IEEE Conference on Communications and Network Security, pp. 67–72, 2014. 12. K. Islam et al., "Security and privacy considerations for wireless sensor networks in smart home environments", Computer Supported Cooperative Work in Design, IEEE 16th International Conference on, pp. 626–633, 2012. 13. H. Chan and A. Perrig, "Security and privacy in sensor networks", Computer, vol. 36, no. 10, pp. 103–105, 2003 14. M. M. Hossain et al., "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things", Services, pp. 2128, 2015. 15. M. Anwar et al., "Anytime, anywhere access to secure, privacy-aware healthcare services: Issues, approaches and challenges", Health Policy and Technology, vol. 4, pp. 299–311, 2015. 16. S. L. Keoh et al., "Securing the internet of things: A standardization perspective", Internet of Things Journal, IEEE, vol. 1, no. 3, pp. 265–275, 2014. 17. D. Altolini et al., "Low power link layer security for IoT: Implementation and performance analysis", Wireless Communications and Mobile Computing Conference, pp. 919–925, 2013. 18. H. C. Pohls et al., "RERUM: Building a reliable IoT upon privacy-and security-enabled smart objects", Wireless Communications and Networking Conference Workshops, pp. 122–127, 2014. 19. G. Mantas et al., "Security in smart home environment", Wireless Technologies for Ambient Assisted Living and Healthcare: Systems and Applications, pp. 170–191, 2010 20. N. P. Hoang and D. Pishva, "A TOR-based anonymous communication approach to secure smart home appliances", Advanced Communication Technology, pp. 517–525, 2015. 21. A. Riahi et al., "A systemic approach for IoT security", Distributed Computing in Sensor Systems, pp. 351–355, 2013. 22. A. Jacobsson and P. Davidsson, "Towards a Model of Privacy and Security for Smart Homes," IEEE 2nd World Forum on Internet of Things, vol. 2, pp. 727–732, 2015 23. M. Henze et al., "A comprehensive approach to privacy in the cloud-based Internet of Things," Future Generation Computer Systems, vol. 56, pp. 701–718, 2016. 24. D. Barnard-Wills et al., "ENISA Threat Landscape and Good Practice Guide for Smart Home and Converged Media", ENISA (The European Network and Information Security Agency), 2014.