Digital Communications and Networks 4 (2018) 149–160

Contents lists available at ScienceDirect

Digital Communications and Networks

journal homepage: www.keaipublishing.com/en/journals/digital-communications-and-networks/

A blockchain future for internet of things security: a position paper

Mandrita Banerjee [a], Junghee Lee [a], Kim-Kwang Raymond Choo [b,a,*]

[a] Department of Electrical and Computer Engineering, University of Texas at San Antonio, San Antonio, TX 78249, USA
[b] Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249, USA

ARTICLE INFO

Keywords:
Blockchain
Blockchain security
Collaborative security
Internet-of-military things
IoT dataset
IoT self-healing
IoT security
Intrusion-prevention system
Predictive IoT security
Predictive security

ABSTRACT

Internet of Things (IoT) devices are increasingly being found in civilian and military contexts, ranging from smart cities and smart grids to Internet-of-Medical-Things, Internet-of-Vehicles, Internet-of-Military-Things, Internet-of-Battlefield-Things, etc. In this paper, we survey articles presenting IoT security solutions published in English since January 2016. We make a number of observations, including the lack of publicly available IoT datasets that can be used by the research and practitioner communities. Given the potentially sensitive nature of IoT datasets, there is a need to develop a standard for sharing IoT datasets among the research and practitioner communities and other relevant stakeholders. Thus, we posit the potential for blockchain technology in facilitating secure sharing of IoT datasets (e.g., using blockchain to ensure the integrity of shared datasets) and securing IoT systems, before presenting two conceptual blockchain-based approaches. We then conclude this paper with nine potential research questions.

1. Introduction

Technologies have changed the way we live, particularly in our data-driven society. This is partly due to advances in semiconductor and communication technologies, which allow a multitude of devices to be connected over a network, providing us with ways to connect and communicate between machines and people (e.g., machine-to-machine). Such a trend is also commonly referred to as the Internet-of-Everything, comprising the Internet-of-Things (IoT), Internet-of-Medical-Things (IoMT), Internet-of-Battlefield-Things (IoBT), Internet-of-Vehicles (IoV), and so on. Given the pervasiveness of such devices in our society (e.g., in smart cities, smart grids and smart healthcare systems), security and privacy are two of several key concerns. For instance, it was reported in 2014 that more than 750,000 consumer devices were compromised to distribute phishing and spam emails [40]. In data-sensitive applications such as IoMT and IoBT, ensuring the security of the data, systems and the devices, as well as the privacy of the data and data computations, is crucial. However, a threat to a system can be the result of a security measure that is not well thought out. For example, in a typical civilian or military hospital setting, the Information Technology (IT) team generally has the control of the entire network, including endpoint devices and IoMT devices (basically, any devices with an IP address). It is not realistic to expect the IT team to be familiar with every individual connected device, although they have the system administrator capability to install patches, and access the device and their data remotely, and so on.

What happens if in the middle of a surgical operation, one of the IoMT devices administering drugs shuts down and reboots itself after a patch is applied remotely by the IT system administrator? This is likely to result in chaos in operating theaters, as the surgical team will not have any idea what happened not to mention, the trauma and potential consequences to the patient (e.g., depriving the patient of oxygen could result in brain damage and fatality). In other words, things can go wrong very quickly during seemingly routine operations, such as applying patches and the devices rebooting themselves.

In this paper, we survey articles on security techniques that are either designed for, or are applicable to IoT, published in English since January 2016. We defer a survey of IoT privacy techniques as future work. The located articles are then sorted into reactive and proactive approaches, we further categorize the reactive approaches into (1) Intrusion Detection Systems (IDS) only and Intrusion Prevention Systems (IPS), and (2) collaborative security approaches.

2. Survey of existing IoT and related security approaches

2.1. Intrusion detection and prevention techniques

Modern-day malware designers and cyber attackers are innovative

* Corresponding author.
E-mail addresses: mandrita82@gmail.com (M. Banerjee), Junghee.Lee@utsa.edu (J. Lee), raymond.choo@fulbrightmail.org (K.-K.R. Choo).

https://doi.org/10.1016/j.dcan.2017.10.006
Received 11 September 2017; Received in revised form 10 October 2017; Accepted 30 October 2017
Available online 31 October 2017

and constantly seeking to circumvent existing measures (e.g., generating different versions of malware using mutation). Most existing IDS and IPS approaches are designed to detect unauthorized access attempts and Distributed Denial of Service (DDoS) attacks. For example, Alsunbul et al. [11] presented a network defense system for detecting and preventing unauthorized access attempts by dynamically generating a new protocol to replace the standard protocol. The aim is to confuse scanning attempts. The network path is also changed periodically to prevent unauthorized access and scanning of traffic. However, the number of packets generated can be excessive. In the approach of Zitta, Neruda and Vojtech [19], Raspberry Pi 3 is used to secure Ultra High-Frequency (UHF) Radio Frequency IDentification (RFID) readers running the Low-Level Reader Protocol (LLRP). Specifically, Fail2ban and Suricata were selected as the solution owing to their functionality and high scalability. Fail2ban supports complex architecture; thus, it is suitable for deployment in a cloud environment with multiple sensors and servers. Suricata provides better performance than Snort and allows multithread processing required for the multicore CPU of Raspberry Pi 3. Park and Ahn [50] analyzed and compared the detection and performance of Snort and Suricata when dealing with DoS attacks, and determined that Snort has lower CPU consumption. However, the multithreaded Suricata provides better single and multicore detection performance.

Next, we discuss recent intrusion detection and/or prevention systems. For simplicity, IDPS is used to refer to intrusion detection and/or prevention systems in the remainder of this paper.

2.1.1. Classification by approaches

Cryptography is a common approach used to provide data confidentiality and integrity, such as in the multilayered security approaches reported in Refs. [27,32]. Specifically, Chang and Ramachandran [27] proposed a multilayered security solution for cloud computing. The first security layer is firewall and access control, designed to ensure that only authorized and authenticated users can access the system and data. The second layer is identity management and intrusion prevention to identify users again and to remove any detected malicious files. The third layer is convergent encryption, which provides a top-down security policy. To evaluate the proposed approach, the authors conducted penetration testing on 10 PB data of data centers. Their findings indicated that the time to recover from an unauthorized access attempt is a minimum of 125 h. Makkaoui et al. [32] proposed a multilayered Cloud Security and Privacy Model (CSPM), which consists of five layers: a Physical and Environmental Security Layer (PESL), Cloud Infrastructure Security Layer (CISL), Network Security Layer (NSL), Data Layer (DL), and Access Control and Privilege Management Layer (ACPML).

Jin, Tomoishi and Matsuura [36] provided an enhanced method of Virtual Private Network (VPN) authentication using a Global Positioning System (GPS). The proposed method provides geo-privacy protection on mobile devices. Here, a VPN client sends a hash value of the GPS information instead of sending the raw value, protecting the geo-privacy of the client. Instead of providing only GPS coordinates, an area is provided for registering with an authentication server for each client. Google maps were used to check the hit rate of client GPS coordinates of the targeted area, and the authors' evaluation results reported accuracy rates of 99.29% and 92.96% for latitude and longitude, respectively.

Olagunju and Samu [4] designed an automated honeypot for real-time intrusion detection, prevention and correction by using a centralized logging system management technique (also known as puppet and virtual machines). The centralized system collects information from the source address, time and country of attackers. The approach reduces the manual effort required to dynamically modify the highly interactive honeypot system by using freely available and open-source technologies. The file transfer protocol is useful in attracting attackers that leave traces or evidence of usernames, passwords and source ports from various countries. However, the manual work needed to convert honeypots into a honeynet is significant. Agrawal and Tapaswi [48] proposed a honeypot-based multilayered IDS to detect and prevent rogue access point attacks. The approach combines the existing IDS and a honeypot to improve the accuracy of the existing IDS, and comprises filtering, intrusion detection and a honeypot. The system was implemented on a small wireless network. However, deploying the system on the cloud and adopting a machine learning technique can enhance the overall performance by maintaining a low false alarm rate and a low overhead of the honeypot.

Merlo, Migliardi and Spadacini [13] proposed an adaptive mechanism that considers full account prediction errors and residual traffic. This model was evaluated using a network simulator and delays were calculated. The results indicated that only a minimal delay is introduced, owing to the security analysis. However, this model lacks an ideal prediction algorithm; thus, it produces packet delay for false prediction.

Indre and Lemnaru [16] presented an IPS against cyber attacks and botnet malware. The authors proposed different learning algorithms by focusing on the feature selection and extraction stages, and their evaluations indicated 98% prediction scores. In addition, based on their evaluations using the DARPA benchmark dataset, they concluded that duplicated and redundant records affect real-time traffic with poor classification. A new training set was generated with a successful identification of an attack signature. The approach identified new attacks not present in the initial DARPA set. Keshri et al. [21] presented a Denial of Service (DoS) prevention technique using a firewall and IDS based on data mining techniques, which comprises data selection, data preprocessing, transformation, and model selection and evaluation. They used the NSL-KDD dataset, a refined version of the KDD99 cup dataset, for evaluation.

Sato et al. [43] suggested a Field Programmable Gate Arrays (FPGA) architecture for Application Specific Integrated Circuits (ASIC)–FPGA co-design to streamline the processing of IDPS and to improve the processing speed of the FPGA compared to that of the ASIC/CPU (Central Processing Unit). Here, FPGAs were designed using RTL (Register Transfer Logic) technology, and arithmetic circuits were configured in ASIC. To validate the result, adders in ASIC were developed in the FPGA with Complementary Metal-Oxide-Semiconductor (CMOS) technology.

A summary of recent IDS and IPS approaches is presented in Table 1.

2.1.2. Classification by network structure

Yevdokymenko [5] designed an adaptive method to detect and prevent active attacks in telecommunication systems. However, this approach is unable to detect new attacks (e.g., attacks using zero-day exploits). There is no foolproof solution, and it is impractical to eliminate all security threats in a network. In order to obtain information about network nodes and their priority based on their position in the attack graph, Abazari, Madani and Gharaee [49] proposed a model to calculate threats based on a weighted attack graph. Specifically, this is a dynamic proactive multipurpose threat response model designed to minimize threats and costs. Other optimization methods such as genetic algorithms could be implemented to respond optimally and quickly to threats in the future.

