A Software Defined Network based Security Assessment Framework for CloudIoT

Zhuobing Han, *Student Member, IEEE,* Xiaohong Li, *Member, IEEE,* Keman Huang, *Member, IEEE,* and Zhiyong Feng, *Member, IEEE*

***Abstract*—The integration of cloud and internet of things (IoT), named CloudIoT, has been considered as an enabler for many different applications. However, the suspicion about the security issue is one main concern that some organizations hesitate to adopt such technologies while some just ignore the security issue while integrating the CloudIoT into their business. Therefore, given the numerous choices of cloud-resource providers and IoT devices, how to evaluate their security level becomes an important issue to promote the adoption of CloudIoT as well as reduce the business security risks. To solve this problem, considering the importance of the business data in CloudIoT, we develop an end-to-end security assessment framework based on Software Defined Network (SDN) to evaluate the security level for the given CloudIoT offering. Specially, in order to simplify the network controls and focus on the analysis about the data flow through CloudIoT, we develop a three-layer framework by integrating SDN and CloudIoT, which consists of 23 different indicators to describe its security features. Then, the interviews from industry and academic are carried out to understand the importance of these features for the overall security. Furthermore, given the relevant evidences from the CloudIoT offering, the Google Brillo and Microsoft Azure IoT Suite, our framework can effectively evaluate the security level which can help the consumers for their CloudIoT selection.**

***Index Terms*—Cloud Computing, Internet of Things (IoT), CloudIoT, Software Defined Network (SDN), Security Assessment, Data-Security-Oriented.**

I. Introduction

THE Internet of Things (IoT) has recently emerged as a novel networking paradigm to connect a large amount of smart objects for data sharing and exchanging, so that we can measure, communicate and interact with the real physical world [1]. On the other hand, cloud computing has been accepted as a cost-effective approach for providing high performance computing and virtually unlimited storage resource [2], [3]. Therefore, the integration of these two complementary technologies, the sensor-capability from IoT and the computing-capability from Cloud, has been accepted as a novel IT paradigm, named CloudIoT [4], [5], [6], for many different applications, including smart grid [7], smart cities [8], healthcare [9], [10], video surveillance [11], environmental monitoring [12] etc. Actually, the CloudIoT is playing an important role for the current IT system, especially for the critical infrastructure. Considering the fact that information security has become increasing important for current IT environment [13] while we can observe many cyber attacks these years, for example, the Ukraine Power Grid Attacks in December 2015 resulting into power lost for a few hours electricity lost for around 1.4 million populations[1], the security of CloudIoT is no doubt an urgent issue for both industry and academic.

On the other hand, with the prosperity of the cloud and IoT these years, some CloudIoT solutions, such as Google Brillo[2], Microsoft Azure IoT Suit[3], have been developed for the consumers. Due to the complexity of the CouldIoT solutions, how to evaluate the security level is a non-trivial task for the consumers. Some organizations will hesitate to adopt such technology due to the suspicion about the security and the incomprehension of risk, which may harm the development of the related business as well as affect the acceptance of the CloudIoT. Conversely, some organizations may just integrated CloudIoT into their business without considering the security issue, resulting into high risk for them. Therefore, a methodology to assist the security assessment of the CloudIoT solutions is necessary for the consumers.

Recently, some researches on security assessment turn to focus on the security for the cloud-based applications [14], [15] or IoT environment [16], [17], [18]. Since they have been independently evolved, most of the existing approaches evaluate the security separately and expose some weak-points in openness and standardization [19]. Actually, since CloudIoT brings data from real world through IoT System, uses cloud services to deal with these data and then enables triggering actions into the real world, only focus on cloud or IoT is not comprehensive for assessing the secure data transmission, i.e., network security should be take into consideration. Due to the fact that legacy network architecture based on closed networks has a restriction on expanding to various services and interworking with other devices or services, an independent scheme to integrate the entire networks is needed [19].

As Software Defined Network (SDN) provides flexibility to manage the network by separating the control plane from the

Manuscript received Aug 15, 2017; revised Dec 04, 2017.

Z. Han and X. Li are with the Tianjin Key Laboratory of Advanced Networking (TANK), School of Computer Science and Technology, Tianjin University, Tianjin, China, 300350 (e-mail: {zhuobinghan, xiaohongli}@tju.edu.cn).

K. Huang is with the Sloan School of Management, Massachusetts Institute of Technology, Cambridge, USA (e-mail: keman@mit.edu).

Z. Feng is with the School of Computer Software, Tianjin University, Tianjin, China, 300350 (e-mail: zyfeng@tju.edu.cn).

[1]http://www.securityweek.com/ukraine-power-grid-attacks-part-2-year-campaign

[2]https://developers.google.com/brillo/

[3]https://www.microsoft.com/en-us/cloud-platform/internet-of-things-azure-iot-suite

data plane, the integration of SDN and CloudIoT enables more agile and scalable networks based on demand and a simplified and strain less network control. In a SDN, data plane devices are used as a packet forwarding device and leaving the network control management to a logically centralized system called controller [20]. The controller connects to the switch through a secured OpenFlow [21] channel and manages this switch via the OpenFlow protocol [22]. Several research works have been published on SDN-based architecture [23], [24], [25], [26].

