КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№2 (6), 2019
ISSN 2663 - 4023
DOI:10.28925/2663-4023.2019.6.134141
УДК 004.056.55

Білова Анастасія Олександрівна
магістр факультету інформаційних технологій
Державний університет телекомунікацій,
Python Software Engineer Remme, Київ, Україна
ORCID: 0000-0001-7395-6079
anastasiabilova@gmail.com

Онищенко Вікторія Валеріївна
доктор технічних наук, професор,
завідувач кафедри Інженерія програмного забезпечення,
Державний університет телекомунікацій, Київ, Україна
ORCID: 0000-0002-3126-2260
oviva@ukr.net

МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ РОЗУМНОГО БУДИНКУ

Анотація. Дане дослідження присвячене проблемі безпеки Інтернет речей (IoT), а саме: здійснено огляд загроз інформаційній безпеці розумного будинку та проаналізовані існуючі методи безпеки його пристроїв. Інтернет речей зазнає експоненціального зростання в галузі досліджень та промисловості. Разом з цим все більше постає загроз, пов'язаних з безпекою інформаційних програм та баз даних. Як відомо, фундамент безпеки інтернету речей складається з чотирьох частин: безпека зв'язку, захист пристроїв, контроль пристроїв і контроль взаємодії в мережі. Відповідно досліджуються джерела загроз та характеристики уразливостей інформаційній безпеці IoT. Звичайні підходи до безпеки та конфіденційності, як правило, не застосовуються для IoT, головним чином через його децентралізовану топологію та обмеження ресурсів більшості її пристроїв. Аналіз наукових джерел дозволив дослідити різні підходи забезпечення безпеки розумного будинку: архітектурний метод з трьома модулями для захисту конфіденційності аналізу даних розумного будинку; метод обмеження на рівні мережі; технологія Blockchain. Визначено, що запропонована платформа розумного будинку на основі Blockchain дозволяє забезпечити безпеку інформації з урахуванням основних цілей безпеки - конфіденційності, цілісності та доступності. Блокчейн може використовуватися для відстеження вимірювань даних сенсора та запобігання дублюванню будь-якими іншими шкідливими даними, для автентифікації та безпечної передачі даних. Дане дослідження сприятиме проектуванню та розробці нових методів та технологій забезпечення безпеки розумного будинку.

Ключові слова: Інтернет речей (IoT, Internet of Things); розумний будинок; Blockchain; безпека.

1. ВСТУП

Постановка проблеми. Наше сьогодення – це стрімке зростання інформаційно-комунікаційних технологій та їх застосування у різних сферах виробництва, навчання, побуту. Не виняток – технологія Інтернет речей (Internet of Thing), інтеграція якої у людське життя забезпечує покращання останнього, тому дана технологія прогресує своїми розробками та впровадженням. Вбачається, що у 2025-2030 роках ринок технологій IoT у Європі буде складати 1 трлн. євро. Вважають, що технології Інтернету речей дозволять у 2030-2040 роках: 10-15% - економії бюджету на охорону здоров'я; 10-15 років – збільшення тривалості життя; 40-50 % - збільшення врожайності; 15-20%

збільшення пропускної здатності доріг у містах; 85-90 % зменшення кількості автомобілів; 10-15 разів зменшення витрат на логістику [1, с. 8].

Оскільки IoT – це комплекси та системи, які з'єднані між собою мережею Internet, містять сучасні алгоритми штучного інтелекту, технології хмарних обчислювань, то слід відзначити, що з розвитком даної технології постають загрози, пов'язані з безпекою інформаційних програм та баз даних. Основними складовими безпеки інтернету речей є безпека зв'язку, захист пристроїв, контроль пристроїв і контроль взаємодії в мережі. У річному звіті Cisco за 2018 рік [2] вказується, що спеціалісти із захисту швидкими темпами впроваджують IoT-пристрої, проте звертають мало уваги на безпеку цих систем. Незахищені та неконтрольовані IoT-пристрої надають зловмисникам можливість проникати в мережі. Так, дослідники загроз із компанії Cisco виявили 224 нових вразливості в продуктах, які не належать Cisco: з них 74 уразливостей з IoT-пристроями. Як розвивається та розширюється IoT, те саме відбувається і з мережами ботів IoT. Та оскільки ці мережі ботів зростають та вдосконалюються, зловмисники використовують їх для запуску DDoS-атак з усе більшою інтенсивністю та масштабністю. Звіт IoT за 2018 рік компанії Gemalto свідчить, що найбільшою проблемою є захист даних, обсяги яких зростають: тільки 60% організацій визнають шифрування цих даних, а 40% залишають їх уразливими; 48% компаній не можуть виявити, який пристрій IoT має порушення.