Different security systems have been proposed for different wireless networks such as Mobile Ad Hoc Networks (MANETs), Wi-fi, Local Area Networks (LANs), honeypots, and sensor networks. For example, Filipek and Hudec [12] proposed a security model for MANETs, based on the functionality of the distributed Public Key Infrastructure (PKI), firewall

Table 1
Summary of recent IDS and IPS, based on approaches.

Approach	References
Cryptography	Access control [27, 32] Geo-privacy protection [36]
Adaptive	[13,16,21]
Application Specific Integrated Circuits – Field Programmable Gate Arrays (ASIC-FPGA) joint design	[43]

and IPS. Here, every node contains the same security model, thus, providing efficient secure routing, data communications and monitoring of attacks. Routing and data information are signed and encrypted, and nodes can only access other nodes and services for which they are authorized. However, an IPS used in this system only controls the network conditions made by PKI and the firewall. Existing energy-aware IPSs allow for early detection and the discarding of malicious packets, resulting in additional delays for packet delivery. Filipek and Hudec [25] proposed a secure architecture for MANETs consisting of a secure RSA-based routing protocol, PKI, firewall and IPS. Routing packets are signed and negotiated symmetric keys with short validity are used to encrypt traffic. The IPS monitors traffic alerts the nodes of suspicious activities. Limitations of this approach include traffic restrictions due to the presence of firewall, and significant overheads due to the sending of messages by nodes, database lookups, control packets and encryption.

Yacchirena et al. [31] developed a Wi-Fi wireless network running on a Linux operating system, using Snort and Kismet as the IDS and IPS, respectively. Penetration tests were conducted with Backtrack 5 R3 using Fern Cracker and Ettercap to study the response of the IPS. Integrating the functionalities of Snort and Kismet, in theory, could enhance system performance by increasing the detection rate at the upper layers of Kismet and Wi-Fi wireless networks in Snort.

Dewanjee [18] proposed an Intrusion Filtration System (IFS), which provides strong security and the capability to terminate the execution and distributing of corrupted files. The system can be used offline and provides high throughput. In the approach, all files available in the system are checked, in the sense that the system log is scanned and information about all application and software installed in the system is stored in the IFS database. The regular updating of the database is designed to terminate the dissemination of corrupted files. However, there is no real-world implementation of IFS. Liu and Qiu [47] evaluated the utility of the 802.11w standard using extensive experimental data and a queuing model for preventing Rushing Attack Prevention (RAP)-based DoS attacks. In the work, a reliable STA-based queuing model was proposed to analyze the performance of 802.11w. In addition, to prevent DeauthF and DisassF attacks at low and high attacking rates, an integrated approach of 802.11w and traffic shaping (referred to as 802.11w-TS in the paper) was proposed.

Kalnoor and J. Agarkhed [8] proposed an IDS for wireless sensor networks using a pattern matching technique. Pattern matching defines a set of signatures to describe undesirable events, and when the pattern matches an event, a particular action is performed and defined by a set of signatures or rules. Then, the IDS analyzes the collected data and compares these data with a large signature set. A continuous mismatch between current and previous patterns will produce an alert. Waskita, Suhartanto and Handoko [45] studied the entropy method for an anomaly detection system, and evaluations were conducted at Intel Berkeley Research Laboratory using real data from distributed sensor networks. The evaluation was performed in two dimensional space by calculating the entropy from data series of temperature and humidity nodes. The findings suggested that unlike the elliptical method, the entropy method is able to detect the scattered anomalies regardless of the patterns.

Jokar and Leung [15] proposed a model that uses IDPS for ZigBee-based home area networks. This model employs a dynamic machine learning-based prevention technique with a low false positive rate, without the need to rely on prior knowledge about the attackers. In the model, a set of defensive actions (e.g., spoofing prevention, interference avoidance and dropping malicious packets) is defined to prevent attacks. The Q-learning method is used to determine the best strategy against an attack.

Sedjelmaci, Senouci and Messous [20] implemented a cyber security system based on IDS to protect an Unmanned Aerial Vehicle (UAV) against a cyber attack. It relies on a threat estimation model based on the Belief approach which aims to minimize false positive and false negative rates. Here, each UAV can activate an IDS monitoring agent to observe the behavior of its neighbors. If an IDS agent is suspected as a malicious node, then the particular node cannot operate as a monitoring node.

Different solutions for Software-Defined Networks (SDN) have been proposed. For example, Monshizadeh, Khatri and Kantola [33] proposed a multilayered IDS model with programmability features of an SDN application to detect and prevent unauthorized attacks, using programming SDN controlled switches. The proposed architecture has an SDN application, an SDN controller, a clustering algorithm, two switches and several detection nodes (referred to as Detection as a Service – DaaS). The architecture comprises three layers: an application layer, management layer and data layer. The application layer has an SDN application and an application interface. The management layer includes the SDN controller and switches, and the data layer has switches, a clustering algorithm and several DaaS nodes to detect unauthorized traffic. Two approaches were proposed: first, clustering is performed on individual packets of the mirrored traffic, and second, clustering is performed on sampled traffic. A combination of a load-balancing technique and clustering on sampled traffic is used to reduce computational cost and latency in the SDN controller. Machado, Granville and Schaeffer-Filho [37] proposed an architecture, ANSwer, with both Network Function Virtualization (NFV) and SDN features to create network resilience strategies. A key aspect of this approach is the feedback control loop for analyzing the behavior of the network infrastructure to identify a network anomaly. Ammar et al. [38] proposed a framework to enhance the security in an SDN-based data center. The authors suggested that the programmability features of SDN, along with the integration of the application and security layers, increase data center security by providing an adaptive layer. In the approach, advanced persistent threats are detected by searching for abnormal patterns and analyzing network traffic. A security agent is then used to collect and analyze security logs, as well as to block attackers.

McCune and Shay [41] proposed a real-time IPS for an automotive network, specifically, a Controller Area Network (CAN) bus. It includes Electronic Control Units (ECU), security on the base network, and external interfaces. Messages are categorized in three ways. Valid messages from the manufacturer are encoded into the various ECUs. Replayed messages are those captured from a CAN bus segment or that are already known. An invalid message with an arbitration identifier not associated with the ECU on the CAN bus segment will result in an alert.

A summary of recent IDS and IPS based on network structures is presented in Table 2.

2.1.3. Classification by applications

A number of studies have been dedicated to proposing various smart mobile devices, such as smart phones. For example, Vij and Jain [7] reviewed existing IDPS approaches for smart phones. They determined that a network-based IDPS can perform real-time emulation and facilitate the detection of malicious files before actual download, unlike a host-based IDPS. On the other hand, a host-based IDPS is cheaper and does not require as much (dedicated) hardware. Normally, a network-based IDPS is preferred over a host-based IDPS. Saracino et al. [10] designed a multilevel behavior-based anomaly detector for Android devices, designed to analyze and correlate several features at four different Android levels (i.e., kernel, application, user and package). The proposed

Table 2
Summary of recent IDS and IPS, based on network structure.

Network structure	References
Telecommunication networks	[5,49]
Mobile ad hoc networks (MANETs)	[12,25]
Wi-Fi	[31]
Local area networks (LAN)	[18,47]
Sensor networks	[8,45]
Smart grids	[15]
Aerial vehicle networks	[20]
Software-defined networks	[24,33,37,38]
Controller area networks	[41]

detector identifies and blocks suspected threats by detecting specific behavior patterns for a set of known security threats, and assesses the security risk by checking the requested permission and reputation meta-data, each time a new app is installed.

Rashid et al. [17] developed an intelligent IPS for homes equipped with a system-on-chip computer based on image processing and voice identification technology to differentiate between genuine guests and intruders. It will unlock the door for faces that are known and are authorized. For an unknown face as well as those that are unauthorized, it will make a voice call to the home owner using a smart phone application and connect to the visitor. The visitor can enter the home if the owner approves access. If the owner denies access to the visitor, then the owner also has the option to contact the police directly.

Cadet and Fokum [2] designed and implemented an IPS for the Voice over Internet Protocol (VoIP). Though efficient and simple, this system produces significant overhead owing to the use of Snort. Chenet al. [29] proposed an ASIC design and implementation for a VoIP IPS that comprises a hierarchical architecture of Statistical Anomaly-based Detection (SAD) and Stateful Protocol Anomaly Detection (SPAD) methodologies. While the detection accuracy and performance of SAD is not optimal, it can quickly differentiate between normal and abnormal traffic as a traffic filter. On the other hand, the throughput of SPAD is poor owing to its complex analysis algorithm. When SAD is used with SPAD to complement each other, IPS processing performance increases significantly. The profile analysis module is used to reduce SAD's false positive rate by updating SAD profile threshold.

Osop and Sahama [30] proposed three security control measures, namely preventive, detective and corrective measures, to ensure the security and privacy of Electronic Health Record (EHR) systems. Preventive control is meant to prevent an attack before it actually occurs, which can be achieved using password, paraphrase and different authentication measures. The detective control solution uses IDS/IPS for the detection of an attack. Corrective control (e.g., system back-up measures) is done after an attack to control the damage caused by attackers. By adopting different solutions for each measure, the EHR system can protect against various attacks.

Artificial Immune System (AIS) is an adaptive computational intelligence method that can be used to detect and prevent cyber attacks. Kumawat, Sharma and Kumawat [9] proposed a hybrid cloud-based model for intrusion detection and prevention to detect unidentified attacks. In their approach, Snort is used for intrusion detection and prevention and new signatures for current and unidentified attacks are forwarded to the behavior-based IDS, thus, minimizing subsequent false alarm rates. Farhaoui [23] developed an IPS based on an artificial immune system inspired by the Natural Immune System (NIS). It uses two theories of immune response: the theory of clonal selection and the theory of negative selection. The former is appropriate for a network-based IDPS in a scenario analysis, and the latter is appropriate for a behavioral analysis in a host-based IDPS. In this work, a hybrid IDPS is designed hierarchically and distributed across multiple machines, which requires the analysis of data from different sources. Al-Douri, Pangracious and Al-Doori [44] proposed a Two-Level Artificial Immune System (TLAIS) that distinguishes between normal access and attack records (antigen) by generating decision antibodies (rules). A genetic algorithm is used to define the first level and a decision tree classifier is used to define the second level. Access records are classified as normal, antigen or unknown. An unknown access record in level 1 is passed to level 2 to decide whether it is normal or antigen. If it is again classified as unknown, then the record will be considered as antigen.

