Обеспечение Информационной Безопасности Киберфизических Систем

Расим Алгулиев[1], Ядигар Имамердиев[2], Людмила Сухостат[3]
[1,2,3]Институт Информационных Технологий НАНА, Баку, Азербайджан
[1]*rasim@science.az*, [2]*yadigar@lan.ab.az*, [3]*lsuhostat@hotmail.com*

***Аннотация*— В статье представлен обзор решений обеспечения безопасности киберфизических систем. Описывается принцип работы киберфизической системы. Рассматриваются основные типы атак на киберфизические системы. Приводятся направления будущих исследований.**

Ключевые слова— киберфизическая система; безопасность киберфизической системы; атаки на киберфизическую систему; защита персональных данных

I. Введение

Киберфизическая система (Cyber-Physical System, CPS) – это система, которая может эффективно интегрировать кибер- и физические компоненты, используя современные сенсорные, вычислительные и сетевые технологии [1, 2].

Новая вычислительная парадигма, известная как кибер-физико-социальные или физико-кибер-социальные вычисления [3], возникла из CPS и киберсоциальных систем (cyber-social systems, CSS). Кибер-физико-социальные системы (cyber-physical-social systems, CPSS) расширяют CPS и включают социальное пространство, и признаки участия и взаимодействия людей [4].

Повсеместное внедрение CPS связано с концепцией «Индустрия 4.0», которая формирует процесс объединения технологий и знаний, обеспечивая автономность, надежность, системность, контроль без участия человека.

Ключевые технологические тенденции, лежащие в основе CPS, включают: «Интернет вещей» (Internet of Things), Big Data, смарт-технологии, облачные вычисления и т.д.

CPS системы являются основой для развития следующих сфер: смарт-производство, смарт-медицина, смарт-здания и инфраструктуры, «умные» автомобили, мобильные системы, системы обороны и системы метеонаблюдения (Рис. 1).

Быстрый рост использования приложений CPS приводит к ряду проблем с безопасностью и конфиденциальностью.

В связи с широким применением беспроводных технологий для сбора и передачи данных и команд управления, где используется беспроводная сенсорная сеть (Wireless Sensor Network, WSN), растет необходимость в разработке систем защиты информации в промышленности. Удаленное расположение CPS устройств и их автономность приводят к риску вторжений и атак.

Работа с большими группами устройств может привести к тому, что некоторые из устройств будут скомпрометированы.

Рис. 1. Киберфизические системы.

Безопасность CPS поднимает целый ряд новых проблем. Проблемы по обеспечению безопасности CPS включают [5]:

- моделирование угроз безопасности;
- разработка формального подхода к оценке уязвимостей CPS;
- проектирование надежных и отказоустойчивых архитектур для обработки быстро развивающихся кибер- и физических угроз.

Таким образом, новые методологии и технологии должны быть разработаны для удовлетворения требований

DOI: 10.25045/NCSoftEng.2017.07

CPS с точки зрения безопасности, надежности и конфиденциальности персональных данных.

II. Принцип Работы Киберфизической Системы

Киберугрозы в CPS приводят к проблемам безопасности, вызванным интегрированием вычислительных процессов, связей и работой в сети (networking) при управлении физическими системами [1].

Компоненты CPS, включая сенсоры, актуаторы, распределенные центры управления и проводные и беспроводные сети связи, должны быть эффективно интегрированы для обеспечения эффективного мониторинга и управления физическими системами [6, 7].

Текущее состояние CPS можно описать путем захвата значений важных переменных процесса. Два вида важных процессов или переменных состояния в CPS включают: 1) измеренные переменные, представляющие данные, полученные с помощью сенсоров и 2) управляющие переменные, представляющие управляющие сигналы [8]. Нормальное значение некоторого параметра процесса, называется контрольной точкой (set point). В CPS расстояние между значениями переменных процесса и соответствующими контрольными точками рассчитывается контроллерами. После вычисления этого смещения, контроллеры, используя сложный набор уравнений, разрабатывают стратегию актуации, и вычисляют новые переменные актуации или управления. Полученное управляемое значение посылается к соответствующему актуатору, чтобы держать процесс ближе к определенной контрольной точке [9].