Therefore, to solve these existing issues, this paper aims to offer an end-to-end security assessment approach for CloudIoT solution selection. Since CloudIoT will collect data from real-world and then use these data to enable further applications, based on the analysis of the data flow, we develop a SDN-based three-layer framework consisting of 23 different indicators to evaluate the data-security-oriented security for the CloudIoT solution. Then in order to assign the weight for these indicators, an online interview with researchers and practitioners is carried out and then three different methodologies, including AdaRank [27], analytic hierarchical process (AHP) [28] and weighted-mean, are used to integrate the survey to generate a crowd-wisdom weight for different indicators. Finally, given the document for the CloudIoT solution, the Google Brillo based on Google Cloud and Microsoft Azure IoT Suite based on Azure Cloud, we are success to identify the security-related evidences and map them into the framework so that we can get an overall security level to facilitate the selection for consumers. Hence, the main contribution of this paper is the first end-to-end data-security-oriented security assessment approach to assist the CloudIoT selection, consisting of:

- a SDN-based three-layer indicator framework for security level assessment,
- the methodology to integrate indicator weight learning and solutions' security-related evidences mapping to offer the real-world CloudIoT solution security assessment.

The rest of paper is organized as follows. Section II surveys the current efforts on security assessment. Section III presents our indicator framework. Section IV reports the interview weight learning process and results. Section V shows the security assessment for the two real-world solutions and discusses our findings. Section VI concludes this paper and proposes some future works.

II. Related Work

Generally, state-of-the-art CloudIoT security publications can be classified into the following categories. Many works in literature have surveyed Cloud and IoT security separately. A broad number of publications review cloud-security issues, challenges, as well as the auditing and assessment approaches, while some studies focus on the security concerns of IoT. In addition, and more related to our work, there are several cloud-based IoT researches and SDN-based IoT researches which aim to reveal the challenges and open issues in terms of security.

A. Cloud Security

Various studies have investigated the methodologies of cloud-security auditing and assessment. Pilevari et al. [29] present a model to assess the satisfaction of users of a given cloud service with two main stages: the first stage is a conceptual model consists of several attributes including security, efficiency and performance, adaptability, and cost; the second one is a Fuzzy Inference System (FIS) architecture which consists of five main rules and eleven inputs (the attributes). Taha et al. [30] propose an AHP-based framework to quantitatively compare, benchmark and rank the security level provided by different Cloud Service Providers (CSP) based on its Security Level Agreements (SLA) depending on Cloud user security requirements. Li et al. [31] adopt Multi-Fuzzy Comprehensive Evaluation (MFCE) and AHP method to assess the potential risk of cloud environment including asset, vulnerability , threat, and control measures. The result accurately reflects the overall safety condition of cloud platform.

There are also some works focus on reviewing the cloud security open issues and challenges. Abuhussein et al. [14] study security evaluation of cloud services by identifying and categorizing 17 attributes of cloud security and privacy. By comparing three cloud service providers: Amazon EC2, Microsoft Azure and Google AppEngine based on their attributes, consumers can get a better view of their security features. Subashini et al.[32] review the security issues based on the service delivery models of cloud computing. They present 14 security issues in SaaS and also make a general survey on PaaS and IaaS.

B. IoT Security

Most of the IoT security researches review the security issues within different frameworks. Zhang et al. [18] propose a four-level security index system including perceptual layer security, transport layer security, application layer security and Cloud Computing security. Fuzzy-AHP method is adopted to evaluate the selected indicators and to find the key indicators of the IoT security development. Farooq et al. [33] present a four layer architecture of IoT and set the main security goal to keep data confidentiality. Then they discussed 18 open security challenges which should be addressed at each layer. Finally, a security architecture of IoT with 11 security issues is proposed. Chen et al. [34] describe five types of IoT security requirements: RFID tag information security, wireless communications and information security, network transmission of information security, privacy protection, information processing security. Sathishkumar et al. [35] also lists several security concerns and privacy concerns of IoT. Three categories of security concerns are proposed: front-end sensors and equipment, network, and back-end of it systems. Sicari et al. [16] surveys 8 main security issues in IoT: authentication, confidentiality, access control, privacy, trust, enforcement, middleware and mobile. The existing solutions are provided as well to hint for future research. And in their work of [36] , an architecture for ensuring IoT security and data quality is introduced. As it is the common believe that it is important

to ensure the incoming data security, they design a reference system architecture to overcome the issues of data extraction, integration, standardized design and reconfiguration.

In addition, there are also some works deal with IoT security from different aspects such as device security, vulnerability scanning and security control related problems. Shipley et al. [37] proposes the thought of building security into the IoT bottom up and addresses five security issues throughout the device lifecycle: secure booting, access control, device authentication, fire-walling and IPS, and updates and patches. Markowsky et al. [38] represent three types of scanning for vulnerable devices in the internet of things to ensure adequate security. Hassanzadeh et al. [39] focus on the security control problems in IoT environment and proposed a framework for analyzing the effectiveness of security controls which can be used by security architects to design and deploy new systems.