Qinglin and Xiujuan [26] designed a Uniform Resource Locator (URL) filtering algorithm. The proposed algorithm combines hash table for indexing the host information and an AVL tree for storing URL path information. However, the URL compressing technique is not well structured owing to the large memory requirement during preprocessing. Prokhorenko et al. [28] proposed a real-time supervision framework for Hypertext Preprocessor (HPP)-based web applications, designed for an IPS. Protection is provided on the server side and does not require client-side assistance. The proposed architecture ensures the expected behavior of web application execution by the application author and enforces behavior determined by the protection administrator.

Su et al. [46] simulated attacks using TCP and evaluated the results using UDP to study different types of DDoS attacks on a firewall. They also proposed a visualization method to help determine whether an attack has occurred, and to identify abnormal packet combinations and traffic by modeling the behavior of the attacker.

Sedjelmaci, Senouci and Messous [52] implemented a cyber security system based on IDS to protect an Unmanned Aerial Vehicle (UAV) against cyber attacks. It relies on a threat estimation model based on the Belief approach, aiming to reduce false positive and false negative rates. Here, each UAV can activate an IDS monitoring agent to observe the behavior of its neighbors. If an IDS agent is suspected as a malicious node, then it cannot operate as the monitoring node.

Mirza, Mohi-Ud-Din and Awan [1] proposed a cloud-based energy efficient security system with two main modules: a cloud engine and a local agent. The cloud-based detection engine is used for anomaly detection, comprising 15 antivirus engines, a malware analysis module, and a cyber threat intelligence data collection module. The local agent is a lightweight host agent that is used to detect suspicious files by leveraging the cloud engine. The results of the authors' evaluation against 10,000 malware samples reported a detection rate of 98%, while using a maximum of 6% CPU power. However, the open source static analysis tool in the cloud engine is only designed to run on Microsoft Windows, and not on other operating systems. Moreover, the host agent cannot detect malicious files on the system until it appears in the process log after execution, making the system more attack prone. Sharma, Dhote and Potey [3] proposed an on-demand portable intrusion management Security-as-a-Service (lM-SecaaS) framework. This cloud-based system provides intrusion detection, prevention and response, and reporting and logging capabilities. It detects attack attempts by monitoring web traffic. Incoming streams are verified and filtered if necessary before reaching the organization. A proof-of-concept was implemented in a public cloud, and the authors' evaluations indicated that the overall overhead is dependent on traffic in the public cloud. In addition to being inefficient, the system is at risk of a single point of failure.

Chen et al. [14] proposed a cloudlet-based healthcare system by utilizing the functions of cloudlets, such as privacy protection, data sharing and intrusion detection and prevention. The NTRU (Number Theory Research Unit) method is used for data protection during data transmission. A trust model is designed to decide the trust level and whether data should be shared. Then, data stored in remote clouds are categorized into three parts and encrypted in different ways to maximize the transmission efficiency. In another independent research, a collaborative IDS was proposed by Shaghaghi, Kaafar and Jha [24]. Specifically, the authors designed WedgeTail, a controller-diagnostic IPS, to secure a Software-Defined Network (SDN) data plane. Malicious forward devices and their exact behavior can be automatically detected by analyzing the actual and expected trajectories of a packet. However, accuracy under different attack scenarios and use cases needs further investigation. The stability of snapshots used in the system analysis is also challenging. WedgeTail is not currently compatible with a distributed SDN controller.

Osanaiye, Choo and Dlodlo [34] studied DDoS (Distributed Denial of Service) attacks in the cloud, and presented two taxonomies, one for cloud DDoS attacks and one for cloud DDoS defense. Their review suggested that anomaly-based detection and access point deployments are suitable DDoS mitigation strategies. Furthermore, they presented a conceptual framework for the change point detection of a packet that is dependent on packet Inter-Arrival Time (IAT). Swapna et al. [35] proposed a cloud model, where fuzzy logic is integrated with the firewall in a hybrid cloud. The authors then evaluated the performance of the fuzzified firewall model on a simulated hybrid cloud using a heavy load database and a web server application. Their evaluations suggested that a

fuzzified firewall results in a slightly reduced (i.e., 10%) response time than that of a conventional firewall.

Salek and Madani [42] proposed an IPS based on a Virtual Machine Monitor (VMM) in cloud computing. The authors attempted to improve packet drop and resource usage without affecting efficiency. This approach allows dynamic configuration, based on the risk level of users, where a user's risk level is inversely proportional to the trust level of each user. Users are divided into three groups: high risk, medium risk and low risk. The IDS is categorized in the same way, as a High-risk IDS (HIDS), Medium-risk IDS (MIDS) or Low-risk IDS (LIDS). After identifying the risk level, a pre-configured IDS agent is allocated to each user's VM. However, the present architecture does not support dynamic configuration of IDS based on dynamic security levels.

A summary of recent IDS and IPS based on applications is presented in Table 3.

2.1.4. Summary

It is clear that IDPS is an active area of research. In addition to those discussed in Sections 2.1.1 to 2.1.3, there have been several other research efforts on the topic. For example, Ford et al. [6] developed an adaptive enterprise IDPS. A free open-source break-in prevention software, Fail2ban, is used to create the data collection agent. Here, all software agents, interconnected to the central behavior analysis database service, collect and record attack meta-information during prior attack attempts. The agents use both real-time and previous data by applying integrating rules from the information analysis method into the intrusion prevention policies. However, this proposed system has a high false-positive rate. Gharib et al. [22] proposed an evaluation framework for IDS and IPS datasets based on various characteristics, such as attack diversity, anonymity, available protocols, complete capture, complete interaction, complete network configuration, complete traffic, feature set, heterogeneity, labeled dataset, and metadata. A flexibility coefficient W is defined, and this is the weight of each feature defined based on the type of IDS/IPS selected for evaluation. KDD99 and KYOTO were used to evaluate the framework. Patel, Patel and Kleopa [39] proposed a framework where network administrator can examine network traffic in more details than in a conventional firewall. The approach also allows the collection of information on bandwidth consumptions for each network application, based on which unwanted applications are blocked. Administrators can create application detectors, which are written in the Lua programming language. These detectors can be interfaced with Snort.

2.2. Collaborative security techniques

Security cannot work in isolation, and in recent times there has been an interest in a collaborative security paradigm owing to its potential in detecting and preventing a wider range of attacks. In this subsection, we discuss recent literature on collaborative security approaches.

A number of multiparty access control mechanisms have been proposed in the literature. For example, Zhang, Patwa and Sandhu [86] proposed an access control mechanism for customers on the Amazon Web Services (AWS) platform, which facilitates secure information sharing. Specifically, it allows organizations to collaborate and communicate by exchanging their security data with other organizations during a cyber attack period.

Table 3
Summary of recent IDS and IPS, based on applications.

Application	References
Smart phones and Android security	[7,10,17]
Voice over Internet Protocol (VoIP)	[2,29]
Electronic health records	[30]
Artificial immune system	[9,23,44]
Web server	[26,28]
Firewall	[46]
Unmanned aerial vehicles	[52]
Cloud	[1,3,14,27,32,34,35,42]

Indumathi and Sakthivel [59] proposed an IDS for MANETs, which uses a digital signature scheme to eliminate receiver collisions and limited transmission power to minimize the false alarm rate.

Different collaborative security approaches for privacy preserving have also been proposed in the literature. For example, Freudiger et al. [64] presented privacy-preserving protocols for measuring data quality matrices of completeness, validity, uniqueness, consistency and timeliness using the homomorphic encryption technique. Here, a client only discovers the value of a quality metric for a semi-honest party. Data quality assessment ensures that the poor quality data will be rejected; this reduces the overhead required in cleaning the data on high-fidelity platforms. Vasilomanolakis et al. [85] proposed a locality-aware collaborative IDS, which distributes alerts to monitoring sensors. By exchanging compact alert data, the proposed system is capable of handling locality and privacy preserving communication. The authors also introduced a privacy-preserving data dissemination mechanism based on a bloom filter. Freudiger, Cristofaro and Brito [90] proposed a controlled data sharing approach on collaborative predictive blacklisting for collaborative threat mitigation. Cryptographic tools were used to decide how to share the dataset in a privacy-preserving way. Different sharing strategies were evaluated using real-world datasets.

Hiran, Carlsson and Shahmehri [63] proposed a distributed framework for the collaborative Border Gateway Protocol (BGP) monitoring and protection against prefix/sub-prefix and edge-based attacks. This is an application layer service that controls the sharing of network activity observed by routers and network monitors. Overheads, alert rates and scalability are calculated from a public wide-area BGP announcement, simulation results and traces.

Sharma, Bhuriya and Singh [84] proposed a hybrid encryption technique using RSA and a digital signature algorithm to achieve high throughput and security and reduced overheads in MANETs. The performance of the proposed technique using the Secure Ad hoc On-Demand Distance Vector (SAODV) routing protocol is evaluated using the NS-2 network simulator tool.

The game theory approach has also been utilized for collaborative IDS. Narang, Mehta and Hota [66] discussed a randomized, non-deterministic and game theory approach for intrusion detection in collaborative peer-to-peer networks to reduce the chance of a successful attack. Here, target nodes are selected arbitrarily and there is no comprehensive way of choosing the target nodes in this approach. In addition, this approach focuses on a single IDS at any point in time. As this approach is based on taking snapshots of network topologies, the network topologies must remain constant. Moreover, it is assumed that players are always rational. However, attackers and defenders do not behave rationally in each scenario. Ghorbani, Ghorbani and Hashemi [70] discussed a collaborative IDS framework to show the interactions between attackers and the IDS by modeling a multiplayer nonzero-sum stochastic game. The expected behavior of attackers as well as defenders and the optimal configuration of each IDS are described using the solution of a stationary Nash equilibrium. Wu et al. [71] described a security situational awareness mechanism based on the analysis of big data for smart grids. Security situational analyses use the fuzzy cluster-based association method, game theory and reinforcement learning. The proposed mechanism helps to extract the network security situation factors and to determine security situational prediction in smart grids.

The collaborative security approach of Bennaceur et al. [60] combines adaptive security and collaborative adaptation. Here, adaptive security helps to identify the security controls needed for security requirements irrespective of changes in the environment, whereas collaborative adaptation focuses on the mechanisms required for making multiple components collaborative. A collaborative robotic implementation was also presented.

