

Accepted Manuscript

A blockchain future to Internet of Things security: A position paper

Mandrita Banerjee, Junghee Lee, Kim-Kwang Raymond Choo

PII: S2352-8648(17)30290-0

DOI: [10.1016/j.dcan.2017.10.006](https://doi.org/10.1016/j.dcan.2017.10.006)

Reference: DCAN 118

To appear in: *Digital Communications and Networks*

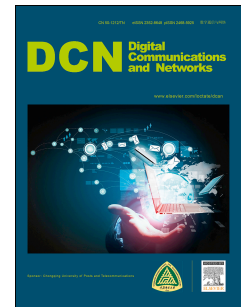
Received Date: 11 September 2017

Revised Date: 10 October 2017

Accepted Date: 30 October 2017

Please cite this article as: M. Banerjee, J. Lee, K.-K.R. Choo, A blockchain future to Internet of Things security: A position paper, *Digital Communications and Networks* (2017), doi: 10.1016/j.dcan.2017.10.006.

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.



A Blockchain Future to Internet of Things Security: A Position Paper

Mandrita Banerjee¹, Junghee Lee¹, Kim-Kwang Raymond Choo^{2,1}

¹Department of Electrical and Computer Engineering, University of Texas at San Antonio, San Antonio, TX 78249, USA

²Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249, USA

mandrita82@gmail.com, Junghee.Lee@utsa.edu, raymond.choo@fulbrightmail.org

Abstract

Internet-of-Things (IoT) are increasingly found in civilian and military contexts, ranging from Smart Cities to Smart Grids to Internet-of-Medical-Things to Internet-of-Vehicles to Internet-of-Military-Things to 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, include the lack of publicly available IoT datasets that can be used by the research and practitioner communities. Given the potential sensitive nature of IoT datasets, there is a need to develop a standard for the sharing of IoT datasets among the research and practitioner communities and other relevant stakeholders. We then 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.

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

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 multitudes of devices to be connected over a network providing us ways to connect and

communicate between machines and human (e.g. machine-to-machine). Such a trend is also commonly referred to as Internet-of-Everything, comprising 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, threat to a system can be a 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 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, access the device and their data remotely, and so on.

What happen 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 at the operating theaters, as the surgical team will not have any idea what happen at that time in time. Not to mention, the trauma or 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 “pear-shaped” very fast in a seemingly normal situation 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 from January 2016. We will defer the survey of IoT privacy techniques as future work. The located articles are then sorted into reactive and proactive approaches, and of the reactive approaches, we further categorize them into (1) intrusion detection systems (IDS) only, and intrusion prevention systems (IPS), and (2) collaborative security approaches – see next Section.

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 and they constantly seek 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. Network path is also changed periodically to prevent unauthorized access and scanning of traffic. However, the amount of packet 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 due to their functionalities 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 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 a lower CPU consumption. However, the multi-threaded Suricata provides better single and multi-core detection performance.

We will now discuss recent intrusion detection and/or prevention systems. For simplicity, IDPS is used to refer to intrusion detection and/or prevention systems in the remaining 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 multi layered security approaches reported in [27, 32]. Specifically, Chang and Ramachandran [27] proposed a multi layered 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 identify management and intrusion prevention to ensure user identify would be verified once again and any detected malicious files will be removed. The third layer is convergent encryption, which provides a top down security policy. To evaluate the proposed approach, the authors conducted a 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 hours. Makkaoui et al. [32] proposed a multi layered cloud security and privacy model (CSPM), which consists of five layers, namely: 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 global positioning system (GPS). The proposed method provides geo-privacy protection on mobile devices. Here, a VPN client sends hash value of the GPS information instead of sending the raw value; thus, 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 was used to check the hit rate of client GPS coordinates of the targeted area, and the authors' evaluation results reported an accuracy rate 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 source

address, time and country of attackers. The approach reduces the manual effort required to dynamically modify high interactive honeypot system by using freely available and open-source technologies. File transfer protocol is useful in attracting attackers that leave traces or evidence of username, passwords and source ports from various countries. However, the manual work needed to convert honeypots into honeynet is significant. Agrawal and Tapaswi [48] proposed a honeypot based multi-layered IDS to detect and prevent rogue access point attacks. The approach combines existing IDS and honeypot to improve the accuracy of existing IDS, and comprises filtering, intrusion detection and honeypot. The system was implemented on a small wireless network. However, deploying the system on cloud and adopting 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, which takes into consideration full account prediction errors and residual traffic. This model was evaluated using a network simulator and delays were calculated. The results indicated only minimal delay is introduced, due to the security analysis. However, this model lacks an ideal prediction algorithm; thus, producing 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 feature selection and extraction stages, and their evaluations indicated 98% prediction scores. Also, based on their evaluations using by the DARPA benchmark data set, 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 attack signature. The approach identified new attacks not present in initial DARPA set. Keshri et al. [21] presented a denial of service (DoS) prevention technique using firewall and IDS based on data mining techniques, which comprises data selection, data preprocessing, transformation, and model selection and evaluation. They used NSL-KDD dataset, a refined version of KDD99 cup data set, for evaluation.

Sato et al. [43] suggested an Field Programmable Gate Arrays (FPGA) architecture for Application Specific Integrated Circuits (ASIC)–FPGA co-design to streamline the processing of IDPS and improve the processing speed of FPGA compared to 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 are developed in the FPGA with complementary metal-oxide-semiconductor (CMOS) technology.

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

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

Approaches	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]

2.1.2 Classification by network structures

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 weighted attack graph. Specifically, this is a dynamic proactive multi-purpose threat response model designed to minimize threats and cost. Other optimization methods such as genetic algorithm could be implemented to respond quickly to threats optimally 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 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 they are authorized to. However, IPS used in this system only controls the network conditions made by PKI and firewall. Existing energy aware IPS allows early detection and discarding of malicious packets; thus, resulting in additional delays for packet delivery. Filipek and Hudec [25] proposed a secure architecture for MANETs consisting of secure RSA-based routing protocol, PKI, firewall and IPS. Routing packets are signed and the negotiated symmetric keys with short validity are used to encrypt traffic. IPS monitors traffic and alerts the nodes of suspicious activities. Limitations of this approach include traffic restriction due to the presence of firewall, and significant overheads due to sending of messages by nodes, database lookup, control packet and encryption.