Є очевидним, що забезпечення надійного захисту останніх є актуальною і найбільш складною проблемою сучасності.

Аналіз останніх досліджень і публікацій. Інтернет речей (IoT) складається з пристроїв, які генерують, обробляють та обмінюються величезною кількістю критично важливих для безпеки даних, а також конфіденційної інформації, і, отже, є привабливими для різних кібератак [3].

Існують різні дослідження щодо безпеки та конфіденційності IoT та розумного будинку. Цим питанням присвячені експериментальні дослідження вітчизняних та закордонних вчених: Л. Монастирського, О. Петришина, A. Chakravorty, T. Wlodarczyk, C. Rong, A. Dorri, R. Jurdak, S. S. Kanhere, P. Gauravaram, S. Fan, L. Song, C. Sang та інші. Вони одностайні в тому, що технологія IoT вимагає легкої, масштабованої та розподіленої безпеки та захисту конфіденційності. Важливим для таких систем є створення мереж малого радіуса дії, здатних тримати зв'язок основного процесора з багатьма пристроями і надійно передавати дані, економно витрачаючи живлення IoT пристроїв [4].

Метою статті є узагальнення та аналіз існуючих методів та засобів забезпечення безпеки та конфіденційності IoT та розумного будинку.

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Основними складовими безпеки інформації, інформаційної системи або технології виділяють наступні категорії: доступність, цілісність, конфіденційність. У нашому розумінні доступність інформації технології розумного будинку – це можливість власникам (або самим підсистемам розумного будинку) здійснювати дозволені операції та/або здійснювати своєчасно обмін між пристроями. Наприклад, відкрити / закрити двері; перевірити температуру, щоб включити або виключити кондиціонер. Цілісність інформації забезпечується повною і достовірною інформацією про стан всіх пристроїв розумного будинку. Наприклад, система знає як реагувати, коли відчувається витік газу

з відкритої конфорки. Конфіденційність інформації розумного будинку визначається тим, що витік приватної інформації не є можливим. Є зрозумілим, що порушення хоч однієї з цих складових може привести до серйозних наслідків: починаючи з курйозних ситуацій та закінчуючи випадками, які загрожують здоров'ю та життю людини.

Так, автори [5] виділили цілий спектр джерел загроз інформаційній безпеці розумного будинку та наслідки таких дій. Серед них виділяють антропогенні (хакерські атаки на основний сервер, перехват інформації, крадіжка пристроїв, наявність порушників серед персоналу); технічні (перебої в мережі електроживлення, помилки програмного забезпечення, поломка апаратури системи) та стихійні лиха.

Дослідження «Security Analysis of Emerging Smart Home Applications» науковців [6] розбиває уразливості інформаційній безпеці розумного будинку на дві категорії: надмірні привілеї (excessive privilege) і незахищений обмін повідомленнями (insecure messaging). Надмірні привілеї – це злом системи безпеки, коли мобільний додаток отримує доступ / права на операції, які йому насправді не потрібні для роботи. Коли шкідливі програми (malware) отримують необмежений доступ до SMS APIs або логи, це може привести до витоку особистої інформації (PII), включаючи пінкод або паролі.

З цими проблемами згодні автори «Smart-phones attacking smart-homes» [7]. Вони вважають, що розумні будинки вразливі до атак, здійснених смартфонами користувачів, навіть якщо домашній шлюз контролює обмін пакетами удома та поза ним. Вчені виявили серйозні недоліки безпеки у численних пристроях розумного дому: наприклад, підключені до Інтернету смарт-лампочки та комутатори живлення легко можуть бути скомпрометованими, оскільки вони мають поганий контроль аутентифікації. Цифрові фотографії-кадри, камери та динаміки передають дані в простому тексті, який легко прослухати, щоб поставити під загрозу конфіденційність користувача. Ця вразливість може бути легко використана зловмисником.