Christoforidis and Vlachos [58] presented a collaborative lightweight client application that employs collaborative intelligence to prevent

against online attacks. Similarly, Wilson, Brown and Biddle [61] proposed a collaborative Analysis of Competing Hypotheses (ACH) system enabled by a walkthrough process. This work highlights the potential of surface technologies in collaborative intelligence analysis. The system aims to look up an ACH analysis using face-to-face discussions about different aspects of the analysis, such as completeness and correctness. The model also uses visualization techniques; thus, enabling collaboration and reflection. Kim, Woo and Kim [73] proposed a general framework for the efficient correlation analysis of cyber threat incidents using cyber threat intelligence. Here, an Event Relation Tree (ERT) is used to represent related events, and an Event Transition Graph (ETG) is used to describe the temporal transition of an event's characteristic. The proposed approach can infer an attacker's intention by tracing the transition of related cyber incidents.

2.2.1. Classification by network structures

Arya, Singh and Singh [83] studied worm hole attacks and collaborative black hole attacks in MANETs, and how to detect these attacks using trusted Ad-hoc On Demand Distance Vector (AODV) routing algorithms. Trust values are calculated for these two attack scenarios using various parameters (i.e., energy, throughput and packet delivery ratio). Evaluation was undertaken using NS-2 simulations.

Sonchack and Aviv [62] proposed LESS, a host-agent based simulator for large-scale evaluation of security systems. This is a stochastic host-based methodology, where host agents generate background traffic from real traces, and malicious traffic from parameters of user-defined threat models. Using these samples, it automatically builds and configures the behavior of the host agent and monitors their activities throughout simulation results to generate experimentation data sets.

Saied et al. [65] proposed collaborative schemes for three different networks: routing, security and radio in wireless Ad-Hoc communications. They also discussed two security solutions for handling internal attacks. These are a security-by-design mechanism and a trust-based mechanism. The latter is more flexible and efficient owing to its autonomous security procedures; however, it requires additional inputs and service aspects to design a clearer situation-based model.

Rathee and Saini [75] proposed a cache-based secure AODV routing protocol, which uses the last sequence number of the packet, in order to mitigate grey hole and black hole attacks in a wireless mesh network. Using this approach, network throughput could be increased significantly. However, the number of computations and the storage overhead required are significant.

Pan et al. [76] designed an SDN-based honeypot-type grid to enable different parties to collaborate dynamically and to decouple gateways and honeypots. They also proposed a software-defined marketplace, HogMap, where different parties would publish and subscribe to cyber threat intelligence services flexibly.

Li et al. [67] proposed a distributed host-based collaborative detection to mitigate False Data Injection (FDI) attacks in a smart grid cyber-physical system. A rule-based real-time majority voting algorithm was proposed to detect anomalies in a compromised Phasor Measurement Units (PMU). To evaluate the overall running status of PMUs, a new reputation system was designed that follows the adaptive reputation updating algorithm. The approach was evaluated using real-time measurement data from the PowerWorld simulator.

Liu and Bi [82] proposed a distributed collaboration system for inter-AS (Autonomous Systems) spoofing defense. This system facilitates efficient and flexible collaboration in spoofing defense in a distributed manner. Evaluation results from real datasets demonstrated that it has a low false positive rate, increasing deployment incentives, modest resource consumption and high security level. Here, a distributed control plane and a backward compatible with incrementally deployable data plane were designed for IPv4 and IPv6.

2.2.2. Classification by applications

Ganesh and RamaPrasad [57] proposed a multiparty access control model along with multiparty policy specification and evaluation system for online social networks. A polling system is also proposed for achieving efficient and flexible multiparty conflict resolution. Different security issues have been studied in three different situations: sharing of user profiles, relationship sharing and content sharing in an OSN. They discussed a prototype proof-of-concept implementation of the approach called DController. Bouchami et al. [81] proposed an enhancement to existing access control mechanisms with security risk approaches on Professional Social Networks (PSN). Risk for an incoming request is defined using three values, i.e., the impact, the threat and the vulnerability. An organization can refuse an access request by defining a risk threshold value.

Karantjias, Polemi and Papastergiou [55] proposed a collaborative security management system for critical infrastructure, which is integrated with a risk management technique based on modeling and group decision-making capabilities. This approach uses the collective knowledge of each user, and analyzes physical and cyber threats, attack modes and geographical areas. Koelle, Markarian and Kolev [56] described collaborative security management as a situation management capability, where the security function is designed based on networks of GAMMA (Global ATM Security Management) nodes. A decision-making loop is formed by collecting these conceptualized nodes, providing an existing security situation. Kolevet et al. [80] discussed a collaborative security situation management capability for air transportation and navigation. The approach uses dynamic identification and assessment of security threats, and the coordination of security measures. A threat prediction capability model was also developed to formulate situation management problems. This approach is designed to provide security capabilities in future air traffic management frameworks, such as SESAR and NextGen. Papastergiou, Polemi and Karantjias [89] proposed a collaborative cyber-physical security management system for critical information infrastructures. The risk assessment module provides various automated and customized self-risk assessment methodologies that are implemented using open-source visualization tools.

Sallabi and Shuaib [69] proposed a network management system architecture to manage IoT for smart healthcare. A multilayered Telecommunications Management Network (TMN) model was defined for managing different components of the healthcare system. The proposed management architecture consists of four layers: smart healthcare elements, smart healthcare context, resource management and service management. AlMotiri, Khan and AlGhamdi [72] described a mobile health system based on an Internet of Things (IoT) infrastructure to reduce healthcare costs and unnecessary hospitalization. The proposed system consists of smart sensors and communication devices to monitor blood pressure, sugar level, ECG, asthma, etc. These devices are wirelessly connected to IoT servers, and store, transmit and receive data. In other words, this is a multilayered architecture that consists of data collection, data storage, and data processing layers.

Chen et al. [51] presented a cloudlet-based healthcare system, designed for privacy protection, data sharing and intrusion detection. Specifically, Number Theory Research Unit (NTRU) is used to encrypt users' body data collected by wearable devices, prior to transmission to a cloudlet in the vicinity. Xie et al. [68] proposed a collaborative anomaly detection framework for modeling distributed network behavior, based on a hidden Markov random field. Different algorithms were generated for parameter estimation, forward prediction, backward smooth, and the normality evaluation of global and local behavior models. The proposed solutions were validated using real datasets for four kinds of network scenarios, i.e., regular network, scale-free network, random network, and small-world network. Boukhtouta et al. [74] presented a combined study to classify malicious packets at the network level, using a data mining technique. Collaborative IDSs have been proposed for a cloud environment. Mirza et al. [53], for example, proposed using a windows function hooking technique to mitigate Advanced Persistent Threats (APTs) or zero-day attacks. An open-source version of Security Information and Event Management (SIEM) is used to detect DoS attacks. The

collaborative IDS framework of Liang et al. [87] consists of three parts: an Intrusion Detection Region Control Manager (IDRCM), Intrusion Detection Region Controller (IDRC), and Intrusion Detection Agent (IDA). An alert exchange mechanism is introduced between IDAs in the same cloud region for sharing information about attacks. In another work, MacDermott, Shi, and Kifayat [88] proposed a framework to build a robust collaborative IDS to protect infrastructure services in a federated cloud environment.

In Ref. [91], the authors proposed category/cluster-based Android-Package (APK) analysis schemes for quantifying the risk of an APK. This was achieved using category and cluster information generated from online metadata. The performance of the cluster-based scheme is better, owing to its more accurate capturing of functional features. Cordero et al. [92] proposed a community-based distributed and collaborative IDS for learning models of normality to detect network anomalies. Communities of sensors were used to exchange network traffic to detect anomalies collaboratively. Stochastic algorithms were developed to group the sensors into different communities for observing samples of network traffic.

Júnior et al. [79] proposed a self-adaptive distributed firewall system architecture, based on the cooperation of different components in a network infrastructure. Here, a vulnerability assessment system is integrated with the proposed system for mitigating attacks from known vulnerabilities. Two units, analysis and decision engines, are used for this purpose.

Herold, Kinkelin and Carle [77] proposed a collaborative incident-handling system based on the blackboard pattern. It permits interleaving and collaborative interaction between the incident-handling steps that are further divided into exchangeable functional units distributed across the network. The main parts of the system are an information model for blackboard and an execution model for accessing information on the blackboard.

Wagner et al. [78] presented a malware information-sharing platform and threat-sharing project platform to collect and share the important Indicators of Compromise (IoC) attack targets. The aim of this project is to provide a platform where users from private and public organizations can share information and IoC on existing threats in a trusted environment.

Chen et al. [54] presented a collaborative network security prototype system with a centralized collaborative scheme for providing network security in multiple-tenant data center. It is integrated with a smart packet verdict scheme for packet inspection and to protect from possible network attacks inside the data center network.

A summary of recent collaborative security based on applications is presented in Table 4.

Table 4
Summary of recent collaborative security, based on applications.

Application	References
Online social network	[57,81]
Transportation	[55,56,80,89]
Smart healthcare	[69,72]
Intrusion	Detection [51,53,68,70,74,85,87,88,91,92] Mitigation [75,79], [89,90]
Incident handling	[77]
Cloud computing and IoT	[53,54,72,78]

2.3. Predictive security techniques

Predictive security is a relatively new research area, as evidenced by the very few review/survey articles. As the proverbial saying goes, prevention is better than cure, and in our context, this refers to detection and fixing. To ensure cyber resiliency in an intelligent and efficient IoT system, it is crucial to have the capability to predict future attacks in a network (in addition to detection and preventing existing attacks). This is the focus in this subsection.

Quantitative security metrics can be very useful to quantify the relative security of a system, given that a perfectly secure system does not exist in reality. It is known that there is a strong relationship between human errors and security breaches, and there have been a number of studies in this direction. For example, Noureddine et al. [93] designed a model based on general deterrence theory that is driven by the human decision-making process. To do so, the authors reviewed theories of human behavior in cyber security by studying fields within the social sciences and psychology and built predictive security models to study the effectiveness of password security and security audit requirement in a typical customer-based organization. Specifically, in this model, employees access the organization's computing resources to process personal and work emails using password-protected accounts. The organization performed frequent security checking for violations. A case study was used to illustrate the behavior of customer service representatives, and Stochastic Activity Networks (SAN) [94] were used to model the interaction between employees and the organization's security policy. The proposed approach has a number of challenges. First, designing a model from the attackers, employees and administrators' points of view at a different level of granularity is very challenging. Second, human behavior that follows descriptive theory rather than normative theory is difficult to capture using mathematical models. Finally, the uncertain behavior of the theory, validation and correct results are challenging to obtain. The authors also proposed an agent-based model that can be used as an alternative approach, where the system is designed as a group of autonomous agents capable of assessing their current situation and making their own decisions.