Yacchirena et al. [31] developed a Wi-Fi wireless network running in Linux operating system, using Snort and Kismet as IDS and IPS, respectively. Penetration testings 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 will

be checked, in the sense that system log will be scanned and information about all application and software installed in the system will be stored in the IFS database. The regular updating of the database is designed to facilitate the termination of 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 attack prevention (RAP) based DoS attacks. In the work, a reliable STA-based queuing model was proposed to analyze the performance of 802.11w. Also, 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 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 defined by 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 the distributed sensor networks. The evaluation was performed in two dimensional space by calculating the entropy from data series of temperature and humidity nodes. 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 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 unmanned aerial vehicle (UAV) against cyber attack. It relies on a threat estimation model based on the Belief approach aiming 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 monitoring node.

Different solutions for software defined networks (SDN) have been proposed. For example, Monshizadeh, Khatri and Kantola [33] proposed a multi layered IDS model with programmability features of 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, namely: 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 packet of the mirrored traffic, and second, clustering is performed on sampled traffic. A combination of 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 network infrastructure to identify network anomaly. Ammar et al. [38] proposed a framework to enhance the security in SDN based datacenter. The authors suggested that the programmability features of SDN, along with integration of application and security layers, increase datacenter security by providing as an adaptive layer. In the approach, advanced persistent threats are detected by searching for abnormal patterns, and analyzing of network traffic. A security agent is then used to collect and analyze security logs, as well as blocking attackers.

McCune and Shay [41] proposed a real time IPS for 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 message from the manufacturer are encoded into the various ECUs. Replayed messages are those captured from a CAN bus segment or are already known. Invalid message whose arbitration identifier is 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.

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

Network structures	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]

2.1.3 Classification by applications

A number of studies have been dedicated to the study of propose various smart mobile devices, such as smart phones. For example, Vij and Jain [7] reviewed existing IDPS approaches for smart phones. They determined that network based IDPS can perform real-time emulation and facilitates the detection of malicious files before actual download, unlike host based IDPS. On the other hand, host based IDPS is cheaper and does not requires as much (dedicated) hardware. Normally, network based IDPS is preferred over host based IDPS. Saracino et al. [10] designed a multi-level 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 detector identifies and blocks suspected threats by detecting a 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 home equipped with 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 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. Visitor can enter the home if the owner approves the access. If the owner denies access to the visitor, then the owner also has the option to contact police directly.

Cadet and Fokum [2] designed and implemented an IPS for voice over Internet Protocol (VoIP). Though efficient and simple, this system produces significant overheads due to the use of Snort. Chenet al. [29] proposed an ASIC design and implementation for VoIP IPS, which 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 due to 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. Detective control solution uses IDS/IPS for detection of an attack. Corrective control (e.g. system back-up measures) is done after attack has been made to control the damage caused by attackers. By adopting different solutions for each measure, EHR system can protect against various attack.

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 artificial immune system inspired from natural immune system (NIS). It uses two theories of immune response: theory of clonal selection and theory of negative selection. The former is appropriate for network based IDPS in scenario analysis, and the latter is appropriate for behavioral analysis in 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 distinguish between normal access and attack records(antigen) by generating decision antibodies (rules).Genetic algorithm is used to define the first level and decision tree classifier is used to define the second level. Access records are classified into normal, antigen or unknown. An unknown access record in level 1 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 AVL tree for storing URL path information. However, URL compressing technique is not well structured due to the large memory requirement during preprocessing. Prokhorenko et al. [28] proposed a real-time supervision framework for hypertext preprocessor (PHP) based web applications, designed for IPS. Protection is provided on the server side and does not require client side assistance. The proposed architecture ensures expected behavior of web application execution by the application author and allows enforcement of behavior determined by the protection administrator.

Su et al. [46] simulated attack using TCP and evaluated the results using UDP to study different types of DDoS attacks on firewall. They also proposed a visualization method to help determine whether an attack has occurred, and 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 unmanned aerial vehicle (UAV) against cyber attacks. It relies on a threat estimation model based on 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 malicious node, then it cannot operate as monitoring node.

Mirza, Mohi-Ud-Din and Awan [1] proposed a cloud-based energy efficient security system with two main modules, namely: cloud engine and 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 Windows, and not for 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 (IM-SecaaS) framework. This cloud-based system provides intrusion detection, prevention and response, 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. NTRU (Number Theory Research Unit) method is used for data protection during data transmission. A trust model is designed to decide the trust level 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-agnostic IPS to secure software defined network (SDN) dataplane. Malicious forward devices and their exact behavior can be automatically detected by analyzing the actual and expected trajectories of packet. However, accuracy under different attack scenarios and use cases needs further investigation. The stability of snapshots used in system analysis is also challenging. WedgeTail is not currently compatible with 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 change point detection of 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 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 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 user's risk level is inversely proportional to the trust level of each user. Users are divided into three groups, namely: high risk, medium risk and low risk. IDS are also categorized in the same way as high risk IDS (HIDS), medium risk IDS (MIDS) and 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.

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

Applications	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]

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 instantaneous and previous data by applying integrating rules from information analysis method into 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 the 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, compared to a conventional firewall. The approach also allows the collection of information on bandwidth consumptions for each network application, and based on this information unwanted applications are blocked. Administrators can create application detectors, which are written in Lua programming language and these can be interfaced with Snort.

2.2 Collaborative Security Techniques

Security cannot work in isolation, and in recent times there has been interest in collaborative security paradigm due 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 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.