Ми поділяємо думку вчених [8], які виділяють п'ять областей, пов'язаних з безпекою IoT. Проаналізувавши 3000 звітів, новин, статей та інше, за допомогою кластеризації їм вдалося виділити наступні уразливості інформаційній безпеці IoT:

1) локальність недовіри (LAN Mistruct) – якщо пристрій здійснює автентифікацію в мережі один раз, то надалі йому довіряють;
2) екологічна недовіра (Environment) – IoT довіряє фізичному середовищу, в межах якого воно розміщене;
3) додаткові привілеї (App Over-privilege);
4) слабка автентифікація або її відсутність (No/Weak Authentication);
5) недоліки реалізації (Implementation Flaws) – витік приватної інформації; не шифрування даних та інше.

Надалі розглянемо методи та технології, що забезпечують інформаційну безпеку IoT на сучасному етапі.

3. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

В ідеалі, розумний дім має забезпечити гарантовану безпеку його мешканцям: його технологія дозволяє реагувати та запобігати аварійним ситуаціям, здійснювати контроль доступу на територію та в житло та інше. Проте, як свідчить велика кількість досліджень [1 - 13], забезпечення інформаційної безпеки розумного дому не завжди вдається, зловмисник може зламати домашню мережу та віддалено керувати пристроями розумного дому, тому ця проблема залишається актуальною у сучасному світі.

У статті [8] проаналізовані підходи до забезпечення безпеки розумного будинку. А саме,

1) підходи, пов’язані з фізичною особою:
   - автентифікація;
   - контроль доступу;
2) підходи, пов’язані з архітектурою програмного та апаратного забезпечення:
   - вбудована система безпеки в пристрій;
   - атестація пристроїв;
   - система виявлення вторгнень;
   - інформаційний потік.

Розглянемо більш детально деякі методи забезпечення безпеки інформаційної системи розумного будинку.

3.1. Архітектурний метод з трьома модулями для збереження конфіденційності аналізу даних для розумних будинків

Автори «Privacy preserving data analytics for smart homes» [9] запропонували архітектурний метод з трьома модулями для захисту конфіденційності аналізу даних для розумних будинків. Модуль збору даних регулярно збирає дані своїх датчиків та надсилає їх модулю приймача даних. Той перетворює та зберігає їх у двох різних наборах даних. Модуль результатів контролює доступ до результатів обробки даних для захисту конфіденційності. Діяльність цього модуля можна класифікувати на чотири групи. Перший — модуль контролю доступу, який автентифікує, авторизує та визначає рівень конфіденційності для будь-якої спільної інформації. Другий — модуль ретривера ідентифікаторів. Він запитує сховище словника ідентифікаторів для створення списку персональних (як фактичних, так і хешованих значень) даних, до яких кінцевий користувач має право доступу. Модуль трансформатора за допомогою цього списку узагальнює фактичні особисті значення та створює набір даних із хешованими, фактичними та узагальненими значеннями. Модуль процесора результатів запускає завдання на ідентифікованому сховищі та замінює хешовані особисті значення в наборі результатів відповідними узагальненими значеннями на основі виходу модуля трансформатора. Цей метод забезпечує доступ до даних лише справжньому користувачеві. Крім того, за допомогою двох наборів даних гарантується, що пов'язувати різні дані користувача один з одним неможливо. Також метод не забезпечує конфіденційність, коли користувачеві необхідно розкрити свої дані постачальнику послуг.

3.2. Метод обмеження на рівні мережі

У дослідженні «An experimental study of security and privacy risks with emerging household appliances» [10] автори продемонстрували, що на позаштатних пристроях IoT відсутні базові гарантії безпеки, зламавши різноманітні пристрої розумного дому, включаючи лампочку, вимикач та димовий сигнал. Вони запропонували рішення щодо захисту таких пристроїв шляхом обмеження доступу на рівні мережі. Щоразу, коли до мережі підключений новий пристрій IoT, користувач мережі, адміністратор або навіть Інтернет-провайдер може запитувати метод захисту від постачальника SaaS. Це рішення не вимагає змін від виробників пристроїв, воно зменшує навантаження на кінцевих користувачів і дозволяє забезпечити безпеку як послугу накладення Інтернет-провайдером або спеціалізованим постачальником в хмарі. Метод не узагальнений на інші пристрої розумного дому. Як недолік, вразливість від атак, здійснених смартфонами користувачів.