В общем, процесс работы CPS можно разделить на следующие этапы: 1) мониторинг; 2) работа в сети (networking); 3) вычислительная обработка; 4) приведение в действие (actuation).

III. Атаки на Киберфизические Системы

Киберфизические угрозы представляют собой угрозы, которые берут начало в киберпространстве, но оказывают влияние на физическое пространство системы. Одной из основных характеристик киберугроз является то, что они масштабируемы, т.е. они легко автоматизируются и тиражируются. Киберугрозы влияют на:

1) конфиденциальность, которая необходима для поддержания безопасности личных данных пользователей в CPS;

2) целостность, когда данные или ресурсы могут быть изменены без разрешения;

3) доступность, когда происходят сбои в вычислительной технике, управлении, коммуникации, оборудовании;

4) достоверность, когда необходимо подтвердить, что обе участвующие стороны есть действительно те, за кого они себя выдают [10, 11].

Классификации угроз CPS включает [12]:

- подмена личности (*Spoofing identity*);
- модификация данных (*Tampering with data*);
- отказ от авторства (*Repudiation of origin*);
- разглашение информации (*Information disclosure*);
- повышение привилегий (*Elevation of privilege*);
- отказ в обслуживании (*Denial of service, DoS*).

По вопросам безопасности атаки на CPS следующие (Рис. 2) [1]:

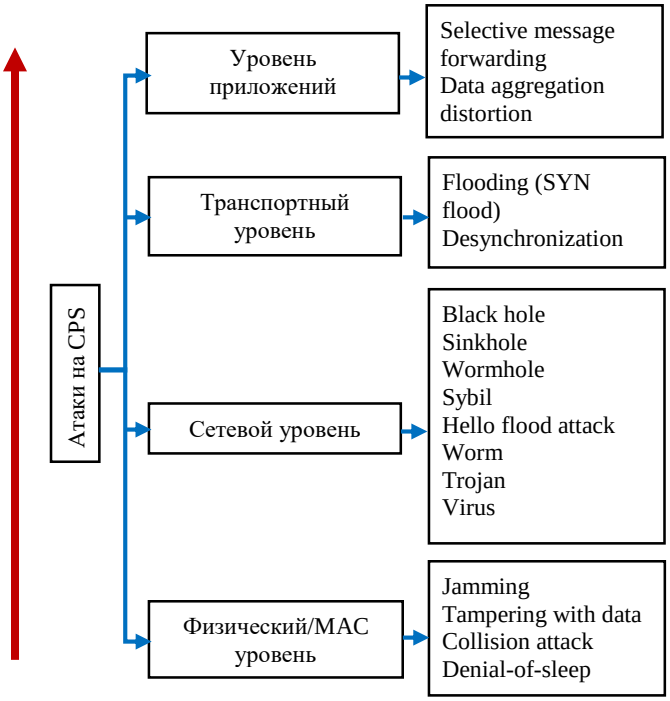

Рис. 2. Атаки на безопасность киберфизических систем.

IV. Технологии Обеспечения Безопасности Киберфизических Систем

Алгоритмы оценки и управления, используемые в CPS, разработаны для удовлетворения определенных оперативных целей, таких как стабильность замкнутого контура (closed-loop stability), защита (safety), живучесть или оптимизация функции производительности. Безопасность состоит в том, чтобы защитить эти цели от злоумышленников, атакующих киберинфраструктуру. Например, если измерения, собранные сенсорной сетью, содержат конфиденциальную информацию, необходимо обеспечить, чтобы только уполномоченные лица могли получить доступ к этим данным.

Подходы для обеспечения информационной безопасности CPS можно разделить на проактивные и реактивные механизмы.