Indumathi and Sakthivel [59] proposed an IDS for MANETs, which uses digital signature scheme to eliminate receiver collision and limited transmission power and minimize 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 homomorphic encryption technique. Here, a client only discovers the value of quality metric for a semi-honest party. Data quality assessment ensures that poor quality data will be rejected; thus, reducing the overheads 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 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 what 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 collaborative Border Gateway Protocol (BGP) monitoring and protection against prefix/sub-prefix and edge-based attacks. This is an application layer service that controls sharing of network activity observed by routers and network monitors. Overheads, alert rates and scalability are calculated from public wide area BGP announcement, simulation results and traces.

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

Game theoretic approach has also been utilized for collaborative IDS. Narang, Mehta and Hota [66] discussed a randomized, non-deterministic and game-theoretic 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 such comprehensive way of choosing

the target nodes in this approach. Also, this approach only 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 the attackers and IDS by modeling a multi-player nonzero-sum stochastic game. The expected behavior of attackers as well as defenders and optimal configuration of each IDS are described using the solution of 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 analysis uses 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 collaborate. A collaborative robotic implementation was also presented.

Christoforidis and Vlachos [58] presented a collaborative lightweight client application, which 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 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 efficient correlation analysis of cyber threat incidents using cyber threat intelligence. Here, event relation tree (ERT) is used to represent related events and event transition graph (ETG) is used to describe temporal transition of the event characteristic. The proposed approach can infer an attacker's intention by tracing the transition of related cyber incidents.

2.2.2 *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 traffic samples, it automatically builds and configures the behavior of host agent and monitors their activities throughout simulation results for gathering experimentation data sets.

Saied et al. [65] proposed collaborative schemes for three different networks, namely: routing, security and radio in wireless Ad-Hoc communications. They also discussed two security solutions for handling internal attacks. These are security-by-design mechanism and trust-based mechanism. The latter is more flexible and efficient due 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 Gray Hole and Black Hole attacks in wireless mesh network. Using this approach, network throughput could be increased significantly. However, the number of computation and storage overhead required is 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 cyber threat intelligence services flexibly.

Li et al. [67] proposed a distributed host-based collaborative detection to mitigate false data injection (FDI) attacks in smart grid cyber-physical system. A rule based real-time majority voting algorithm was proposed to detect anomalies in 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 PowerWorld simulator.

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

2.2.3 *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 profile, relationship sharing and content sharing in OSN. They discussed a prototype proof-of-concept implementation of the

approach called DController. Bouchami et al. [81] proposed an enhancement of 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. 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 collective knowledge of each user, and analyzes physical and cyber threats, attack modes and geographical areas. Koelle, Markarian and Kolev [56] described a collaborative security management as a situation management capability, where the security function is designed on the basis of networks of GAMMA (Global ATM Security Management) nodes. A decision making loop is formed by collecting these conceptualized nodes, providing an existing security situation. Kolevetet 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 multi layered telecommunications management network (TMN) model was defined for managing different components of the healthcare system. The proposed management architecture consists of four layers, namely: 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 cost 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 user 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 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 data mining technique. Collaborative IDS have been proposed for 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, namely: 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 [91], the authors proposed category/cluster-based AndroidPackages (APK) analysis schemes for quantifying the risk of an APK. This was achieved using category and cluster information generated from online available metadata. The performance of cluster based scheme is better due to 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 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, analyze and decision engines, are used for this purpose.

Herold, Kinkelin and Carle [77] proposed a collaborative incident handling systems 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 is an information model for blackboard and execution model for accessing information on 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 their information and IoC regarding existing threats in a trusted environment.

Chen et al. [54] presented a collaborative network security prototype system with centralized collaborative scheme for providing network security in multiple-tenant data center. It is

integrated with a smart packet verdict scheme for the purpose of 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.

Applications	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 detection and fixing’. To ensure cyber resiliency in an intelligent and efficient IoT system, it is crucial to have the capability to predict future attack 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 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, Nouredine et al. [93] designed a model based on general deterrence theory that is driven by human decision making process. To do so, the authors reviewed the theories of human behavior in cyber security by studying the fields of 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 representative and also stochastic activity networks (SAN) [94] was used to model the interaction between employees and organization’s security policy. The proposed approach has a number of challenges. Firstly, designing a model from the attackers, employees and administrators’ point of view at a different level of granularity is very challenging. Secondly, 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 agent capable of assessing its current situation and own decision making.

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 consider 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, security analysis and impact analysis to evaluate the concept. The approach is unique in the sense that it makes use of the CVSS framework by taking account of exploitability and impact, as well as expanding the model with temporal aspects of vulnerabilities in an attack tree. One main challenge of this approach is further enhancement in 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 due to computational and energy requirements. Shi, Abhilash and Hwang [100] proposed a hierarchically structured security model based on a trust chain between mobile devices, cloudlet mesh and remote cloud platform. The aim of this approach is to perform collaborative intrusion detection among multiple WiFi-enabled cloudlets by accessing cloud services via WiFi or mobile networks. Real time filtering of malicious attacks was achieved via trusted remote clouds, where predictive security analytics was 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 dataset. A hybrid intrusion detection system could use cloudlet mesh to detect malware and network anomalies, and data coloring techniques [101] could be integrated with this model to protect and access 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 incoming network security situation in a typical organization. In the proposed model, the combination methods of Trapezoidal rule and Simpson's one-third rule was used to find the background value in the gray differential equation for predicting future outcome. Both Mean Absolute Percentage Error (MAPE) and Root Mean Square Deviation (RMSD) were used to compare efficiency of the proposed model. Findings indicated that the new model achieved 93.3% in predictive accuracy, whereas 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 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 majority of the evaluations in other studies were software based.

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],[61]	[93]
Hardware	[2]	-	-
Software and hardware	[41]	-	-

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.

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], [82], [83], [84]	

The need for publicly available IoT datasets: The role of real-world datasets in the evaluation of any proposed security technique, particularly predictive security, could not be overstated. The relatively small number of real-world datasets available is partly due to the amount of time and efforts to collect and compile these datasets. The challenge is compounded by the diversity of IoT devices and architectures. Also, from the review in this paper, 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 to use the *blockchain* technique to ensure integrity in the shared datasets. In addition, *privacy* should be preserved when datasets are released to the public.