Abraham and Nair [95] worked on a predictive cyber security strategy, designed to protect critical infrastructures from external threats and to reduce the associated risk before they are compromised. They proposed a novel stochastic model for security evaluation based on attack graphs, which considers the temporal aspects of vulnerabilities. A non-homogeneous Markov model was defined using attack graphs, which incorporates time-dependent covariates (i.e., vulnerability age and vulnerability discovery rate) to predict future security states of the network to detect zero-day attacks. An open vulnerability scoring framework Common Vulnerability Scoring System (CVSS) [96–99] was used to bring together all complex exploitability characteristics (e.g., access vector, access complexity and authentication) to provide a powerful actionable insight. Different case studies were provided using attack graph generation and security and impact analyses to evaluate the concept. The approach is unique in the sense that it makes use of the CVSS framework by taking into account exploitability and impact, as well as expanding the model to include temporal aspects of vulnerabilities in an attack tree. One main challenge of this approach is the further enhancement of the decision-making capability of the architecture and the proposed model by anticipating potential security gaps in the future.

Mobile devices can be a device in an IoT infrastructure, and can be vulnerable to the same threats affecting other popular consumer technologies. Enforcing encryption for data protection is typically not viable for these low computing power devices owing to computational and energy requirements. Shi, Abhilash, and Hwang [100] proposed a hierarchically structured security model based on a trust chain between mobile devices, a cloudlet mesh and a remote cloud platform. The aim of this approach is to perform collaborative intrusion detection among multiple Wi-Fi-enabled cloudlets by accessing cloud services via Wi-Fi or mobile networks. Real-time filtering of malicious attacks was achieved via trusted remote clouds, where predictive security analytics were used for malware signature scanning and automated malware/spam removal. The remote clouds have the data-mining capability to provide Security-as-a-Service to all end users. The proposed approach was implemented on EC2 cloud with MapReduce, and evaluated on over 1 TB of Twitter data. A hybrid intrusion detection system could use a cloudlet mesh to detect malware and network anomalies, and data-coloring techniques [101] could be integrated with this model to protect and access a large database in the cloud.

By considering the nature of intrusion attacks and features of

traditional grey Verhulst model, Leau, Yu-Beng and Manickam [102] proposed an adaptive grey Verhulst prediction model to predict an incoming network security situation in a typical organization. In the proposed model, a combination of the Trapezoidal rule and Simpson's one-third rule was used to find the background value in the grey differential equation for predicting the future outcome. Both Mean Absolute Percentage Error (MAPE) and Root Mean Square Deviation (RMSD) were used to evaluate the efficiency of the proposed model. Their findings indicated that the new model achieved 93.3% in predictive accuracy, whereas the GM(1,1) and traditional grey Verhulst model had accuracies of 87.3% and 92.0%, respectively. The authors also designed a complementary model with a residual prediction algorithm to improve prediction accuracy.

3. Discussion

From Table 5, we observe that only a small number of studies had any evaluation attempted on the proposed approach, and the majority of the evaluations in other studies were software based.

As shown in Table 6, the KDD dataset appears to be one of the most widely used datasets in IDS/IPS/IDPS research evaluations, and the DARPA dataset appears to be used in both IDS/IPS/IDPS and collaborative security research evaluations. It also appears that despite the increasing trend in IoT security research, IoT datasets are limited in both breadth and depth, particularly for predictive security research.

The need for publicly available IoT datasets: The role of real-world datasets in the evaluation of any proposed security technique, particularly predictive security, cannot be overstated. The relatively small number of real-world datasets available is partly due to the amount of time and effort needed to collect and compile these datasets. The challenge is compounded by the diversity of IoT devices and architectures. In addition, in our review, we did not locate any publicly available real-world IoT dataset.

The need for secure sharing of public available IoT datasets: To maximize research efforts on IoT security, we reiterate the importance of sharing real-world datasets. To facilitate the sharing of real-world datasets, we recommend the development of a standard for such datasets, and use the blockchain technique to ensure integrity in the shared datasets. In addition, privacy should be preserved when datasets are released to the public.

Table 5
Snapshot of evaluation approaches used in existing studies.

Prototype	IDS/IPS/IDPS	Collaborative security	Predictive security
Software	[4,11,13,15,17,19], [24,25,29,31,35], [43,46,47,48,50,52]	[59,61,74,75,87]	[93]
Hardware	[2]	-	-
Software and hardware	[41]	-	-

We also highlight the importance of having a wide range of IoT datasets, representative of the existing heterogeneous IoT devices and systems. For example, one dataset may include data collected from multiple sources such as network traffic and the operation logs of different IoT devices in a specific industry or context (e.g., smart grids). Even within a single IoT system, we may have different types of IoT devices with different data formats and structures. Thus, we need to categorize the information sources and define the data format and structure, according to the specific industry or context.

In addition, it is likely that these real-world datasets would be large. Thus, having a centralized distribution or sharing paradigm will not scale well. Instead, we may employ a centralized hub that references the various distributed storage servers where datasets are actually stored and can be accessed or distributed. Datasets can then be accessed or shared by registering a storage server with the hub. When the framework is open to the public, the integrity of datasets should be maintained. Thus, blockchain could play a role in ensuring the integrity of datasets (see Section 4).

4. Blockchain for IoT

Blockchain was originally used for recording financial transactions, where transactions are encoded and kept by all participants (e.g., Bitcoins and other cryptocurrencies). Thus, all transactions are transparent and any modifications can be easily traced and detected. Blockchain can be applied to enhance IoT security. We will now present two examples of employing blockchain for IoT security.

Fig. 1 illustrates a typical blockchain process. A block is created when a transaction is made. The block is broadcasted to all nodes in the network. One of the nodes validates the block (called mining in bitcoin) and broadcasts it back to the network. The nodes add the block to their chain of blocks if the block is verified and the block correctly references the previous block.

4.1. Blockchain in dataset sharing

As previously discussed, when datasets are shared among the research and practitioner communities or more widely, their integrity should be maintained. In our context, to ensure integrity of the datasets, a Reference Integrity Metric (RIM) for the dataset is maintained using blockchain. Specifically, whenever a dataset is downloaded, its integrity can be checked using the RIM – see Fig. 2.

In our proposed approach, there is a central hub that only maintains references of member repositories where the datasets are actually stored and distributed. The membership information, such as the address, owner and sharing policy, is maintained by the blockchain. In other words, membership information is recorded and shared by all members including the hub. There is another chain of blocks that maintains the RIM of datasets. This blockchain is used to ensure the integrity of datasets.

When datasets are publicly available, privacy of datasets is a major concern. To preserve privacy and avoid the violation of any data privacy regulations, we emphasize the need for an automated tool that anonymizes datasets prior to the release of these datasets.

Table 6
Snapshot of datasets used in existing evaluations.

Datasets	IDS/IPS/IDPS	Collaborative security	Predictive security
Publicly available datasets (including available upon request)	KDD99 [22] KYOTO [22] Mobile apps [10] Cloud data center-10 PB [27] DARPA [16,42] NSL KDD [21,44] Intel Berkeley Research Laboratory [45]	Three public Routeviewsmonitors and three public traceroute servers [63] CAIDA [68] DARPA [71,92] VirusTotal [73] DShield [85,90]	Tweets [100] DARPA [102]
Non-publicly available datasets	URL pattern set [26] Network [37]	Mobile apps [91]	
Simulations	[1,9]	[51,62,67,77,81–84]	

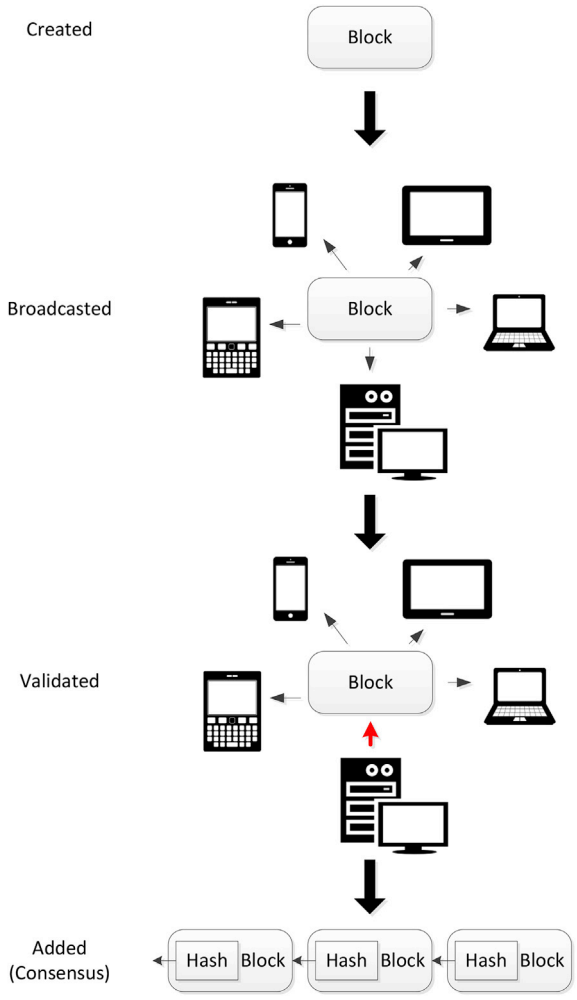

Fig. 1. A typical blockchain work flow (adapted from [104]).

Another challenge we need to consider is the lifetime of datasets. The owners of datasets may not want to share them permanently. However, once any transaction is recorded by the blockchain, it cannot be modified or erased. While this is a strong security property, it may not be conducive to sharing if any record needs to be removed. In the proposed dataset framework, only the RIM is maintained by the blockchain. Therefore, even if the RIM remains in the blockchain, datasets will no longer be available for sharing.

4.2. *Blockchain-based compromised firmware detection and self-healing*

No security technique is foolproof, and IoT devices and systems could be compromised despite the best (security) efforts. Thus, compromised devices need to be able to self-heal. We suggest using blockchain to facilitate self-healing for compromised devices.