A. *Проактивные механизмы*

Важным инструментом для обеспечения безопасности распределенных систем является аутентификация. Контроль доступа предотвращает несанкционированный доступ к системе: он не позволяет не прошедшим проверку

DOI: 10.25045/NCSoftEng.2017.07

подлинности получить доступ, в то же время, налагая надлежащие ограничения на деятельность аутентифицированных пользователей. Безопасная связь между двумя «подлинными» пользователями достигается с помощью кодов аутентификации сообщений или цифровых подписей (они могут обнаружить, что сообщения были подделаны третьей стороной). Время передачи сообщений также может быть гарантировано за счет использования временных меток (для которых требуются безопасные протоколы синхронизации времени) или механизмов реагирования. Кроме того, средства верификации и защита программного обеспечения могут проверять правильность архитектуры и реализацию системы, тем самым ограничивая количество уязвимостей. Безопасность CPS также зависит от безопасности сети сенсоров [13]. Большинство усилий по обеспечению безопасности сенсорных сетей включают следующие эффективные алгоритмы: 1) бутстрэппинг ассоциаций безопасности и управление ключами при загрузке [14, 15] для построения доверительной инфраструктуры, 2) защищенной связи [16, 17] и 3) протоколов безопасной маршрутизации [18,19]. Существуют несколько принципов проектирования безопасных систем управления [20, 21]: резервирование (*redundancy*), многообразие (*diversity*) и принцип разделения привилегий (*separation of privilege*).

B. Реактивные механизмы

Реактивные механизмы – это меры безопасности, предпринимаемые, когда атака уже происходит. Ложных тревог и пропущенных обнаружений невозможно избежать, поскольку обнаружение «злонамеренной» логики является неразрешимой проблемой [22].

Доступные решения безопасности не могут справиться с новыми сценариями атак, и необходимы проактивные меры для защиты встроенных узлов.

V. Обзор Исследований по Кибербезопасности

CPS завтрашнего дня должны намного превосходить сегодняшние системы по возможностям, адаптивности, отказоустойчивости, безопасности, защищенности и удобству использования.

В статье [23] представлен систематический обзор методов интеллектуального анализа данных (Data Mining, DM) с учетом знаний, техники и приложений, включая классификацию, кластеризацию, ассоциациативный анализ, анализ временных рядов и выбросов. Также рассматриваются некоторые новые случаи применения и новые алгоритмы. Обсуждаются проблемы и открытые исследовательские вопросы в этой области, и предлагается большая система DM.

Ряд исследований и обзорных статей посвящен технологиям обнаружения вторжений [24-27] или DM в конкретных приложениях [28, 29]. В [30] методы обнаружения аномалий категоризируются на статистические, на основе нейронных сетей, машинного обучения и гибридные подходы. Важные проблемы были выведены в области кибербезопасности для математических и статистических решений [31]. В [32] авторы категоризируют методы DM для обнаружения вредоносных программ на основе особенностей файлов и анализа (статического или динамического) и обнаружения типов. Структура DM с использованием систем обнаружения вторжений (Intrusion Detection Systems, IDS) была описана в [33].

[34] предлагает концепцию вычисления потока «больших» данных. По мнению авторов, следующим шагом в разработке вычислительных потоков данных должен стать переход от специализированных к более общим алгоритмам и приложениям.

Приблизительно 50 миллиардов устройств с поддержкой Интернета, которые будут развернуты к 2020 году, благодаря появлению IoT или Internet of Everything (IoE), поднимут множество вопросов относительно пригодности и адаптируемости современных компьютерных стандартов безопасности для обеспечения конфиденциальности и целостности данных [35].

В работе [35] представлен протокол, который объединяет доказательства с нулевым разглашением (zero-knowledge proofs) и механизмы обмена ключами для обеспечения безопасной и аутентифицированной связи в статических машинных сетях (Machine-to-machine, M2M). Этот подход применим для устройств с ограниченными вычислительными ресурсами, и может быть развернут в WSN сетях. Несмотря на то, что протокол требует априорных знаний о настройке сети и структуре, он гарантирует совершенную прямую секретность (perfect forward secrecy).

В [36] предлагается структура безопасности, совместимая со стандартными решениями безопасности на базе IP. В работе идентифицируются необходимые компоненты интероперабельной безопасной End-to-End (E2E) связи при участии криптографии с открытым ключом (Public-key Cryptography, PKC).