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 by multiple sources such as network traffic and operation log of different IoT devices in a specific industry or context (e.g. smart grids). Even within a single IoT system, we may have many different types of IoT devices with different data format and structure. 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 the size of 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, which 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 is 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 security of IoT. We will now present two examples of employing blockchain for IoT security.

Figure 1 illustrates the typical process of how the blockchain works. 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.

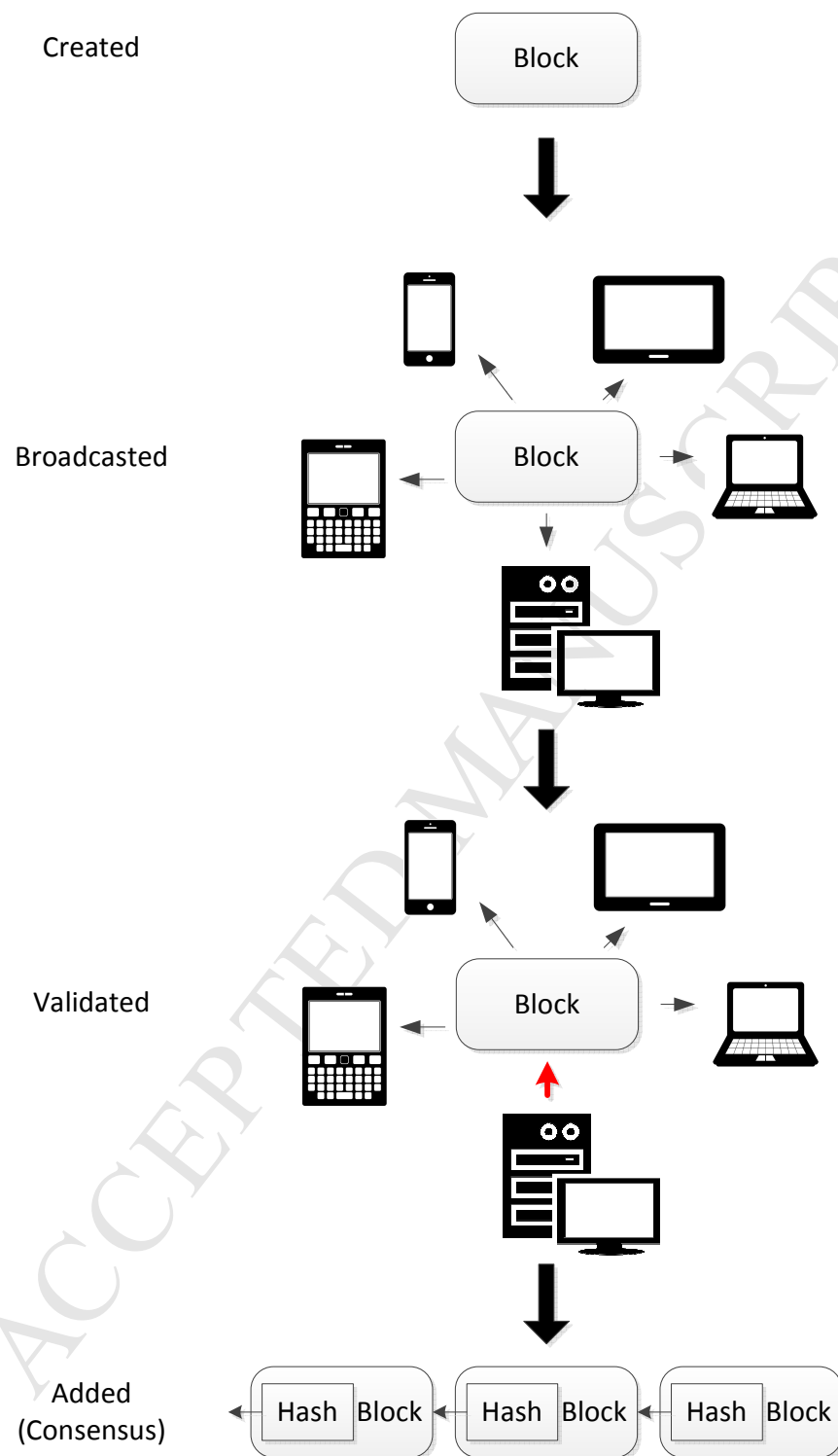


Figure 1: A typical blockchain work flow (adapted from [104])

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 Figure 2.

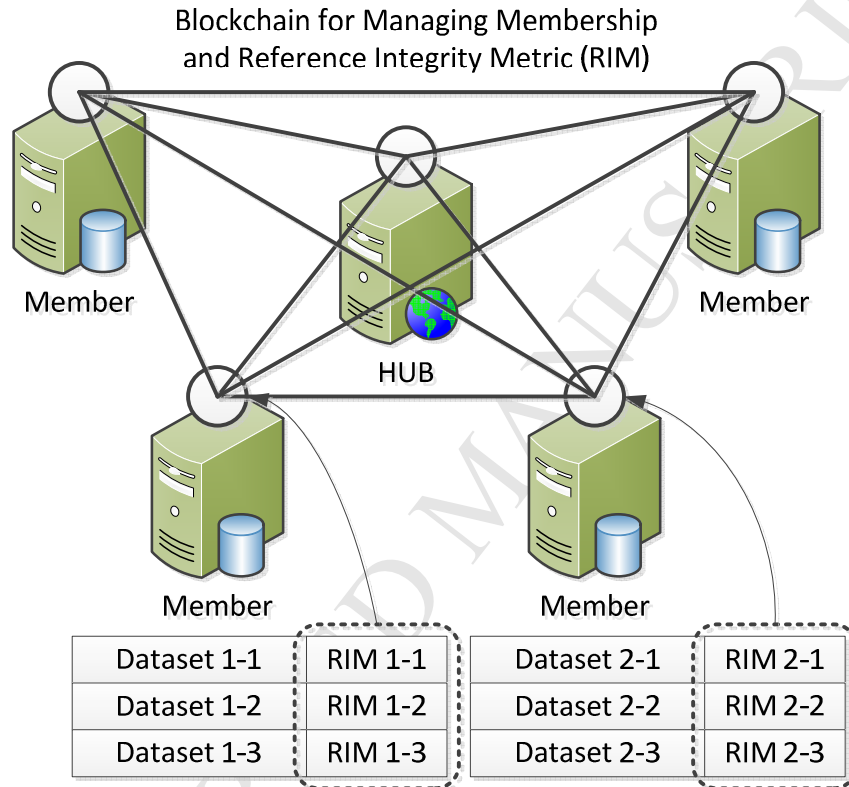


Figure 2: Conceptual blockchain-based management of membership and reference integrity metrics (RIM).