3.3. Технологія Blockchain

Назва походить від складання «Block» і «Chain» і дослівно перекладається як «ланцюжок блоків». Поняття «blockchain» упроваджене програмістом Satoshi Nakamoto у 2008 році, а рік по тому ним же реалізована відповідна технологія в рамках цифрової валюти — Bitcoin [11]. Саме дана технологія стала першою, яка змогла вирішити інформаційну проблему: забезпечення довіри між сторонами до отриманої інформації без залучення зовнішніх гарантів — банків, посередників тощо. Саме ця властивість зумовила впровадження даної технології у різні сфери суспільства і, як стверджують науковці, має великий потенціал в майбутньому.

Розглянемо принцип роботи технології Блокчейн.

Блокчейн – це структурована база даних, «ланцюжок блоків», де кожен блок пов'язаний з попереднім. Блок містить в собі набір записів (інформацію). Кожен новий блок з інформацією додається в кінець ланцюжка. Кожному блоку присвоюється цифровий підпис – хеш–сума, що є унікальним ідентифікатором. Хеш (hash) – це унікальний код, який змінюється при зміні навіть одного символу в тексті, розраховується за складною математичною формулою і завжди буде однаковим для однієї і тієї ж інформації. Отже, не може бути два різних хеша для абсолютно однакової інформації, тому «розірвати ланцюг», тобто внести правки у блок або додати блок між іншими неможливо.

Завдяки загальнодоступності, розподіленості та достовірності бази даних, Блокчейн виявляється привабливою та перспективною технологією для забезпечення безпеки інформаційній системі розумного будинку. Це підтверджують розробки вчених [12, 13].

У дослідженні [13] пропонується розподілене та надійне зберігання інформації IoT на основі комбінації IPFS та алгоритму шифрування. Інформація IoT зберігається в системі IPFS, а повернене хеш-значення шифрується для зберігання шифротексту в Blockchain. Авторизовані користувачі можуть отримати хеш-значення унікального індексу, що зберігається у системі IPFS, через смарт-контракт для підтвердження дозволу. Правило відповіді заздалегідь встановлено у смарт-контракті. Коли користувачеві потрібно отримати доступ до інформації про дані, потрібно ініціювати транзакцію, а інші вузли в Blockchain перевіряють транзакцію, і коли верифікація проходить і встановлене правило доступу дотримується, авторизацію можна отримати.

Прийняття Blockchain в контексті IoT не є простим і тягне за собою декілька суттєвих проблем, таких як: високий попит на ресурси (з точки зору трафіку, часу обробки та споживання енергії), довга затримка на підтвердження транзакцій та низька масштабованість [12].

4. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Вище викладені результати нашого дослідження окреслили проблему забезпечення інформаційної безпеки розумного будинку. Внаслідок аналізу наукових джерел вдалося узагальнити спектр уразливостей та здійснити порівняльну характеристику методів та технологій захисту інформаційної системи розумний будинок. Є очевидним, що дана спроба не вичерпує всіх можливих експериментальних наробок та математичних моделей забезпечення безпеки розумного будинку.

Як відомо, існуючі рішення безпеки не завжди підходять для IoT через великі витрати енергії та переробні витрати, тому надалі наші дослідження будуть спрямовані