C. The Integration of Cloud and IoT

Diaz et al. [5] survey the integration of IoT and cloud computing in three categories and make a summary of the existing proposals for cloud computing and IoT integration, as well as the challenges and open research issues. Botta et al. [40] review the literature survey on the integration of Cloud and IoT with a focus on their specific research challenges and show the research trend. Also they present the security related surveys which is a guide of our work in the security evidence collection. Henze et al. [41] present a UPECSI method providing an integrated solution for User-driven privacy enforcement for Cloud-based services in the IoT, which is a comprehensive approach to privacy in the cloud-based Internet of Things by taking individual end-users and developers of cloud services into consideration in the mean while. Gubbi et al. [1] propose a vision, architectural elements, and future directions of Cloud centric Internet of Things.

D. The Integration of SDN and IoT

Sood et al. [24] review the recent works of integrating SDN and IoT and discuss the opportunities and challenges in SDN and IoT integration in the perspective of security and scalability. Jararweh et al. [42] propose a software defined based IoT framework named SDIoT which is a concept model to accommodate large data produced from IoT objects. Olivier et al.[22], [26] present a security model for the IoT based on the SDN architecture with multiple SDN controllers. The security of the entire network is guaranteed by the concept of grid of security embedded in each controller to prevent attacks. Kim et al. [19] propose a safe data transmission architecture S-DTA based on ClouIoT by adopting some SDN technology. Due to the on-time bypassing data transmission scheme, S-DTA can provide efficient and secure data transmission to various IoT devices in cloud networks.

Though there are many researches to improve cloud and IoT security, and some researches begin to consider the CloudIoT and the integration of SDN and CloudIoT, how to quantitatively evaluate the overall security level of the CloudIoT is still an open issue and it is very necessary for the consumers to select the CloudIoT solution. Therefore, this paper aims to offer an end-to-end security level evaluation framework based on SDN for the CloudIoT solution to facilitate the selection.

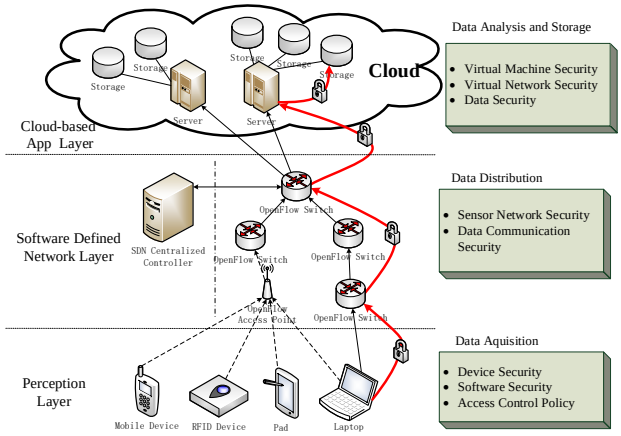

Fig. 1. The High-level Data Flow Diagram of SDN-based CloudIoT.

III. Data-Security-Oriented Security Assessment Index Framework

The typical architecture of CloudIoT consists of three layers: the Perception Layer, the Network and Transport Layer, and the Cloud-based Application Layer. In a CloudIoT system, the deployment data is acquired from sensor-equipped edge devices and aggregated on a wired or wireless network, then transport via a gateway to a public or private cloud, finally stored and analyzed on the cloud platform. Based on a basic thought of ensuring data security during the whole process of data flow and simplify the network control, decision making, and action implementation process, we proposed a SDN-based high-level data flow diagram (see Fig.1) and a data-security-oriented security assessment index framework based on SDN (see Fig.2). All these indicators have been observed and collected during the analysis of primary studies. The difference between the proposed architecture and the legacy architecture is the second layer, which is the Software Defined Network Layer instead of the Network and Transport Layer (detailed in Sec III-B).

A. Perception Layer Indicators

At the perception layer, data is acquired by the devices enabled by open wireless technology such as bluetooth, radio frequency identification (RFID), and telephonic data services as well as embedded sensors. Some of the RFID tags are used in retail applications and access control applications. For instance, the finger print data is usually used to unlock the device and deal with the payment. Therefore, three criterion of security issues should be taken into consideration to protect the data at this layer, i.e. ensure data security at the very beginning of the CloudIoT systems: device security, software security, and Access Control policy. Device security collects the security issues relevant to the embedded physical devices. Software security at this layer focuses on the security of software embedded in the IoT devices. Access control is the