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 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 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 regulation, we emphasize the need for an automated tool that anonymizes datasets prior to the release of these datasets.

Another challenge we need to consider is the lifetime of datasets. The owner 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 RIM is maintained by the blockchain. Therefore, even if the RIM remain 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, we need to have the capability for compromised devices 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, integrity of the next level firmware (operating system and application) is checked before it is executed. The bootloader is stored in a 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 a flash memory to a 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. 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 compared against 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 RIM itself is very important. If the firmware cannot be updated, then RIM should be stored in read-only memory. However, for reasons such as security patch and upgrade of services, update is 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 RIM, as illustrated in Figure 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.

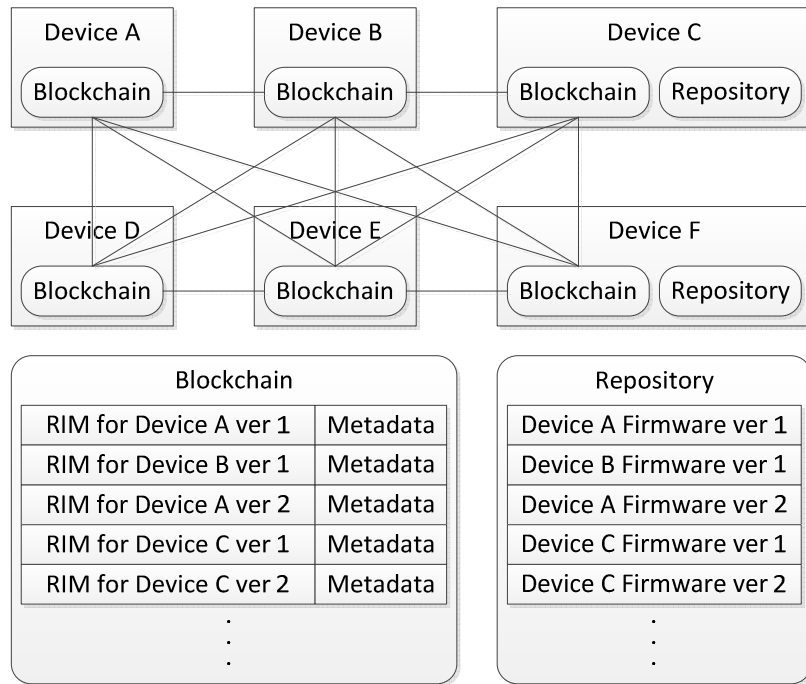


Figure 3: Conceptual blockchain-based compromised firmware detection and self-healing approach.

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 a “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. Due to tight resource constraints, not all devices can retain previous version of the firmware. Thus, some devices in the network (e.g. intermediate nodes with a larger storage capability – e.g. 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 update is 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 of legitimate firmware update through a debugging interface or a remote entity. Any type of firmware update should be handled by the hardware modules for self-healing and 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 repository by the blockchain hardware.

5 A Blockchain Future?

IoT will play an increasingly important role in our society for the foreseeable future, in both civilian and military (adversarial) contexts, such as Internet of Drones, Internet of Battlefield Things 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 potential mitigation strategy (e.g. formulate probable course of action for each identified threat). Due to the time sensitive nature of certain IoT applications (e.g. in military or adversarial context), the identification potential IoT threat vectors and 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 purpose. 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 also 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

processing power required for public blockchain networks—and associated energy costs—are also 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], that 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 keep a watchful brief on 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 from being compromised or tampered if the device is physically accessible?
- *Research topic 9:* Under the 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 and I. Awan, "A Cloud-Based Energy Efficient System for Enhancing the Detection and Prevention of Modern Malware," *2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, Crans-Montana, 2016, pp. 754-761.
- [2] F. Cadet and D. T. Fokum, "Coping with denial-of-service attacks on the IP telephony system," *SoutheastCon 2016*, Norfolk, VA, 2016, pp. 1-7.
- [3] D. H. Sharma, C. A. Dhote and M. M. Potey, "Implementing Intrusion Management as Security-as-a-service from cloud," *2016 International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)*, Bangalore, 2016, pp. 363-366.
- [4] Amos O. Olagunju and Farouk Samu. 2016. 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, 41-46.
- [5] M. Yevdokymenko, "An adaptive algorithm for detecting and preventing attacks in telecommunication networks," *2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T)*, Kharkiv, 2016, pp. 175-177.
- [6] M. Ford et al., "A process to transfer Fail2ban data to an adaptive enterprise intrusion detection and prevention system," *SoutheastCon 2016*, Norfolk, VA, 2016, pp. 1-4.