Most existing firmware protection techniques are based on integrity checking. Starting from a bootloader, the integrity of the next level firmware (operating system and application) is checked before it is executed. The bootloader is stored in secure read-only storage, so that it cannot be modified under any circumstances. It is often called a root of trust. The bootloader checks the integrity of the operating system code while copying it from flash memory to working memory (e.g., DRAM). In a similar vein, the operating system checks the integrity of applications before it launches them. Integrity checking is typically performed by comparing the RIM. The RIM of the operating system and applications is pre-computed and stored in a safe place. Before executing the operating system and applications, their integrity metric is computed and

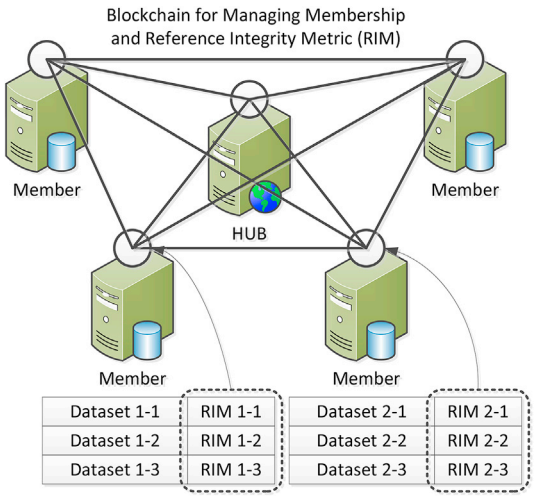

Fig. 2. Conceptual blockchain-based management of membership and Reference Integrity Metrics (RIM).

compared against the RIM. Only if both values are the same can the operating system and applications be executed. To ensure the reliability of the execution or activity, the integrity of the RIM itself is very important. If the firmware cannot be updated, then the RIM should be stored in read-only memory. However, for reasons such as security patches and upgrades of services, updates are usually allowed. When the firmware is updated, its corresponding RIM should also be updated. If an adversary manages to update the RIM for the compromised firmware, then existing integrity checking methods will be ineffective.

We propose using blockchain to protect the RIM, as illustrated in Fig. 3. The blockchain is a distributed database that keeps track of all transactions. Since all participating devices maintain the same records, unless an adversary manages to compromise the majority of devices, the integrity of the records will be assured.

Redundancy is typically used to heal corrupted software, where the same or similar code replaces the corrupted code. In the proposed approach, the compromised firmware is replaced by "known to be good" firmware. By using the blockchain, the history of firmware can be traced. Thus, when compromised firmware is detected, it will be forced to roll back to its previous version. Owing to tight resource constraints, not all devices can retain the previous version of the firmware. Thus, some devices in the network (e.g., intermediate nodes with a larger storage capability, such as in an edge computing environment) can be used to maintain a repository of previous versions of firmware for neighboring devices.

The firmware of embedded systems is often updated through a debugging interface (e.g., JTAG). Since IoT devices are always connected to a network, remote updates are also possible. When a firmware is updated remotely, authentication is crucial to prevent unauthorized modification. In the proposed approach, it is assumed that authentication is achieved using existing tools. The challenge of this task is to define the procedure for legitimate firmware updates through a debugging interface or a remote entity. Any firmware update should be handled by the hardware modules for self-healing and the blockchain. Once the updater is authenticated, the self-healing logic receives the new firmware through a debugging interface or a network. It updates the flash memory and computes the RIM. The RIM, metadata, and the new firmware are stored in the blockchain and the repository by the blockchain hardware.

5. A blockchain future?

IoT technology will play an increasingly important role in our society for the foreseeable future, in both civilian and military (adversarial) contexts, including the Internet of Drones, Internet of Battlefield Things

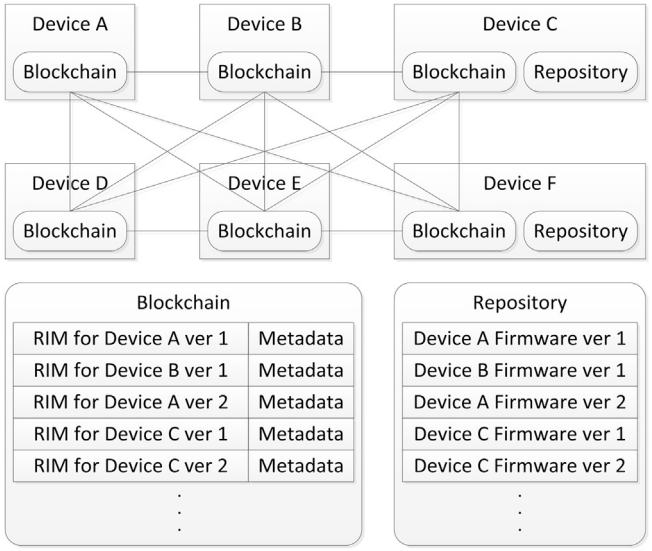

Fig. 3. Conceptual blockchain-based compromised firmware detection and self-healing approach.

and Internet of Military Things. Not surprisingly, IoT security is a topic of ongoing research interest.

In this paper, we reviewed security techniques designed for IoT and related systems published since 2016. While it is important for us to be able to detect and prevent existing threats, the capability to predict potential threats and attacks in the near future is also, if not, more important. Hence, we argue that there is a pressing need for more extensive research in predictive IoT security – *research topic 1*. For example, how can we reliably and effectively identify potential IoT threat vectors to inform the formulation of a potential mitigation strategy (e.g., formulate a probable course of action for each identified threat). Owing to the time-sensitive nature of certain IoT applications (e.g., in military or adversarial contexts), the identification of potential IoT threat vectors and the formulation of probable course(s) of action should be automated, with minimal human intervention.

We also observed the lack of publicly available IoT datasets and the absence of representative IoT datasets, both of which are important for IoT security research – *research topic 2*. Thus, we proposed the need for a standard to be established for IoT datasets that will facilitate the sharing of such datasets for research purposes. We also highlighted the potential of blockchain in sharing and distributing such datasets in a research network.

We then presented a conceptual blockchain-based compromised firmware detection and self-healing approach that can be deployed in an IoT environment.

Future research will include exploring how blockchain can be used as a collaborative security foundation to secure other IoT and related systems (e.g., cyber-physical systems) – *research topic 3*.

It has been observed in a recent white paper from Microsoft that the processing power required for public blockchain networks—and associated energy costs—are prohibitive to enterprise scenarios […]. Put another way, the Bitcoin network consumes enough energy to power more than 1.3 million U.S. households [103].

Therefore, one potential research agenda is to study the optimization of blockchains and blockchain-based platforms, such as the recently proposed open-source Coco Framework [103], which will reduce energy consumption while offering more effective and efficient services –*research topic 4*.

In addition to designing efficient and lightweight blockchain-based IoT security solutions (see *research topic 5* and *research topic 6*), we need to monitor the emerging threat landscape (see *research topic 7* to *research topic 9*).

- *Research topic 5*: How can attackers abuse (advanced) security features on IoT devices and anti-forensic techniques to evade investigation and forensic investigation attempts?
- *Research topic 6*: In the event that (advanced) security features on IoT devices and anti-forensic techniques have been used by attackers, how can investigators and incident responders gain access to secured communications stored on and transmitted from IoT devices (e.g., obtaining evidential data from encrypted communications where the investigators and incident responders do not have access to the decryption key)?
- *Research topic 7*: Some IoT devices may be located in publicly accessible areas, and in the event that an IoT device is physically under the control of an adversary, how can blockchain be used to guarantee the security and privacy of the data stored in the device?
- *Research topic 8*: How can blockchain be used to reduce the possibility of the hardware and software of an IoT device being compromised or tampered with if the device is physically accessible?
- *Research topic 9*: Under tight resource constraints, what is the most cost-effective way to implement sophisticated blockchain-based security solutions?

References

[1] Q.K.A. Mirza, G. Mohi-Ud-Din, I. Awan, A cloud-based energy efficient system for enhancing the detection and prevention of modern malware, in: 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), 2016, pp. 754–761. Crans-Montana.
[2] F. Cadet, D.T. Fokum, Coping with denial-of-service attacks on the IP telephony system, in: SoutheastCon 2016, 2016, pp. 1–7. Norfolk, VA.
[3] D.H. Sharma, C.A. Dhote, M.M. Potey, Implementing intrusion management as security-as-a-service from cloud, in: 2016 International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), 2016, pp. 363–366. Bangalore.
[4] Amos O. Olagunju, Farouk Samu, In search of effective honeypot and honeynet systems for real-time intrusion detection and prevention, in: Proceedings of the 5th Annual Conference on Research in Information Technology (RIIT '16), ACM, New York, NY, USA, 2016, pp. 41–46.
[5] M. Yevdokymenko, An adaptive algorithm for detecting and preventing attacks in telecommunication networks, in: 2016 Third International Scientific-practical Conference Problems of Infocommunications Science and Technology (PIC S&T), 2016, pp. 175–177. Kharkiv.
[6] M. Ford, et al., A process to transfer Fail2ban data to an adaptive enterprise intrusion detection and prevention system, in: SoutheastCon 2016, 2016, pp. 1–4. Norfolk, vol. A.
[7] S. Vij, A. Jain, Smartphone nabbing: analysis of intrusion detection and prevention systems, in: 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), 2016, pp. 2209–2214. New Delhi.
[8] G. Kalnoor, J. Agarkhed, Pattern matching intrusion detection technique for Wireless Sensor Networks, in: 2016 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-informatics (AEEICB), 2016, pp. 724–728. Chennai.
[9] S. Kumawat, A.K. Sharma, A. Kumawat, Intrusion detection and prevention system using K-learning classification in cloud, in: 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), 2016, pp. 815–820. New Delhi.
[10] A. Saracino; D. Sgandurra; G. Dini; F. Martinelli, "MADAM: effective and efficient behavior-based android malware detection and prevention," in IEEE Transactions on Dependable and Secure Computing ,vol.PP, no.vol. 99, pp.1–1.
[11] S. Alsunbul, P. Le, J. Tan, B. Srinivasan, A network defense system for detecting and preventing potential hacking attempts, in: 2016 International Conference on Information Networking (ICOIN), 2016, pp. 449–454. Kota Kinabalu.
[12] J. Filipek, L. Hudec, Securing mobile ad hoc networks using distributed firewall with PKI, in: 2016 IEEE 14th International Symposium on Applied Machine Intelligence and Informatics (SAMI), 2016, pp. 321–325. Herlany.
[13] A. Merlo, M. Migliardi, E. Spadacini, Balancing delays and energy consumption in IPS-enabled networks, in: 2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2016, pp. 267–272. Crans-Montana.
[14] M. Chen, Y. Qian, J. Chen, K. Hwang, S. Mao, L. Hu, Privacy protection and intrusion avoidance for cloudlet-based medical data sharing, in: IEEE Transactions on Cloud Computing, 2007. In press.
[15] P. Jokar, V. Leung, Intrusion detection and prevention for ZigBee-based home area networks in smart grids, in: IEEE Transactions on Smart Grid, 2017. In press.
[16] I. Indre, C. Lemnaru, Detection and prevention system against cyber attacks and botnet malware for information systems and Internet of Things, in: 2016 IEEE 12th International Conference on Intelligent Computer Communication and Processing (ICCP), 2016, pp. 175–182. Cluj-Napoca.
[17] M.T. Rashid, I.K. Abir, N.S. Shourove, R. Muntaha, M.K. Rhaman, Intelligent intrusion prevention system for households based on system-on-chip computer, in:

2016 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), 2016, pp. 1–5. Vancouver, BC.
[18] R. Dewanjee, Intrusion Filtration System(IFS)-mapping network security in new way, in: 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), 2016, pp. 527–531. Paralakhemundi.
[19] T. Zitta, M. Neruda, L. Vojtech, The security of RFID readers with IDS/IPS solution using Raspberry Pi, in: 2017 18th International Carpathian Control Conference (ICCC), 2017, pp. 316–320. Sinaia.
[20] H. Sedjelmaci, S.M. Senouci, M.A. Messous, How to detect cyber-attacks in unmanned aerial vehicles network?, in: 2016 IEEE Global Communications Conference (GLOBECOM), 2016, pp. 1–6. Washington, DC.
[21] A. Keshri, S. Singh, M. Agarwal, S.K. Nandiy, DoS attacks prevention using IDS and data mining, in: 2016 International Conference on Accessibility to Digital World (ICADW), 2016, pp. 87–92. Guwahati.
[22] A. Gharib, I. Sharafaldin, A.H. Lashkari, A.A. Ghorbani, An evaluation framework for intrusion detection dataset, in: 2016 International Conference on Information Science and Security (ICISS), 2016, pp. 1–6. Pattaya.
[23] Yousef Farhaoui, Design and implementation of an intrusion prevention system, Int. J. Netw. Secur. 19 (No.5) (2017) 675–683.
[24] Arash Shaghaghi, Mohamed Ali Kaafar, Sanjay Jha, WedgeTail: an intrusion prevention system for the data plane of software defined networks, in: Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS '17), ACM, New York, NY, USA, 2017, pp. 849–861.
[25] Jozef Filipek and Ladislav Hudec, "Advances in distributed security for mobile ad hoc networks," In Proceedings of the 17th International Conference on Computer Systems and Technologies 2016 (CompSysTech '16), Boris Rachev and Angel Smrikarov (Eds.). ACM, New York, NY, USA, 89–96.
[26] He Qinglin, Ma Xiujuan, A large-scale URL filtering algorithm in high-speed flow, in: 2016 2nd IEEE International Conference on Computer and Communications (ICCC), 2016, pp. 1043–1046. Chengdu.
[27] V. Chang, M. Ramachandran, Towards achieving data security with the cloud computing adoption framework, IEEE Trans. Serv. Comput. 9 (1) (Jan.-Feb. 1 2016) 138–151.
[28] V. Prokhorenko, K.K.R. Choo, H. Ashman, Intent-based extensible real-time PHP supervision framework, IEEE Trans. Inf. Forensics Secur. 11 (10) (Oct. 2016) 2215–2226.
[29] M.J. Chen, C.C. Wen, H.C. Lin, Y.S. Chu, ASIC design and implementation for VoIP intrusion prevention system, in: 2016 International Conference on Applied System Innovation (ICASI), 2016, pp. 1–4. Okinawa.
[30] H. Osop, T. Sahama, Quality evidence, quality decisions: ways to improve security and privacy of EHR systems, in: 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), 2016, pp. 1–6. Munich.
[31] A. Yacchirena, D. Alulema, D. Aguilar, D. Morocho, F. Encalada, E. Granizo, Analysis of attack and protection systems in Wi-Fi wireless networks under the Linux operating system, in: 2016 IEEE International Conference on Automatica (ICA-ACCA), 2016, pp. 1–7. Curico.
[32] K. El Makkaoui, A. Ezzati, A. Beni-Hssane, C. Motamed, Cloud security and privacy model for providing secure cloud services, in: 2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech), 2016, pp. 81–86. Marrakech.
[33] M. Monshizadeh, V. Khatri, R. Kantola, Detection as a service: an SDN application, in: 2017 19th International Conference on Advanced Communication Technology (ICACT), 2017, pp. 285–290. Bongpyeong.
[34] O. Osanaiye, K.-K.R. Choo, M. Dlodlo, Distributed denial of service (DDos) resilience in cloud: review and conceptual cloud DDoS mitigation framework, J. Netw. Comput. Appl. 67 (2016) 147–165.
[35] A.I. Swapna, Z. Rahman, M.H. Rahman, M. Akramuzzaman, Performance evaluation of fuzzy integrated firewall model for hybrid cloud based on packet utilization, in: 2016 First IEEE International Conference on Computer Communication and the Internet (ICCCI), 2016, pp. 253–256. Wuhan.
[36] Y. Jin, M. Tomoishi, S. Matsuura, Enhancement of VPN authentication using GPS information with geo-privacy protection, in: 2016 25th International Conference on Computer Communication and Networks (ICCCN), 2016, pp. 1–6. Waikoloa, HI.
[37] C.C. Machado, L.Z. Granville, A. Schaeffer-Filho, ANSwer: combining NFV and SDN features for network resilience strategies, in: 2016 IEEE Symposium on Computers and Communication (ISCC), 2016, pp. 391–396. Messina.
[38] M. Ammar, M. Rizk, A. Abdel-Hamid, A.K. Aboul-Seoud, A framework for security enhancement in SDN-based datacenters, in: 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2016, pp. 1–4. Larnaca.
[39] N.V. Patel, N.M. Patel, C. Kleopa, OpenAppID - application identification framework next generation of firewalls, in: 2016 Online International Conference on Green Engineering and Technologies (IC-GET), 2016, pp. 1–5. Coimbatore.
[40] Proofpoint, Proofpoint uncovers internet of things (IoT) cyberattack, Proofpoint Release (2014). http://investors.proofpoint.com/releasedetail.cfm?releaseid=819799 (last accessed October 31, 2017).
[41] S. Abbott-McCune, L.A. Shay, Intrusion prevention system of automotive network CAN bus, in: 2016 IEEE International Carnahan Conference on Security Technology (ICCST), 2016, pp. 1–8. Orlando, FL.
[42] Z. Salek, F.M. Madani, Multi-level Intrusion detection system in cloud environment based on trust level, in: 2016 6th International Conference on Computer and Knowledge Engineering (ICCKE), 2016, pp. 94–99. Mashhad.
[43] T. Sato, S. Chivapreecha, P. Moungnoul, K. Higuchi, An FPGA architecture for ASIC-FPGA Co-design to streamline processing of IDSs, in: 2016 International Conference on Collaboration Technologies and Systems (CTS), 2016, pp. 412–417. Orlando, FL.
[44] Y.K. Al-Douri, V. Pangracious, M. Al-Doori, Artifical immune system using Genetic Algorithm and decision tree, in: 2016 International Conference on Bio-engineering for Smart Technologies (BioSMART), 2016, pp. 1–4. Dubai.
[45] A.A. Waskita, H. Suhartanto, L.T. Handoko, A performance study of anomaly detection using entropy method, in: 2016 International Conference on Computer, Control, Informatics and its Applications (IC3INA), 2016, pp. 137–140. Tangerang.
[46] T.J. Su, S.M. Wang, Y.F. Chen, C.L. Liu, Attack detection of distributed denial of service based on Splunk, in: 2016 International Conference on Advanced Materials for Science and Engineering (ICAMSE), 2016, pp. 397–400. Tainan.
[47] Chibiao Liu, Jinming Qiu, Performance study of 802.11w for preventing DoS attacks on wireless local area networks, Wirel. Personal. Commun. 95 (2) (2017) 1031–1053.
[48] Agrawal Neha, Shashikala Tapaswi, The performance analysis of honeypot based intrusion detection system for wireless network, Int. J. Wirel. Inf. Netw. 24 (1) (2017) 14–26.
[49] F. Abazari, A. Madani, H. Gharaee, Optimal response to computer network threats, in: 2016 8th International Symposium on Telecommunications (IST), 2016, pp. 729–734. Tehran.
[50] Wonhyung Park, Ahn Seongjin, Performance comparison and detection analysis in Snort and Suricata environment, Wirel. Personal. Commun. 94 (2) (2017) 241–252.
[51] M. Chen; Y. Qian; J. Chen; K. Hwang; S. Mao; L. Hu, "Privacy protection and intrusion avoidance for cloudlet-based medical data sharing," in IEEE Transactions on Cloud Computing, vol.PP, no.vol. 99, pp.1–1.
[52] H. Sedjelmaci, S.M. Senouci, M.A. Messous, How to detect cyber-attacks in unmanned aerial vehicles network?, in: 2016 IEEE Global Communications Conference (GLOBECOM), 2016, pp. 1–6. Washington, DC.
[53] N.A.S. Mirza, H. Abbas, F.A. Khan, J. Al Muhtadi, Anticipating Advanced Persistent Threat (APT) countermeasures using collaborative security mechanisms, in: 2014 International Symposium on Biometrics and Security Technologies (ISBAST), 2014, pp. 129–132. Kuala Lumpur.
[54] Z. Chen, W. Dong, H. Li, P. Zhang, X. Chen, J. Cao, Collaborative network security in multi-tenant data center for cloud computing, Tsinghua Sci. Technol. 19 (1) (Feb. 2014) 82–94.
[55] A. Karantjias, N. Polemi, S. Papastergiou, "Advanced security management system for critical infrastructures, in: IISA 2014, the 5th International Conference on Information, Intelligence, Systems and Applications, 2014, pp. 291–297. Chania.
[56] R. Koelle, G. Markarian, D. Kolev, GAMMA - filling the security management void of SESAR and NextGen, in: 2014 Integrated Communications, Navigation and Surveillance Conference (ICNS) Conference Proceedings, 2014. H3-H1-H3-9, Herndon, VA.
[57] D. Ganesh, V.V. RamaPrasad, Protection of shared data among multiple users for online social networks, in: 2014 International Conference on Contemporary Computing and Informatics (IC3I), 2014, pp. 768–773. Mysore.
[58] C. Christoforidis, V. Vlachos, I. Androulidakis, A crowdsourcing approach to protect against novel malware threats, in: 2014 22nd Telecommunications Forum Telfor (TELFOR), 2014, pp. 1063–1066. Belgrade.
[59] G. Indumathi, S. Sakthivel, Securely detecting an intruders in MANETs system, in: International Conference on Information Communication and Embedded Systems (ICICES2014), 2014, pp. 1–5. Chennai.
[60] Amel Bennaceur, Arosha K. Bandara, Michael Jackson, Wei Liu, Lionel Montrieux, Thein Than Tun, Yijun Yu, Bashar Nuseibeh, Requirements-driven mediation for collaborative security, in: Proceedings of the 9th International Symposium on Software Engineering for Adaptive and Self-managing Systems (SEAMS 2014), ACM, New York, NY, USA, 2014, pp. 37–42.
[61] Jeff Wilson, Judith M. Brown, Robert Biddle, ACH walkthrough: a distributed multi-device tool for collaborative security analysis, in: Proceedings of the 2014 ACM Workshop on Security Information Workers (SIW '14), ACM, New York, NY, USA, 2014, pp. 9–16.
[62] John Sonchack, Adam J. Aviv, LESS is more: host-agent based simulator for large-scale evaluation of security systems, in: European Symposium on Research in Computer Security,Computer Security – ESORICS, 2014, pp. 365–382.
[63] Rahul Hiran, Niklas Carlsson, Nahid Shahmehri, PrefiSec: a distributed alliance framework for collaborative BGP monitoring and prefix-based security, in: Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security (WISCS '14), ACM, New York, NY, USA, 2014, pp. 3–12.
[64] Julien Freudiger, Shantanu Rane, Alejandro E. Brito, Ersin Uzun, Privacy preserving data quality assessment for high-fidelity data sharing, in: Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security (WISCS '14), ACM, New York, NY, USA, 2014, pp. 21–29.
[65] Yosra Ben Saied, Alexis Olivereau, Djamal Zeghlache, Maryline Laurent, A survey of collaborative services and security-related issues in modern wireless Ad-Hoc communications, J. Netw. Comput. Appl. 45 (2014) 215–227. ISSN 1084-8045.
[66] Pratik Narang, Chittaranjan Hota, Game-theoretic strategies for IDS deployment in peer-to-peer networks, Inf. Syst. Front. 17 5 (October 2015) (2015) 1017–1028.
[67] Beibei Li, Rongxing Lu, Wei Wang, Kim-Kwang Raymond Choo, Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system, J. Parallel Distrib. Comput. 103, C (May 2017) (2017) 32–41.
[68] Y. Xie, Y. Wang, H. He, Y. Xiang, S. Yu, X. Liu, A general collaborative framework for modeling and perceiving distributed network behavior, IEEE/ACM Trans. Netw. 24 (5) (October 2016) 3162–3176.