Авторы в [37] предлагают неявный механизм проверки подлинности на основе сертификатов для WSN в распределенных приложениях IoT. Разработанный двухфазный протокол аутентификации позволяет узлам сенсоров и конечным пользователям аутентифицировать друг друга и инициировать безопасные соединения. Предложенный протокол поддерживает дефицит ресурсов узлов сенсоров, неоднородность и масштабируемость сети. Анализ производительности и безопасности оправдывает возможность использования предложенного подхода в WSN с ограниченными ресурсами.

В [38] представлено приложение для обеспечения простого и эффективного способа доступа граждан к важной информации, такой как время прибытия автобуса, автобусные маршруты и туристические ориентиры с использованием смартфонов и технологии дополненной реальности (Augmented reality, AR). Предложенная инфраструктура IoT основана на шинных устройствах IoT, которые используют безопасный программный протокол CoAP для передачи данных на соответствующие облачные серверы. Обеспечивается безопасность всей системы,

DOI: 10.25045/NCSoftEng.2017.07

уделяя особое внимание упрощенному шифрованию, используемому в устройствах IoT с низким энергопотреблением.

VI. Защита персональных данных

Растущая популярность и развитие технологий DM создают серьезную угрозу безопасности конфиденциальной информации личности. Защита персональных данных может быть нарушена из-за несанкционированного доступа к персональным данным.

Конфиденциальность частных данных сохраняется одним из трех способов: без разглашения какой-либо информации, с раскрытием некоторой информации, с раскрытием измененной информации [39].

Вездесущее применение алгоритмов DM и машинного обучения позволяют злонамеренным пользователям использовать интеллектуальный анализ для получения частной информации. Эта проблема может быть решена с помощью двух аспектов: этического и технологического.

Легитимное использование личных данных было бы полезно исследователям, занимающимся DM, и частным владельцам. Различные страны разработали нормативные положения и законодательство для защиты владельцев данных и контроля над их распространением. Детально разработанное правило защиты частной жизни может запрещать злоупотребление конфиденциальной информацией и избегать нарушения прав человека. Хотя правила могут защищать частные данные от неправильного использования, технологические решения могут активно применять различные алгоритмы DM без ущерба конфиденциальности.

CPS системы окружают людей сенсорами, которые непрерывно собирают информацию о персональных данных, что представляет собой угрозу конфиденциальности.

Проактивные подходы предвидят и устраняют уязвимости в CPS, в то время как реактивные готовы быстро и эффективно защищаться от атак. Чтобы правильно функционировать, проактивные решения безопасности требуют проверки подлинности пользователя (например, пароль пользователя и биометрические данные), систему, способную избежать ошибок программирования и защиту информации (например, методы интеллектуального анализа данных неприкосновенности частной жизни (privacy-preserving data mining, PPDM)). Методы PPDM можно охарактеризовать распределением данных, модификацией данных, алгоритмами DM, правилами сокрытия (rule hiding) и методами сохранения конфиденциальности.

Методы сохранения конфиденциальности, наиболее важные методы селективной модификации данных, делятся на три группы: эвристические методы, методы криптографии, методы на основе реконструкции [40]. Они включают дерево решений, ассоциативные правила, байесовские сети, искусственные нейронные сети, кластеризацию, SVM классификацию и классификацию на основе к-ближайших соседей [41-44].

VII. Оценка Доверия в Киберфизической системе

Надежная CPS должна достигать высокого уровня доверия. Проблема доверительности (trustworthiness) к данным является основной проблемой для приложений CPS, отчасти из-за следующих сложностей [45]:

- *Огромный размер.* Типичная CPS включает сотни сенсоров, и каждый из них генерирует данные каждые несколько минут. Система управления должна обрабатывать огромный массив данных и оценивать аварийные сигналы с высокой эффективностью.

- *Зашумленные данные.* Многие опыты по внедрению показали, что ненадежные и зашумленные данные являются серьезными проблемами для CPS приложений. В [46] были перечислены трудности при получении точных данных CPS. Ошибки могут возникать при самых неожиданных обстоятельствах, и менее 49% данных могут быть использованы для осмысленной интерпретации [47].