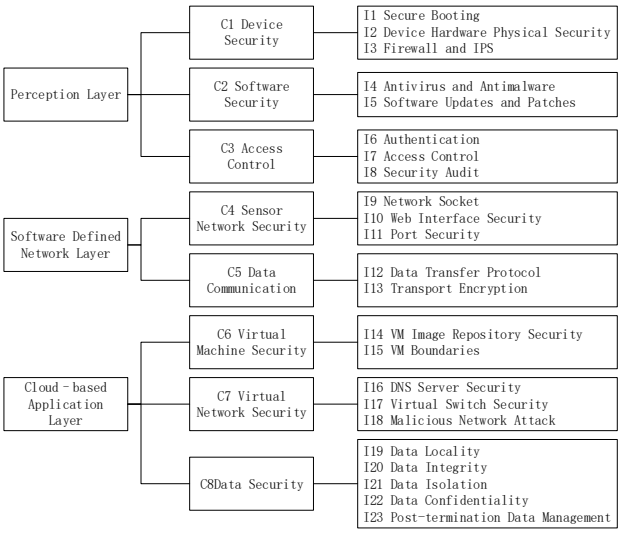

Fig. 2. Data-Security-Oriented Security Assessment Index Framework.

policy of assigning privileges to access the resources and data collected by devices and software at perception layer. Around these three criterion, 8 indicators are collected (see Fig. 2).

- **Secure Booting** (I_1) [37] Secure boot is a security standard used to help make sure that the device boots using only software that is verified by cryptographically generated digital signatures. When the device is plugged in for the fist time, the firmware should have the mechanism to check the signature of each piece of boot software.
- **Device Hardware Physical Security** (I_2) [35], [43], [44] Since data is received via sensors and equipment in devices, it is important to protect the physical security of multiple sensors so that to ensure data security at the very beginning. Thus physical security mechanisms ought to be provided by the providers.
- **Firewall and IPS** (I_3)[37], [33] In order to make sure the incoming network traffic is legitimate, preventative technical control mechanisms such as firewall and Intrusion Prevention System (IPS) should be provided in the IoT devices to filter the data.
- **Antivirus and Antimalware** (I_4) [33] Antivirus software and antimalware are software that used to prevent, detect and remove computer viruses and malicious software. The devices embedded in IoT systems should be equipped with antivirus software or antimalware to ensure the security of the system.
- **Software Updates and Patches** (I_5) [37] Software updates and patches are new software which can fix some bugs and issues. They should be delivered through the limited bandwidth and intermittent connectivity of an device in order to eliminate the security concerns.
- **Authentication** (I_6) [14], [35], [37], [33] Authentication is the process of verifying the validity of the identification by providing digital signatures to the terminals. IoT devices are suggested to provide authentication mechanisms such as dynamic passwords and biometrics identities.
- **Access Control** (I_7) [14], [35], [37] Access control is defined as system making a decision on whether to assign privileges or permissions to requested users for accessing system resources. IoT devices should be equipped with access control mechanisms.
- **Security Auditing** (I_8) [45] An audit trail provides records of the sequence of system activities which is also a security-relevant documentary evidence for stakeholders. Therefore, it is recommended that a security measurement is established in the system, in charge of inspecting, controlling, handling and auditing the security of the system.

B. Software Defined Network Layer Indicators

At the software defined network layer, control plane and data plane are decoupled (see Fig. 1), where the data plane is used to forwarding packets according to the forwarding tables prepared by the control plane in the controller [46]. The protocol adopted in this layer is OpenFlow [22], which works as follows: when a packet arrives at a switch, the switch evaluates the incoming flow to find whether there is a matching flow. If there is a match, the switch performs the associated action. If no match is found, the switch forwards the packet to controller for getting instructions on how to deal with the packet. The SDN controller populates the switch with flow table entries [24].

In order to keep the data security, strategies on sensor network security and data communication should be provided. Both of them are considered with the security issues during the process of spatially distributed sensors cooperatively pass the collected data through the network to a specific location. 5 indicators are discussed to refine these criterion at this layer (see Fig. 2).

- **Network Socket** (I_9) [32] A network socket is an endpoint of a connection across a network, which determines whether a local program can transport to the networking Application Programming Interface (API) to use the connection.
- **Web Interface Security** (I_{10}) [47] The web interface is an IP configuration front-end which can be accessed via web browsers on the internal network by authenticated users. Web interface security issues includes persistent cross-site scripting, poor session management and weak default credentials.
- **Port Security** (I_{11}) [34] Port security mechanisms is used to configure switch port with a unique list of MAC addresses of devices which are authorized to access the network via the port, which enables individual ports to detect, prevent, and log intrusions by unauthorized devices.
- **Data Transfer Protocol** (I_{12}) [14] Traditionally, a data transfer protocol is a standardized format for transmitting data between two devices. Cryptographic protocols such as FTPS (SSL), SFTP (SSH) and HTTPS protects the data when it travels over network. In SDN, the data transfer protocol is usually OpenFlow.

- **Transport Encryption** (I_{13}) [32] Transport encryption techniques encrypted all the communications at the beginning of information transferring through devices. Certain encryption algorithms should put on constrained devices to provide communications security during transport.