- [7] S. Vij and A. Jain, "Smartphone nabbing: Analysis of intrusion detection and prevention systems," *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, 2016, pp. 2209-2214.
- [8] G. Kalnoor and J. Agarkhed, "Pattern matching intrusion detection technique for Wireless Sensor Networks," *2016 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)*, Chennai, 2016, pp. 724-728.
- [9] S. Kumawat, A. K. Sharma and A. Kumawat, "Intrusion detection and prevention system using K-learning classification in cloud," *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, 2016, pp. 815-820.
- [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. 99, pp. 1-1
- [11] S. Alsunbul, P. Le, J. Tan and B. Srinivasan, "A network defense system for detecting and preventing potential hacking attempts," *2016 International Conference on Information Networking (ICOIN)*, Kota Kinabalu, 2016, pp. 449-454.
- [12] J. Filipek and L. Hudec, "Securing Mobile Ad Hoc Networks using distributed firewall with PKI," *2016 IEEE 14th International Symposium on Applied Machine Intelligence and Informatics (SAMi)*, Herlany, 2016, pp. 321-325.
- [13] A. Merlo, M. Migliardi and E. Spadacini, "Balancing Delays and Energy Consumption in IPS-Enabled Networks," *2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, Crans-Montana, 2016, pp. 267-272.
- [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*, 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*, In press
- [16] I. Indre and C. Lemnaru, "Detection and prevention system against cyber attacks and botnet malware for information systems and Internet of Things," *2016 IEEE 12th International Conference on Intelligent Computer Communication and Processing (ICCP)*, Cluj-Napoca, 2016, pp. 175-182.
- [17] M. T. Rashid, I. K. Abir, N. S. Shourove, R. Muntaha and M. K. Rhaman, "Intelligent intrusion prevention system for households based on system-on-chip computer," *2016 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, Vancouver, BC, 2016, pp. 1-5.

- [18] R. Dewanjee, "Intrusion Filtration System(IFS)-mapping network security in new way," 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPEs), Paralakhemundi, 2016, pp. 527-531.
- [19] T. Zitta, M. Neruda and L. Vojtech, "The security of RFID readers with IDS/IPS solution using Raspberry Pi," 2017 18th International Carpathian Control Conference (ICCC), Sinaia, 2017, pp. 316-320.
- [20] H. Sedjelmaci, S. M. Senouci and M. A. Messous, "How to Detect Cyber-Attacks in Unmanned Aerial Vehicles Network?," 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, 2016, pp. 1-6.
- [21] A. Keshri, S. Singh, M. Agarwal and S. K. Nandiy, "DoS attacks prevention using IDS and data mining," 2016 International Conference on Accessibility to Digital World (ICADW), Guwahati, 2016, pp. 87-92.
- [22] A. Gharib, I. Sharafaldin, A. H. Lashkari and A. A. Ghorbani, "An Evaluation Framework for Intrusion Detection Dataset," 2016 International Conference on Information Science and Security (ICISS), Pattaya, 2016, pp. 1-6.
- [23] Yousef Farhaoui, "Design and Implementation of an Intrusion Prevention System," 2017 International Journal of Network Security, Vol.19, No.5, PP.675-683.
- [24] ArashShaghaghi, Mohamed Ali Kaafar, and Sanjay Jha. 2017. 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, 849-861.
- [25] JozefFilipek and LadislavHudec, "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 and Ma Xiujuan, "A large-scale URL filtering algorithm in high-speed flow," 2016 2nd IEEE International Conference on Computer and Communications (ICCC), Chengdu, 2016, pp. 1043-1046.
- [27] V. Chang and M. Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework," in IEEE Transactions on Services Computing, vol. 9, no. 1, pp. 138-151, Jan.-Feb. 1 2016.
- [28] V. Prokhorenko, K. K. R. Choo and H. Ashman, "Intent-Based Extensible Real-Time PHP Supervision Framework," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 10, pp. 2215-2226, Oct. 2016.

- [29] M. J. Chen, C. C. Wen, H. C. Lin and Y. S. Chu, "ASIC design and implementation for VoIP intrusion prevention system," *2016 International Conference on Applied System Innovation (ICASI)*, Okinawa, 2016, pp. 1-4.
- [30] H. Osop and T. Sahama, "Quality evidence, quality decisions: Ways to improve security and privacy of EHR systems," *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Munich, 2016, pp. 1-6.
- [31] A. Yacchirena, D. Alulema, D. Aguilar, D. Morocho, F. Encalada and E. Granizo, "Analysis of attack and protection systems in Wi-Fi wireless networks under the Linux operating system," *2016 IEEE International Conference on Automatica (ICA-ACCA)*, Curico, 2016, pp. 1-7.
- [32] K. El Makkaoui, A. Ezzati, A. Beni-Hssane and C. Motamed, "Cloud security and privacy model for providing secure cloud services," *2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech)*, Marrakech, 2016, pp. 81-86.
- [33] M. Monshizadeh, V. Khatri and R. Kantola, "Detection as a service: An SDN application," *2017 19th International Conference on Advanced Communication Technology (ICACT)*, Bongpyeong, 2017, pp. 285-290.
- [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. Network Comput. Appl.* 67 (2016) 147–165.
- [35] A. I. Swapna, Z. Rahman, M. H. Rahman and M. Akramuzzaman, "Performance evaluation of fuzzy integrated firewall model for hybrid cloud based on packet utilization," *2016 First IEEE International Conference on Computer Communication and the Internet (ICCCI)*, Wuhan, 2016, pp. 253-256.
- [36] Y. Jin, M. Tomoishi and S. Matsuura, "Enhancement of VPN Authentication Using GPS Information with Geo-Privacy Protection," *2016 25th International Conference on Computer Communication and Networks (ICCCN)*, Waikoloa, HI, 2016, pp. 1-6.
- [37] C. C. Machado, L. Z. Granville and A. Schaeffer-Filho, "ANSwer: Combining NFV and SDN features for network resilience strategies," *2016 IEEE Symposium on Computers and Communication (ISCC)*, Messina, 2016, pp. 391-396.
- [38] M. Ammar, M. Rizk, A. Abdel-Hamid and A. K. Aboul-Seoud, "A Framework for Security Enhancement in SDN-Based Datacenters," *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Larnaca, 2016, pp. 1-4.