- *Отсутствие обучающих наборов.* Многие традиционные методы обнаружения ложных тревог строятся на основе обучающих наборов данных [48]. Такие средства трудно получить в CPS, поскольку они дорогостоящи и подвержены ошибкам, чтобы вручную маркировать большой набор данных, генерируемый сенсорами.

- *Конфликты сенсоров.* Хорошо развернутая CPS имеет избыточную информацию, например, стандарт, называемый k-охватом (k-coverage), требует, чтобы каждый регион контролировался, по меньшей мере, k различными сенсорами [49]. Иногда один сенсор работает неправильно, тогда, как другие могут предоставить точную информацию. В таких случаях конфликты возникают между надежными и неисправными сенсорами. Поскольку пользователь не знает заранее, какой сенсор заслуживает доверия, система должна получить истину из противоречивых данных.

- *Неопределенность объектов.* Система должна интегрировать данные из нескольких сенсоров для оценки подробной информации об объекте. Из-за аппаратных ограничений сенсоры не могут предоставить подробную информацию об объектах вторжения. Большинство из них могут оценить только возможный регион объектов.

VIII. Заключение

CPS системы являются перспективной парадигмой для разработки текущих и будущих инженерных систем и, как ожидается, окажут важное влияние на реальный мир. Они несут высокий потенциал для создания новых рынков и решений социальных рисков, но налагают высокие требования качества, защиты, безопасности и неприкосновенность частной жизни [13-15,39]. Основополагающие научные исследования необходимы для достижения предсказуемого уровня качества проверки и измерения, эффективной борьбы с внешними и внутренними изменениями, поддержки необходимых

DOI: 10.25045/NCSoftEng.2017.07

переходов между механической, электрической и программной инженериями, а также интеграции аспектов управления, проектирования и применения.

В будущем планируются следующие исследования:

- Проведение анализа существующих методов защиты CPS систем, их уязвимостей и атак.
- Разработка архитектуры, защищенной CPS с встроенной системой обнаружения атак и вторжений.
- Получение набора метрик, по которым будет рассчитываться уровень доверия к компоненту CPS.
- Разработка алгоритма определения уровня доверия к компоненту CPS, для определения его подлинности.
- Разработка методов обеспечения защиты персональных данных.

Благодарности

Данная работа выполнена при финансовой поддержке Фонда Развития Науки при Президенте Азербайджанской Республики – **Грант № EİF-KETPL-2-2015-1(25)-56/05/1**.

Литература

[1] S. Zeadally, N. Jabeur, “Cyber-Physical System Design with Sensor Networking Technologies,” 2015, 416 p.

[2] S. H. H. N. Ghazani, J. J. Lotf, R. M. Alguliev, “A study on QoS models for mobile ad-hoc networks,” Int-l Journal of Modeling and Optimization, Vol. 2, No. 5, pp. 634-636, 2012.

[3] A. Sheth, P. Anantharam, C. Henson, “Physical-cyber-social computing: an early 21st century approach,” IEEE Intelligent Systems, Vol. 28, No. 1, pp. 78–82, 2013.

[4] J. Zeng, L. T. Yang, M. Lin, H. Ning, J. Ma, “A survey: Cyber-physical-social systems and their system-level design methodology,” Future Generation Computer Systems, August 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X1630228X

[5] C. H. Liu, Y. Zhang, “Cyber physical systems: architectures, protocols and applications,” 2016, 249 p.

[6] A. A. Cardenas, S. Amin, S. Sastry, “Secure control: towards survivable cyber-physical systems,” Proc. of WCPS, pp. 495–500, 2008.

[7] M. Pajic, A. Chernoguzov, R. Mangharam, “Robust architectures for embedded wireless network control and actuations,” Transactions on Embedded Computing System, Vol. 11, No. 4, p. 24, 2012.

[8] M. Krotofil, A. Cardenas, “Resilience of process control systems to cyberphysical attacks,” Proc. of the 18th Nordic Conference on Secure IT Systems, pp. 166–182, 2013.

[9] H. Kopetz, “Real-Time Systems: Design Principles for Distributed Embedded Applications,” 2011, 378 p.