C. Cloud-based Application Layer indicators

At the Cloud-based Application Layer, data is stored and analyzed on the cloud due to its high reliability, scalability and autonomy to provide ubiquitous access. However, the virtual environment of cloud may bring security threats to user data. Thus, virtual machine security, virtual network security and data security should be taken into consideration. Since virtual machine security and virtual network security are key problems in cloud computing, especially at the Infrastructure as a Service (IaaS) layer, they must be considered in cloud-based IoT systems. Data security focuses on the data acquired from sensor-equipped devices, finally stored and analyzed on the cloud platform. Around these three criterion, 10 indicators are examined in order to analyze issues related to cloud-based application layer security (see Fig. 2).

- **VM Image Repository Security** (I_{14}) [48] The virtual-machine (VM) image may be attacked by malicious viruses or even stolen. Moreover, VM templates may contain information of previous users, which could be accesses by subsequent users. Since attackers may place a new image or produce poisoned images, scanning and filtering mechanisms are suggested to cloud providers.
- **VM Boundaries** (I_{15}) [49] The VMs are coexisted on the same server, so that they share resources with limited CPU and memory. As there is no physical isolation among VM resources, an artificial boundary for the virtual machine is the responsibility of the cloud providers.
- **DNS Server Security** (I_{16}) [50] When a DNS server resolves a DNS name request to an IP address, the response ought to exactly match the query. However, if the resolving server caches a malicious request, security problems may ensue. Thus DNS firewalls and the latest DNS software patches are suggested to ensure the DNS Server security.
- **Virtual-Switch Security** (I_{17}) [51] Virtual switches enable the specification of a logical network among a set of VMs. There are many types of virtual-switch security mechanisms, such as isolation and content inspection between VMs.
- **Malicious Network Attacks** (I_{18}) [32] Malicious network attacks may happen when user data transmitted via the virtual network with illegal access. Routine vulnerability scanners are suggested to mitigate malicious attacks.
- **Locality** (I_{19}) [14], [32] Data locality focuses on the storage location of the cloud data, the circumstances that data ever transferred from the cloud location, the location of management and control structures.
- **Integrity** (I_{20}) [35], [32], [33] Data integrity is the maintenance of the accuracy and consistency of data over its entire life-cycle. Service providers should provide some tracking methods to protect user information from unauthorized tampering during data transmission.
- **Isolation** (I_{21}) [14] Data isolation determines how transaction integrity is visible to other users and systems. In order to guarantee user transactions being independently executed, mechanisms on supporting data isolation such as the two-phase locking protocol should be provided by service providers.
- **Confidentiality** (I_{22}) [35], [37], [33] Data confidentiality focuses on the ability to protect user privacy and sensitive data which means only authorized users can get access to the data. There are several mechanisms to ensure data confidentiality such as virtual private networks (VPN) or physical media encryption.
- **Post-termination Data Management** (I_{23}) [14] Some cloud service providers may not erase the customer's data immediately when their contract expires. Post-termination data-management is a way of maintaining the client data and ensure the security of data before the client retrieve it or for a period of time.

IV. Index Weight Learning

Straightforwardly, we can employ the presented indicators to evaluate the security level for the CloudIoT. However, different indicators in different layers have different contributions for the overall security. Therefore, to get the weight for different indicators, in this section, an online interview with researchers and practitioners is carried out to assign the weight for these indicators based on their experiences. Then three different methodologies, including AdaRank [27], Analytic Hierarchical Process (AHP) [28] and weighted-mean, are used to integrate the survey to generate a crowd-wisdom weight.

A. Online Interview

A 13-item short-form[4] was constructed to survey the relative importance of the proposed CloudIoT security evaluation indicators. The survey was designed for use in obtaining the experts knowledge on CloudIoT security assessment and indicator importance ranking list, which includes 12 multi-item scale that assesses all the 8 criterion and 23 indicators. As the CloudIoT security is a specific knowledge and experience intensive domain, we should not use the general crowd sourcing platform such as Amazon Mechanical Turk[5] to hire people for interview. Instead, based on the online community focusing on the related domains, we succeed to invite 46 persons with an average of 7-year background in computer science or IT security to join our survey research, including 3 engineers from IT companies, 16 professors from different universities and 27 postgraduate students.

For each question, we use the well known Likert Scale [52] and ask every expert to rate each indicator's importance in five levels: "*Not at all*","*Weak*", "*Medium*","*High*","*Extremely High*". Finally, we can get their inputs for further analysis.