на розробку алгоритму безпеки розумного будинку на базі технології Blockchain з урахуванням економії ресурсів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] 1.Баранов О.А. Інтернет речей (IoT): огляд правових проблем // Інтернет речей: проблеми правового регулювання та впровадження: Матеріали науково-практичної конференції. 24 жовтня 2017 р., м. Київ. / Упоряд. В. М. Фурашев, С. Ю. Петряєв. – К.: НТУУ «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка». 2017. http://ipp.kpi.ua/wp-content/uploads/2017/-_14.11.2017.pdf
[2] 2.Звіт Cisko із кібербезпеки за 2018 рік. URL: https://www.cisco.com/c/uk_ua/products/security/security-reports.html#~download-th.
[3] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini. Security, privacy and trust in internet of things: The road ahead, Computer Networks, vol. 76, pp. 146–164, 2015.
[4] Монастирський Л., Петришин О. Особливості збирання та опрацювання масивів даних для управління розумним об'єктом / Л. Монастирський, О. Петришин // Електроніка та інформаційні технології. – 2017. – Випуск 7. – С. 86–92
[5] Снегуров А. В. Риски информационной безопасности систем, построенных по технологии "Умный дом" / А. В. Снегуров, Е. А. Ткаченко, А. Д. Кравченко // Восточно-Европейский журнал передовых технологий. - 2011. - № 4(3). - С. 30-34. - Режим доступу: http://nbuv.gov.ua/UJRN/Vejpte_2011_4(3)__9.
[6] E. Fernandes, J. Jung, A. Prakash Security Analysis of Emerging Smart Home Applications. 2016 IEEE Symposium on Security and Privacy. http://iotsecurity.eecs.umich.edu/img/Fernandes_SmartThingsSP16.pdf
[7] V. Sivaraman, D. Chan, D. Earl, and R. Boreli, "Smart-phones attacking smart-homes," in Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks. ACM, 2016. http://www2.ee.unsw.edu.au/~vijay/pubs/conf/16wisec.pdf
[8] N. Zhang, S. Demetriou, X. Mi, W. Diao, K. Yuan, P. Zong, F. Qian, X. Wang, K.Chen, Y. Tian, C. A.Gunter, K. Zhang, P. Tague and Y. Lin. Understanding IoT Security Through the Data Crystal Ball: Where We Are Now and Where We Are Going to Be. 2017 https://arxiv.org/pdf/1703.09809.pdf
[9] A. Chakravorty, T. Wlodarczyk, and C. Rong, "Privacy preserving data analytics for smart homes," in Security and Privacy Workshops (SPW). IEEE, 2013, pp. 23–27. https://www.ieee-security.org/TC/SPW2013/papers/data/5017a023.pdf
[10] S. Notra, M. Siddiqi, H. H. Gharakheili, V. Sivaraman, and R. Boreli, "An experimental study of security and privacy risks with emerging household appliances," in Communications and Network Security (CNS), 2014 IEEE Conference on. IEEE, 2014
[11] http://www2.eet.unsw.edu.au/~vijay/pubs/conf/14M2Msec.pdf
[12] S. Nakamoto Peer-to-Peer Electronic Cash System. Bitcoin. Available at: https://bitcoin.org/bitcoin.pdf
[13] A. Dorri, R. Jurdak, S. S. Kanhere, and P. Gauravaram, "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home," in International Conference on Pervasive Computing and Communications Workshops, 2017, IEEE https://allquantor.at/blockchainbib/pdf/dorri2017blockchain.pdf
[14] S. Fan, L. Song, and C. Sang, "Research on Privacy Protection in IoT System Based on Blockchain," in International Conference on Smart Blockchain, SmartBlock 2018: Smart Blockchain https://easychair.org/publications/preprint_download/Vg7v

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (6), 2019
ISSN 2663 - 4023

Anastasia A. Belova
Master of Information Technology Faculty
State University of Telecommunications,
Python Software Engineer Remme, Kiev, Ukraine
ORCID: 0000-0001-7395-6079
anastasiabilova@gmail.com

Viktoria V. Onischenko
Doctor of Engineering, Professor,
Head of Software Engineering,
State University of Telecommunications, Kyiv, Ukraine
ORCID: 0000-0002-3126-2260
oviva@ukr.net

METHODS OF SAFETY DOMESTIC SECURITY

Abstract. This study focuses on the problem of Internet of Things (IoT) security, namely: an overview of threats to the information security of a smart home and the analysis of existing security methods for its devices. The Internet of Things is experiencing an exponential growth in research and industry. At the same time, security threats to information programs and databases are increasing. As it is known, the foundation of Internet of Things security consists of four parts: communication security, device security, device monitoring and network interaction control. The sources of threats and vulnerabilities of IoT information security are accordingly investigated. Conventional security and privacy approaches are generally not applicable to IoT, mainly because of its decentralized topology and limited resources of most of its devices. The analysis of scientific sources has allowed us to explore different approaches to secure a smart home: an architectural method with three modules to protect the confidentiality of smart home data analysis; network-level constraint method; Blockchain technology. It is determined that the proposed blockchain smart home platform enables the security of information, taking into account the basic security goals - confidentiality, integrity and accessibility. Blockchain can be used to track sensor data measurements and prevent duplication of any other malicious data, for authentication and secure data transmission. This research will help design and develop new methods and technologies for smart home security.