[69] F. Sallabi, K. Shuaib, Internet of things network management system architecture for smart healthcare, in: 2016 Sixth International Conference on Digital Information and Communication Technology and its Applications (DICTAP), 2016, pp. 165–170. Konya.
[70] M. Ghorbani, H.R. Ghorbani, M.R. Hashemi, Configuration strategies for collaborative IDS using game theory, in: 2016 24th Iranian Conference on Electrical Engineering (ICEE), 2016, pp. 261–266. Shiraz.
[71] J. Wu; K. Ota; M. Dong; J. Li; H. Wang, "Big data analysis based security situational awareness for smart grid," in IEEE Trans. Big Data, vol.PP, no.99, pp.1–1.
[72] S.H. Almotiri, M.A. Khan, M.A. Alghamdi, Mobile health (m-Health) system in the context of IoT, in: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), 2016, pp. 39–42. Vienna.
[73] Daegeon Kim, JiYoung Woo, Huy Kang Kim, I know what you did before": general framework for correlation analysis of cyber threat incidents, in: MILCOM 2016-2016 IEEE Military Communications Conference, 2016, pp. 782–787. Baltimore, MD.
[74] Amine Boukhtouta, Serguei A. Mokhov, Nour-Eddine Lakhdari, Mourad Debbabi, Joey Paquet, Network malware classification comparison using DPI and flow packet headers, J. Comput. Virology Hacking Tech. 12 (2) (2016) 69–100.
[75] Geetanjali Rathee, Hemraj Saini, Mitigation techniques for gray hole and black hole attacks in wireless mesh network, in: Proceedings of the International Congress on Information and Communication Technology, 2016, pp. 383–392.
[76] Xiang Pan, Vinod Yegneswaran, Yan Chen, Phillip Porras, Seungwon Shin, HogMap: using SDNs to incentivize collaborative security monitoring, in: Proceedings of the 2016 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization (SDN-NFV Security '16), ACM, New York, NY, USA, 2016, pp. 7–12.
[77] Nadine Herold, Holger Kinkelin, Georg Carle, Collaborative incident handling based on the blackboard-pattern, in: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security (WISCS '16), ACM, New York, NY, USA, 2016, pp. 25–34.
[78] Cynthia Wagner, et al., MISP: the design and implementation of a collaborative threat intelligence sharing platform, in: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, ACM, 2016.
[79] da Costa Júnior, Edmilson P., et al. "An Architecture for Self-adaptive Distributed Firewall.".
[80] D. Kolev, R. Koelle, Rosa Ana Casar Rodriguez, P. Montefusco, Security situation management - developing a concept of operations and threat prediction capability, in: 2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC), 2015, 4C2-1-4C2-11, Prague.
[81] A. Bouchami, E. Goettelmann, O. Perrin, C. Godart, Enhancing access-control with risk-metrics for collaboration on social cloud-platforms, in: 2015 IEEE Trustcom/BigDataSE/ISPA, 2015, pp. 864–871. Helsinki.
[82] B. Liu, J. Bi, DISCS: a DIStributed collaboration system for inter-as spoofing defense, in: 2015 44th International Conference on Parallel Processing, 2015, pp. 160–169. Beijing.
[83] N. Arya, U. Singh, S. Singh, Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm, in: 2015 International Conference on Computer, Communication and Control (IC4), 2015, pp. 1–5. Indore.
[84] A. Sharma, D. Bhuriya, U. Singh, Secure data transmission on MANET by hybrid cryptography technique, in: 2015 International Conference on Computer, Communication and Control (IC4), 2015, pp. 1–6. Indore.
[85] E. Vasilomanolakis, M. Krügl, C.G. Cordero, M. Mühlhäuser, M. Fischer, SkipMon: a locality-aware collaborative intrusion detection system, in: 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC), 2015, pp. 1–8. Nanjing.
[86] Y. Zhang, F. Patwa, R. Sandhu, Community-based secure information and resource sharing in AWS public cloud, in: 2015 IEEE Conference on Collaboration and Internet Computing (CIC), 2015, pp. 46–53. Hangzhou.
[87] Hong Liang, Yufei Ge, Wenjiao Wang, Lin Chen, Collaborative intrusion detection as a service in cloud computing environment, in: 2015 IEEE International Conference on Progress in Informatics and Computing (PIC), 2015, pp. 476–480. Nanjing.
[88] Á. Mac Dermott, Q. Shi, K. Kifayat, Detecting intrusions in federated cloud environments using security as a service, in: 2015 International Conference on Developments of E-systems Engineering (DeSE), 2015, pp. 91–96. Duai.
[89] Spyridon Papastergiou, Nineta Polemi, Athanasios Karantjias, CYSM: an innovative physical/cyber security management system for ports, in: International Conference on Human Aspects of Information Security, Privacy, and Trust, 2015, pp. 219–230.
[90] Julien Freudiger, Emiliano De Cristofaro, Alejandro E. Brito, Controlled data sharing for collaborative predictive blacklisting, in: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, Cham, 2015.
[91] Takeshi Takahashi, Tao Ban, Takao Mimura, Koji Nakao, Fine-grained risk level quantication schemes based on APK metadata, in: International Conference on Neural Information Processing, 2015, pp. 663–673.
[92] C.G. Cordero, E. Vasilomanolakis, M. Mühlhäuser, M. Fischer, Community-based collaborative intrusion detection, in: SecureComm, 2015 Oct 26, pp. 665–681.
[93] M.A. Noureddine, A. Marturano, K. Keefe, M. Bashir, W.H. Sanders, Accounting for the human user in predictive security models, in: 2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC), 2017, pp. 329–338. Christchurch, New Zealand.
[94] W.H. Sanders, J.F. Meyer, Stochastic activity networks: formal definitions and concepts, in: E. Brinksma, H. Hermanns, J.-P. Katoen (Eds.), Lectures on Formal Methods and Performance Analysis, Ser. Lecture Notes in Computer Science, vol. 2090, Springer Berlin Heidelberg, 2001, pp. 315–343.
[95] S. Abraham, S. Nair, A novel architecture for predictive CyberSecurity using non-homogenous Markov models, in: 2015 IEEE Trustcom/BigDataSE/ISPA, 2015, pp. 774–781. Helsinki.
[96] A. Oluwaseun, Z. Pavol, L. Dale, R. Ron, An analysis of CVSS v2 environmental scoring, in: Privacy, Security, Risk and Trust (PASSAT), Oct. 2011. Date: 9–11.
[97] M. Schiffman, "Common vulnerability scoring system (CVSS)," http://www.first.org/cvss/.
[98] Assad Ali, Pavol Zavarsky, Dale Lindskog, Ron Ruhl, A Software Application to Analyze Affects of Temporal and Environmental Metrics on Overall CVSS V2 Score, Concordia University College of Alberta, Edmonton, Canada, October 2010.
[99] https://nvd.nist.gov/[last accessed 11September 2017].
[100] Y. Shi, S. Abhilash, K. Hwang, Cloudlet mesh for securing mobile clouds from intrusions and network attacks, in: 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, 2015, pp. 109–118. San Francisco, CA.
[101] K. Hwang, D. Li, Trusted cloud computing resources and data coloring, IEEE Internet Co. 14 (Sept. 2010).
[102] Yu-Beng Leau, Selvakumar Manickam, A novel adaptive grey verhulst model for network security situation prediction, Int. J. Adv. Comput. Sci. Appl. 1 (7) (2016) 90–95.
[103] Microsoft 2017. The Coco Framework Technical Overview. https://raw.githubusercontent.com/Azure/coco.framework/master/docs/Coco%20Framework%20whitepaper.pdf [last accessed 10 October 2017].
[104] K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access 4 (2016) 2292–2303.