[4]https://sojump.com/jq/10302676.aspx
[5]https://www.mturk.com/mturk/welcome

Algorithm 1: The AdaRank Algorithm

Input: $S = \{(q_i, d_i, y_i)\}_{i=1}^{m}$, and parameters E and T
Output: Output ranking model: $f(\overrightarrow{x}) = f_T(\overrightarrow{x})$

Initialize $P_1(i) = 1/m$.
foreach $t = 1, \cdots, T$ **do**
- Create weak ranker h_t with weighted distribution P_t on training data S.
- Choose α_t, $\alpha_t = \frac{1}{2} \cdot \ln \frac{\sum_{i=1}^{m} P_t(i)\{1+E(\pi(q_i,d_i,h_t),y_i)\}}{\sum_{i=1}^{m} P_t(i)\{1-E(\pi(q_i,d_i,h_t),y_i)\}}$.
- Create f_t, $f_t(\overrightarrow{x}) = \sum_{k=1}^{t} a_k h_k(\overrightarrow{x})$.
- Update P_{t+1}, $p_{t+1}(i) = \frac{\exp\{-E(\pi(q_i,d_i,f_t),y_i)\}}{\sum_{j=1}^{m} \exp\{-E(\pi(q_j,d_j,f_t),y_j)\}}$.

TABLE I
ADARANK NOTATIONS AND EXPLANATIONS

Notations	Explanations
$q_i \in Q$	i^{th} query
$d_i = \{d_{i1}, d_{i2}, \cdots, d_{i,n(qi)}\}$	List of documents for q_i
$y_{ij} \in \{r_1, r_2, \cdots, r_t\}$	Rank of $d_{ij} w.r.t. q_i$
$y_i = \{y_{i1}, y_{i2}, \cdots, y_{i,n(qi)}\}$	List of ranks for q_i
$S = \{(q_i, d_i, y_i)\}_{i=1}^{m}$	Training set
$\overrightarrow{x}_{ij} = \Psi(q_i, d_{ij}) \in \aleph$	Feature vector for (q_i, d_{ij})
$f(\overrightarrow{x}_{ij}) \in \Re$	Ranking model
$\pi(q_i, d_i, f)$	Permutation for q_i, d_i, and f
$h_t(\overrightarrow{x}_{ij}) \in \Re$	t^{th} weak ranker
$E(\pi(q_i, d_i, f), y_i) \in [-1, +1]$	Performance measure function

B. Learning Methods

Note that the inputs from experts may be affected from their experiences and will result into the bias. In order to get a more objective weights, we use three different methodologies, including AdaRank [27], Analytic Hierarchical Process (AHP) [28] and weighted-average, to integrate the survey to generate a crowd-wisdom weight for different indicators.

1) Learning To Rank: Firstly, the result of the survey can be extracted as a 23×46 matrix and each element is a score of the question item given by participants, ranged from $1, 5$. Therefore, it can be considered as the ranking for these 23 items so that we can use the learning to rank algorithms [53] to learn the weight for each indicators. Specially, in our context, we consider the inputs from the survey as the training dataset and the results from industry participants and professors as the label due to their experience. Then the AdaRank [27] algorithm is used as a library of to train the weights. Since we are not focusing on the algorithm, we only report the algorithm process in Algorithm 1). Finally, the layer weight is generated by normalization the average score of the indicators in each level.

2) Analytic Hierarchy Process (AHP): Secondly, Analytic Hierarchy Process (AHP) [54], [28] is a hierarchical decision analysis method for assigning weights to multi-factor problems. AHP is based on pair-wise comparison of the relative importance of each variables, which allows the decision maker to determine the trade-offs among the various criteria under consideration. The AHP methodology consists of four steps: problem decomposition, prioritization, priority aggregation, and consistency verification.

TABLE II
0-2 SCALE OF RELATIVE IMPORTANCE

Scale	Definition
0	Parameter i is less important than parameter j
1	The two parameters are of equally importance
2	Parameter i is more important than parameter j

TABLE III
RANDOM CONSISTENCY INDEX TABLE

n	1	2	3	4	5	6	7	8	9
RI	0.0	0.0	0.58	0.89	1.12	1.24	1.32	1.41	1.45

Step 1: Problem Decomposition The first step for AHP is to map the situation into a hierarchical structure. In our context, the hierarchical structure is generally divided into three levels: Layer level, criterion level and indicator level.

Step 2: Prioritization In traditional AHP method, each variable is assigned a relative weight by comparing it against the others, in a 1-9 scale to indicate its importance [54]. However, it is difficult for experts and participants to make such precise numerical assignments. Therefore, we adopt an improved AHP method with 0-2 scale [28] to overcome this shortcoming (see Table II). By calculating the importance order index $x_i = \sum_{i=1}^{n} C_{ij}, i = 1, 2 \cdots n$, the elements in pairwise comparison matrix can be established by (1). Therefore, in this paper, we do pairwise comparisons between the average scores of each indicators (or criterion,layers) by the 46 participants with 0-2 scale.

$$a_{ij} = \begin{cases} \frac{x_i - x_j}{x_{\max} - x_{\min}} (a_m - 1) + 1, x_i \geq x_j \\ 1, x_{\max} = x_{\min} \\ \left[\frac{x_j - x_i}{x_{\max} - x_{\min}} (a_m - 1) + 1 \right]^{-1}, x_i < x_j \end{cases} \quad (1)$$

where $a_m = x_{\max}/x_{\min}$.

Step 3: Priority Aggregation The relative weights is obtained by the *root mean square (RMS)* method, which is used to calculate the eigenvectors of the pairwise comparison matrix generated by Step 1.