Keywords: Internet of Things (IoT); smart home; Blockchain; security.

REFERENCES

[1] Baranov OA Internet of Things (IoT): A Review of Legal Issues // Internet of Things: Problems of Legal Regulation and Implementation: Proceedings of a Scientific and Practical Conference. October 24, 2017, Kyiv. / Order. VM Furashev, S. Yu. Petryayev. - K .: NTUU "Igor Sikorsky Kyiv Polytechnic Institute" Publishing House "Polytechnic". 2017. http://ipp.kpi.ua/wp-content/uploads/2017/-_14.11.2017.pdf
[2] 2. Cisko Cybersecurity Report 2018. URL: https://www.cisco.com/c/en/products/security/security-reports.html#~download-th.
[3] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini. Security, privacy and trust in the Internet of Things: The Road ahead, Computer Networks, vol. 76, pp. 146-164, 2015.
[4] Monastyrsky, L., Petryshyn, O. Features of data collection and processing for smart object management / L. Monastyrsky, O., Petryshyn // Electronics and Information Technologies. - 2017. - Issue 7. - P. 86–92
[5] AV Snegurov, Information Security Risks of Intelligent House Systems / AV Snegurov, EA Tkachenko, AD Kravchenko // Eastern European Journal of Advanced Technologies. - 2011. - № 4 (3). - P. 30-34. - Access mode: http://nbuv.gov.ua/UJRN/Vejpte_2011_4(3)__9.
[6] E. Fernandes, J. Jung, A. Prakash Security Analysis of Emerging Smart Home Applications. 2016 IEEE Symposium on Security and Privacy. http://iotsecurity.eecs.umich.edu/img/Fernandes_SmartThingsSP16.pdf
[7] V. Sivaraman, D. Chan, D. Earl, and R. Boreli, “Smartphones attacking smart homes,” in Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks. ACM, 2016. http://www2.ee.unsw.edu.au/~vijay/pubs/conf/16wisec.pdf

[8] N. Zhang, S. Demetriou, X. Mi, W. Diao, K. Yuan, P. Zong, F. Qian, X. Wang, K. Chen, Y. Tian, CAGunter, K. Zhang, P. Tague and Y. Lin. Understanding IoT Security Through the Data Crystal Ball: Where We Are Now and Where We Are Going To Be. 2017 https://arxiv.org/pdf/1703.09809.pdf
[9] A. Chakravorty, T. Wlodarczyk, and C. Rong, "Privacy preserving data analytics for smart homes," in Security and Privacy Workshops (SPW). IEEE, 2013, pp. 23–27. https://www.ieee-security.org/TC/SPW2013/papers/data/5017a023.pdf
[10] S. Notra, M. Siddiqi, H. H. Gharakheili, V. Sivaraman, and R. Boreli, "An experimental study of security and privacy risks with emerging household appliances," in Communications and Network Security (CNS), 2014 IEEE Conference he. IEEE, 2014
[11] http://www2.eet.unsw.edu.au/~vijay/pubs/conf/14M2Msec.pdf
[12] S. Nakamoto Peer-to-Peer Electronic Cash System. Bitcoin. Available at: https://bitcoin.org/bitcoin.pdf
[13] A. Dorri, R. Jurdak, S.S. Kanhere, and P. Gauravaram, "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home," in International Conference on Pervasive Computing and Communications Workshops, 2017, IEEE https : //allquantor.at/blockchainbib/pdf/dorri2017blockchain.pdf
[14] S. Fan, L. Song, and C. Sang, "Research on Privacy Protection in an IoT Blockchain-Based System," in International Conference on Smart Blockchain, SmartBlock 2018: Smart Blockchain https://easychair.org/publications / preprint_download / Vg7v