[10] E. K. Wang, Y. Ye, X. Xu, S. M. Yiu, L. C. K. Hui, K. P. Chow, “Security Issues and Challenges for Cyber Physical System,” Proc. Of GREENCOM-CPSCOM, pp. 733–738, 2010.

[11] S. Sicari, A. Rizzardi, L. A. Grieco, A. Coen-Porisini, “Security, privacy and trust in Internet of Things: the road ahead,” Computer Networks, Vol. 76, pp. 146–164, 2015.

[12] D. Xu, M. Tu, M. Sanford, L. Thomas, D. Woodraska, W. Xu, “Automated security test generation with formal threat models,” IEEE Trans. on Dependable and Secure Computing, Vol. 9, No. 4, pp. 525–539, 2012.

[13] A. Perrig, J. A. Stankovic, D. Wagner, “Security in wireless sensor networks,” Commun. ACM, Vol. 47, No. 6, pp. 53–57, 2004.

[14] L. Eschenauer, V. Gligor, “A key-management scheme for distributed sensor networks,” Proc. of ACM CCS’02, pp. 41–47, 2002.

[15] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, D. E. Culler, “Spins: security protocols for sensor networks,” Wireless Networks, Vol. 8, No. 5, pp. 521–534, 2002.

[16] C. Karlof, N. Sastry, D.Wagner, “Tinysec: a link layer security architecture for wireless sensor networks,” Proc. of SenSys, pp. 162-175, 2004.

[17] M. Luk, G. Mezzour, A. Perrig, V. Gligor, “Minisec: A secure sensor network communication architecture,” Proc. of IPSN, pp. 479–488, 2007.

[18] C. Karlof, D. Wagner, “Secure routing in sensor networks: attacks and countermeasures,” Ad Hoc Networks, Vol. 1, No. 2–3, pp. 293-315, 2003.

[19] B. Parno, M. Luk, E. Gaustad, A. Perrig, “Secure sensor network routing: a clean-slate approach,” Proc. of CoNEXT, pp. 1-13, 2006.

[20] A. Avizienis, J.-C. Laprie, B. Randell, C. Landwehr, “Basic concepts and taxonomy of dependable and secure computing,” IEEE Trans. on Dependable and Secure Computing, Vol. 1, No. 1, pp. 11–32, 2004.

[21] J. H. Saltzer, M. D. Schroeder, “The protection of information in computer systems,” Proc. of the IEEE, Vol. 63, No. 9, pp. 1278–1308, 1975.

[22] L. Adleman, “An abstract theory of computer viruses,” Proc. of CRYPTO, pp. 354–374, 1990.

[23] F. Chen, P. Deng, J. Wan, D. Zhang, A. V. Vasilakos, X. Rong, “Data Mining for the Internet of Things: literature review and challenges,” International Journal of Distributed Sensor Networks, Vol. 2015, pp. 1-10, 2015.

[24] H. Debar, M. Dacier, A. Wespi, “Toward taxonomy of intrusion detection systems,” Computer Networks, Vol. 31, pp. 805–822, 1999.

[25] S. Axelsson, “Intrusion Detection Systems: A Survey and Taxonomy,” Technical report 99-15, Department of Computer Engineering, Chalmers University of Technology, Goteborg, Sweden, March 2000.

[26] “Homeland Security Council,” National Strategy for Homeland Security, p. 36, 2007.

[27] A. Patcha, J. M. Park, “An overview of anomaly detection techniques: Existing solutions and latest technological trends,” Computer Networks, Vol. 51, No. 12, pp. 3448–3470, 2007.

[28] S. J. Stolfo, W. Lee, P.K. Chan, W. Fan, E. Eskin, “Data mining-based intrusion detectors: an overview of the Columbia IDS project,” ACM SIGMOD Record, Vol. 30, No. 4, pp. 5–14, 2001.

[29] V. Chandola, E. Eilertson, L. Ertoz, G. Simon, anf V. Kumar, “Data mining for cyber security,” In: A. Singhal (ed.) Data Warehousing and Data Mining Techniques for Computer Security, pp. 83-103, 2006.