- [39] N. V. Patel, N. M. Patel and C. Kleopa, "OpenAppID - application identification framework next generation of firewalls," 2016 Online International Conference on Green Engineering and Technologies (IC-GET), Coimbatore, 2016, pp. 1-5.
- [40] Proofpoint, "Proofpoint uncovers internet of things (IoT) cyberattack," Proofpoint Release, 2014
- [41] S. Abbott-McCune and L. A. Shay, "Intrusion prevention system of automotive network CAN bus," *2016 IEEE International Carnahan Conference on Security Technology (ICCST)*, Orlando, FL, 2016, pp. 1-8.
- [42] Z. Salek and F. M. Madani, "Multi-level Intrusion detection system in cloud environment based on trust level," 2016 6th International Conference on Computer and Knowledge Engineering (ICCKE), Mashhad, 2016, pp. 94-99.
- [43] T. Sato, S. Chivapreecha, P. Moungnoul and K. Higuchi, "An FPGA Architecture for ASIC-FPGA Co-design to Streamline Processing of IDSs," 2016 International Conference on Collaboration Technologies and Systems (CTS), Orlando, FL, 2016, pp. 412-417.
- [44] Y. K. Al-Douri, V. Pangracious and M. Al-Doori, "Artificial immune system using Genetic Algorithm and decision tree," 2016 International Conference on Bio-engineering for Smart Technologies (BioSMART), Dubai, 2016, pp. 1-4.
- [45] A. A. Waskita, H. Suhartanto and L. T. Handoko, "A performance study of anomaly detection using entropy method," 2016 International Conference on Computer, Control, Informatics and its Applications (IC3INA), Tangerang, 2016, pp. 137-140.
- [46] T. J. Su, S. M. Wang, Y. F. Chen and C. L. Liu, "Attack detection of distributed denial of service based on Splunk," 2016 International Conference on Advanced Materials for Science and Engineering (ICAMSE), Tainan, 2016, pp. 397-400.
- [47] Chibiao Liu, JinmingQiu, "Performance Study of 802.11w for Preventing DoS Attacks on Wireless Local Area Networks", 2017 Wireless Personal Communication, Volume 95, Issue 2, pp. 1031-1053.
- [48] Agrawal Neha, and Shashikala Tapaswi. "The Performance Analysis of Honeypot Based Intrusion Detection System for Wireless Network." *International Journal of Wireless Information Networks* 24.1 (2017): 14-26.
- [49] F. Abazari, A. Madani and H. Gharaee, "Optimal response to computer network threats," 2016 8th International Symposium on Telecommunications (IST), Tehran, 2016, pp. 729-734.
- [50] Park, Wonhyung, and SeongjinAhn. "Performance comparison and detection analysis in Snort and Suricata environment." *Wireless Personal Communications* 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. 99, pp. 1-1
- [52] H. Sedjelmaci, S. M. Senouci and M. A. Messous, "How to Detect Cyber-Attacks in Unmanned Aerial Vehicles Network?," 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, 2016, pp. 1-6.
- [53] N. A. S. Mirza, H. Abbas, F. A. Khan and J. Al Muhtadi, "Anticipating Advanced Persistent Threat (APT) countermeasures using collaborative security mechanisms," *2014 International Symposium on Biometrics and Security Technologies (ISBAST)*, Kuala Lumpur, 2014, pp. 129-132.
- [54] Z. Chen, W. Dong, H. Li, P. Zhang, X. Chen and J. Cao, "Collaborative network security in multi-tenant data center for cloud computing," in *Tsinghua Science and Technology*, vol. 19, no. 1, pp. 82-94, Feb. 2014.
- [55] A. Karantjias, N. Polemi and S. Papastergiou, "Advanced security management system for critical infrastructures," *IISA 2014, The 5th International Conference on Information, Intelligence, Systems and Applications*, Chania, 2014, pp. 291-297.
- [56] R. Koelle, G. Markarian and D. Koley, "GAMMA - Filling the security management void of SESAR and NextGen," *2014 Integrated Communications, Navigation and Surveillance Conference (ICNS) Conference Proceedings*, Herndon, VA, 2014, pp. H3-1-H3-9.
- [57] D. Ganesh and V. V. RamaPrasad, "Protection of shared data among multiple users for online social networks," *2014 International Conference on Contemporary Computing and Informatics (IC3I)*, Mysore, 2014, pp. 768-773.
- [58] C. Christoforidis, V. Vlachos and I. Androulidakis, "A crowdsourcing approach to protect against novel malware threats," *2014 22nd Telecommunications Forum Telfor (TELFOR)*, Belgrade, 2014, pp. 1063-1066.
- [59] G. Indumathi and S. Sakthivel, "Securely detecting an intruders in MANETs system," *International Conference on Information Communication and Embedded Systems (ICICES2014)*, Chennai, 2014, pp. 1-5.
- [60] AmelBennaceur, Arosha K. Bandara, Michael Jackson, Wei Liu, Lionel Montrieux, Thein Than Tun, Yijun Yu, and 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, and 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," *European Symposium on Research in Computer Security*, Computer Security – ESORICS, 2014, pp 365-382
- [63] Rahul Hiran, Niklas Carlsson, and 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, and 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," *Journal of Network and Computer Applications*, Volume 45, 2014, pp 215-227, ISSN 1084-8045.
- [66] Pratik Narang and Chittaranjan Hota, "Game-theoretic strategies for IDS deployment in peer-to-peer networks," *Information Systems Frontiers* 17, 5 (October 2015), 2015, pp 1017-1028.
- [67] Beibei Li, Rongxing Lu, Wei Wang, and 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, pp 32-41.
- [68] Y. Xie, Y. Wang, H. He, Y. Xiang, S. Yu and X. Liu, "A General Collaborative Framework for Modeling and Perceiving Distributed Network Behavior," in *IEEE/ACM Transactions on Networking*, vol. 24, no. 5, pp. 3162-3176, October 2016.
- [69] F. Sallabi and K. Shuaib, "Internet of things network management system architecture for smart healthcare," *2016 Sixth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, Konya, 2016, pp. 165-170.
- [70] M. Ghorbani, H. R. Ghorbani and M. R. Hashemi, "Configuration strategies for collaborative IDS using game theory," *2016 24th Iranian Conference on Electrical Engineering (ICEE)*, Shiraz, 2016, pp. 261-266.
- [71] J. Wu; K. Ota; M. Dong; J. Li; H. Wang, "Big Data Analysis based Security Situational Awareness for Smart Grid," in *IEEE Transactions on Big Data*, vol. PP, no. 99, pp. 1-1