1) Normalize each column of the pairwise comparison matrix $\overline{w_i} = \sqrt[n]{\sum_{j=1}^{n} a_{ij}}$.
2) Normalize the vector $w = (w_1, w_2, \cdots, w_n)^T$.
$$w_i = \frac{\overline{wi}}{\sum_{i=1}^{n} \overline{wi}}, \mathrm{i} = 1, 2, \ldots \mathrm{n} \quad (2)$$
where $W_i = (w_1, w_2, \cdots, w_n)^T$ is the eigenvector.
3) Calculate the maximum eigenvalue $\lambda_{\max}$ of the matrix.
$$\lambda_{\max} = \frac{1}{n} \sum_{i=1}^{n} \frac{(Aw)_i}{w_i} \quad (3)$$
where, A is the pairwise comparison matrix and $(Aw)_i$ is the ith element of matrix Aw.

Step 4: Consistency Verification Finally, to verify whether the matrix is consistent, the consistency ratio $CR = CI/RI$ is calculated. CI is the consistency index $CI = \frac{\lambda_{\max} - n}{n-1}$. RI is a *Random Index*, randomly generated for a matrix of size n (see Table III). When CR is less than or equal to 0.1, the result is acceptable.

TABLE IV
COMPARING THE RESULTS BY THREE DIFFERENT RANKING METHODS WITH ALL THE PARTICIPANTS DATA.

ID	Indicators	Ranking Results			
		W_Mean	AHP	LTR	Average
A1-C1-I1	Secure Booting	23	23	23	23
A1-C1-I2	Device Hardware Physical Security	22	22	20	22
A1-C1-I3	Firewall and IPS	21	16	19	21
A1-C2-I4	Antivirus and Antimalware	20	19	18	20
A1-C2-I5	Software Updates and Patches	19	9	22	18
A1-C3-I6	Authentication	18	17	16	19
A1-C3-I7	Access Control	16	6	14	15
A1-C3-I8	Security Audit	17	11	21	17
A2-C4-I9	Network Socket	13	13	3	16
A2-C4-I10	Web Interface Security	10	8	5	10
A2-C4-I11	Port Security	9	3	4	5
A2-C5-I12	Data Transfer Protocol	2	1	1	1
A2-C5-I13	Transport Encryption	3	2	2	2
A3-C6-I14	VM Image Repository Security	14	10	9	12
A3-C6-I15	VM Boundaries	15	20	13	14
A3-C7-I16	DNS Server Security	12	18	10	13
A3-C7-I17	Virtual Switch Security	11	12	17	11
A3-C7-I18	Malicious Network Attack	8	7	8	9
A3-C8-I19	Data Locality	7	21	12	8
A3-C8-I20	Data Integrity	5	14	15	6
A3-C8-I21	Data Isolation	4	5	11	4
A3-C8-I22	Data Confidentiality	1	4	7	3
A3-C8-I23	Post-termination Data Management	6	15	6	7

3) Weighted Mean: Thirdly, weighted average is the simplest and most easy to assign importance weight to each indicator. In this paper, we assign the equal weight to each participant so that for each indicator, criterion and layer we can get an average score. Note that the final weight for each indicator will be affected by its hierarchical structure. Additionally, the score for the layer is more important than the criterion while the criterion score is more informative than the leaf indicator. Therefore, we simply assign wights to the hierarchical levels as follows: layer level $3/6$, criterion level $2/6$, and indicator level $1/6$. Finally, we can get the weight for each indicator as follow:

$$Weight\_mean = \sum_{k=1}^{N} \xi_k X_k\left(t\right) \tag{4}$$

Where,$X_k\left(t\right)$ refers to the average score from survey for each indicator in different hierarchical level, and ξ_k are chosen weight which satisfied: $\sum_{k=1}^{N} \xi_k = 1(\xi_k > 0, k = 1, \cdots, N)$.

C. Results and Discussions

Based on the survey, in this section, we will discuss the consistent observations from different methodologies as well as different groups to understand the different importance for the indicators.

TABLE V
PEARSON CORRELATION COEFFICIENT FOR RESULTS BY THREE DIFFERENT RANKING METHODS (N=23)

Correlation		W_Mean	AHP	LTR
W_Mean	Pearson Correlation	1	**0.628****	**0.765****
	Sig. (2-tailed)	-	0.001	0.000
AHP	Pearson Correlation	**0.628****	1	**0.602****
	Sig. (2-tailed)	0.001	-	0.002
LTR	Pearson Correlation	**0.765****	**0.602****	1
	Sig. (2-tailed)	0.000	0.002	-

**. Correlation is significant at the 0.01 level (2-tailed).

Q1: indicator Weight from Different Methodologies

TABLE VI
COMPARING DIFFERENT GROUP OF PARTICIPANTS WITH LTR (ADARANK)