[30] V. J. Hodge, J. Austin, “A survey of outlier detection methodologies,” Artificial Intelligence Review, Vol. 22, No. 2, pp. 85–126, 2004.

[31] J. Meza, S. Campbell, D. Bailey. Mathematical and Statistical Opportunities in Cybersecurity, Paper LBNL-1667E, Lawrence Berkeley National Laboratory, pp. 1-11, 2009.

[32] M. Siddiqui, M. C. Wang, J. Lee, “A survey of data mining techniques for malware detection using file features,” Proc. of ACM-SE46, pp. 509-510, 2008.

[33] W. Lee, W. Fan, “Mining system audit data: Opportunities and challenges,” SIGMOD Record, Vol. 30, No. 4, pp. 33–44, 2001.

[34] A. Kos, S. Tomazic, J. Salom, N. Trifunovic, M. Valero, V. Milutinovic, "New Benchmarking Methodology and Programming Model for Big Data Processing," Hindawi International Journal of Distributed Sensor Networks, pp.1-7, 2015.

[35] P. Flood, M. Schukat, "Peer To Peer Authentication for Small Embedded Systems: A Zero-Knowledge-Based Approach to Security For The Internet Of Things," Proc. of the 10th International Conference on Digital Technologies, pp. 68-72, 2014.

[36] H. Shafagh, A. Hithnawi, "Poster Abstract: Security Comes First, a Public-key Cryptography Framework for the Internet of Things," Proc. of IEEE DCOSS, pp. 135-136, 2014.

[37] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, M. Ylianttila, "Two-Phase Authentication Protocol For Wireless Sensor Networks In Distributed IoT Applications," Proc. Of IEEE WCNC, pp.2728-2733, 2014.

[38] B. Pokric, S. Krcco, M. Pokric, "Augmented Reality Based Smart City Services Using Secure IoT Infrastructure," Proc. of WAINA, pp. 803-808, 2014.

DOI: 10.25045/NCSoftEng.2017.07

[39] C. C. Aggarwal, P. S. Yu, “Privacy-Preserving Data Mining: Models and Algorithms,” 2008, 514 p.

[40] V. S. Verykios, E. Bertino, I. N Fovino, L. P. Provenza, Y. Saygin, Y. Theodoridis, “State-of-the-art in privacy preserving data mining,” ACM SIGMOD Record, Vol. 33, No. 1, pp. 50–57, 2000.

[41] S. Chebrolu, A. Abraham, J. P. Thomas, “Feature deduction and ensemble design of intrusion detection systems,” Computers & Security, Vol. 24, pp. 1–13, 2005.

[42] R. Wright, Z. Yang, “Privacy-preserving Bayesian network structure computation on distributed heterogeneous data,” Proc. of ACM SIGKDD, pp. 713-718, 2004.

[43] M. Barni, C. Orlandi, A. Piva, “A privacy-preserving protocol for neural-network-based computation,” Proc. of MM&Sec, pp. 146–151, 2006.

[44] H. Yu, X. Jiang, J. Vaidya, “Privacy-preserving SVM using nonlinear kernels on horizontally partitioned data,” Proc. of ACM SAC’06, pp. 603-610, 2006.

[45] E. A. Lee, “Cyber physical systems: design challenges,” Proc. of IEEE ISORC, pp. 363-369, 2008..

[46] P. Buonadonna, D. Gay, J. Hellerstein, W. Hong, S. Madden, “Task: sensor network in a box,” Proc. of EWSN, pp. 133-144, 2005.

[47] G. Tolle, J. Polastre, R.Szewczyk, “A macroscope in the redwoods,” Proc. of SenSys, pp. 51-63, 2005.

[48] K. Ni, G. Pottie, “Bayesian selection of non-faulty sensors,” Proc. of ISIT, pp. 616-620, 2007.

[49] Z. Zhou, S. Das, H. Gupta, “Connected k-coverage problem in sensor networks,” IEEE/ACM Trans. on Networking, Vol. 14, No. 1, pp. 55-67, 2006.

DOI: 10.25045/NCSoftEng.2017.07