- [72] S. H. Almotiri, M. A. Khan and M. A. Alghamdi, "Mobile Health (m-Health) System in the Context of IoT," *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, Vienna, 2016, pp. 39-42.
- [73] Daegeon Kim, JiYoung Woo and Huy Kang Kim, "'I know what you did before': General framework for correlation analysis of cyber threat incidents," *MILCOM 2016 - 2016 IEEE Military Communications Conference*, Baltimore, MD, 2016, pp. 782-787.
- [74] Amine Boukhtouta, Serguei A. Mokhov, Nour-EddineLakhdari, MouradDebbabi and Joey Paquet, "Network malware classification comparison using DPI and flow packet headers," *Journal of Computer Virology and Hacking Techniques*, 2016, Volume 12, Issue 2, pp 69-100
- [75] GeetanjaliRathee and Hemraj Saini, "Mitigation Techniques for Gray Hole and Black Hole Attacks in Wireless Mesh Network," *Proceedings of the International Congress on Information and Communication Technology*, 2016, pp 383-392
- [76] Xiang Pan, Vinod Yegneswaran, Yan Chen, Phillip Porras, and 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 Kinkel, and 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] Wagner, Cynthia, et al. "MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform." *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 and P. Montefusco, "Security situation management - developing a concept of operations and threat prediction capability," *2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC)*, Prague, 2015, pp. 4C2-1-4C2-11.
- [81] A. Bouchami, E. Goettelmann, O. Perrin and C. Godart, "Enhancing Access-Control with Risk-Metrics for Collaboration on Social Cloud-Platforms," *2015 IEEE Trustcom/BigDataSE/ISPA*, Helsinki, 2015, pp. 864-871.
- [82] B. Liu and J. Bi, "DISCS: A DIStributed Collaboration System for Inter-AS Spoofing Defense," *2015 44th International Conference on Parallel Processing*, Beijing, 2015, pp. 160-169.

- [83] N. Arya, U. Singh and S. Singh, "Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm," *2015 International Conference on Computer, Communication and Control (IC4)*, Indore, 2015, pp. 1-5.
- [84] A. Sharma, D. Bhuriya and U. Singh, "Secure data transmission on MANET by hybrid cryptography technique," *2015 International Conference on Computer, Communication and Control (IC4)*, Indore, 2015, pp. 1-6.
- [85] E. Vasilomanolakis, M. Krügl, C. G. Cordero, M. Mühlhäuser and M. Fischer, "SkipMon: A locality-aware Collaborative Intrusion Detection System," *2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC)*, Nanjing, 2015, pp. 1-8.
- [86] Y. Zhang, F. Patwa and R. Sandhu, "Community-Based Secure Information and Resource Sharing in AWS Public Cloud," *2015 IEEE Conference on Collaboration and Internet Computing (CIC)*, Hangzhou, 2015, pp. 46-53.
- [87] Hong Liang, Yufei Ge, Wenjiao Wang and Lin Chen, "Collaborative intrusion detection as a service in cloud computing environment," *2015 IEEE International Conference on Progress in Informatics and Computing (PIC)*, Nanjing, 2015, pp. 476-480.
- [88] Á. MacDermott, Q. Shi and K. Kifayat, "Detecting Intrusions in Federated Cloud Environments Using Security as a Service," *2015 International Conference on Developments of E-Systems Engineering (DeSE)*, Duai, 2015, pp. 91-96.
- [89] Spyridon Papastergiou, Nineta Polemi and Athanasios Karantjias, "CYSM: An Innovative Physical/Cyber Security Management System for Ports," *International Conference on Human Aspects of Information Security, Privacy, and Trust*, 2015, pp 219-230
- [90] Freudiger, Julien, Emiliano De Cristofaro, and Alejandro E. Brito. "Controlled data sharing for collaborative predictive blacklisting." *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, Cham, 2015.
- [91] Takeshi Takahashi, Tao Ban, Takao Mimura and Koji Nakao, "Fine-Grained Risk Level Quantification Schemes Based on APK Metadata," *International Conference on Neural Information Processing*, 2015, pp 663-673
- [92] Cordero CG, Vasilomanolakis E, Mühlhäuser M, Fischer M. Community-Based Collaborative Intrusion Detection. In *SecureComm 2015* Oct 26 (pp. 665-681).
- [93] M. A. Nouredine, A. Marturano, K. Keefe, M. Bashir and W. H. Sanders, "Accounting for the Human User in Predictive Security Models," *2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC)*, Christchurch, New Zealand, 2017, pp. 329-338.

- [94] W. H. Sanders and J. F. Meyer, "Stochastic activity networks: Formal definitions and concepts," in *Lectures on Formal Methods and Performance Analysis*, ser. Lecture Notes in Computer Science, E. Brinksma, H. Hermanns, and J.-P. Katoen, Eds., vol. 2090. Springer Berlin Heidelberg, 2001, pp. 315–343.
- [95] S. Abraham and S. Nair, "A Novel Architecture for Predictive CyberSecurity Using Non-homogenous Markov Models," 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, 2015, pp. 774–781.
- [96] A. Oluwaseun, Z. Pavol, L. Dale, R. Ron, "An Analysis of CVSS v2 Environmental Scoring" Privacy, Security, Risk and Trust (PASSAT) Date: 9-11 Oct. 2011
- [97] M. Schiffman, "Common Vulnerability Scoring System (CVSS)," <http://www.first.org/cvss/>
- [98] Assad Ali, Pavol Zavarsky, Dale Lindskog, and 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 11 September 2017]
- [100] Y. Shi, S. Abhilash and K. Hwang, "Cloudlet Mesh for Securing Mobile Clouds from Intrusions and Network Attacks," 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, San Francisco, CA, 2015, pp. 109-118.
- [101] K. Hwang and D. Li, "Trusted Cloud Computing Resources and Data Coloring", IEEE Internet Co Vol.14, Sept. 2010.
- [102] Leau, Yu-Beng, and Selvakumar Manickam. "A novel adaptive grey verhulst model for network security situation prediction", *International Journal of Advanced Computer Science & Applications* 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 and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292-2303, 2016