ID	Indicator Name	Ranking Results			
		Overall	Industry	Prof.	Stu.
A1-C1-I1	Secure Booting	23	23	12	15
A1-C1-I2	Device Hardware Physical Security	20	19	20	18
A1-C1-I3	Firewall and IPS	19	20	18	13
A1-C2-I4	Antivirus and Antimalware	18	10	22	21
A1-C2-I5	Software Updates and Patches	22	14	19	22
A1-C3-I6	Authentication	16	17	16	9
A1-C3-I7	Access Control	14	13	2	12
A1-C3-I8	Security Audit	21	11	5	16
A2-C4-I9	Network Socket	3	15	15	6
A2-C4-I10	Web Interface Security	5	3	6	7
A2-C4-I11	Port Security	4	4	8	5
A2-C5-I12	Data Transfer Protocol	1	2	1	2
A2-C5-I13	Transport Encryption	2	1	4	1
A3-C6-I14	VM Image Repository Security	9	16	11	8
A3-C6-I15	VM Boundaries	13	6	17	23
A3-C7-I16	DNS Server Security	10	21	7	10
A3-C7-I17	Virtual Switch Security	17	22	10	19
A3-C7-I18	Malicious Network Attack	8	9	14	11
A3-C8-I19	Data Locality	12	7	23	14
A3-C8-I20	Data Integrity	15	12	13	17
A3-C8-I21	Data Isolation	11	8	3	20
A3-C8-I22	Data Confidentiality	7	5	9	4
A3-C8-I23	Post-termination Data Management	6	18	21	3

Given the inputs from the 46 experts, based on the three approaches discussed in Section 4.2, we can calculate the weight for each indicator and then rank them according to it. As reported in Table IV, the first column represents the indicator ids. Label A, C, and I are for the three levels (later, criterion and indicator). The second column shows the term of indicators. The rest columns are the weight in ranking. It can be seen that though there are some differences in detail ranking, we can achieve the following consistent observations:

- The security of SDN Layer (A2) and Cloud-based Application Layer (A3) are considered much more important than the Perception Layer (A1). It can be seen that the ranking for the eight indicators in perception layer is much lower than the indicators in the other two layers. Most of these indicators are ranked in the bottoms, only the *Access Control* and *Software Updates and Patches* are rated in Top 10 in the AHP approach.
- The two indicators from Data Communication (A2-C5) are listed top 3 by the three approaches. Therefore, how to guarantee the data security during the transportation is the biggest concern for the consumers to select the CloudIoT solutions.
- Devices security (A1-C1) and the embedded software security (A1-C2) are regarded as the least important indicators by the participants, which is consistent in the three approaches. This means that the customers currently highly trust the physical security of the CloudIoT system.

Furthermore, to test the consistence of the ranking among these three approaches, we calculate the cosine similarity and the Pearson correlation coefficient between them. As reported in Table V, it can be seen that these three ranking are highly relevant, with a cosine similarity larger than 0.9 and the Pearson correlation coefficient are at least 0.602, which are all significant at the 0.01 level. Therefore, these results are consistent and in the following discussion, we will only use the result from AdaRank to show the differences between different groups.

Q2: Differences Between Different Groups

Taking the result from LTR as an example, beside the overall score, we can further calculate the ranking which are based

on the different groups, i.e. Industry, Professor and Student. The results from Table VI shows that:

- All the three groups agree that the "Data Communication (A2-C5)" are top priority for the security. "Device Security (A1-C1)" and "Software Security (A1-C2)" are all rated with relative lower positions. These are consistent with the overall observations.
- Comparing with the other two groups, the Professors consider the "Access Control (A1-C2)" as very important features for the security, while the participants from industry and the students give them a relative lower rating. Furthermore, for the "Data Isolation", which is important for the privacy, the professor group and the industry group have a much higher rating than the student group. Conversely, the student group give the "Authentication" and "Network Socket" much higher rating than the professor and industry group.

Therefore, based on the experiments, we can see that the group's background will affect the ranking about the indicators. We will further discuss the observations in Section 6. Since the rankings about the weight for different indicators from three approaches are consistent, we will use the average of these three approaches for the further solution security level assessment.

V. CloudIoT Solution Security Level Assessment: Case Study

Until now we already get the different weights for different indicators representing their importances for the overall security. Therefore, given a CloudIoT solution, we can map its security-related mechanism into the framework to figure out whether they offer the necessary security guarantee. Since we offer its definition for each indicator, we can use the related key words to search over the solution's description documents to find the related security mechanisms. Then for each found mechanism, we can further evaluate its relevance to the indicator. To assess this relevance, similarly, we invite 5 security experts chosen from the survey participants, then show them the related evidence and ask them to remark the relevance in "Low", "Medium" and "High", which represents the degree that the solution can solve the security concern. Finally we can get the ranking based on the input from these experts and then calculate the overall security score by multiplying the indicators' weights and the covered degree.

To proof the effectiveness of this framework, in this section, we demonstrate how our framework can offer the end-to-end CloudIoT solution security assessment, we use the following two real-world CloudIoT offering as the cases:

- Google Brillo is an OS for low-powered Internet of Things (IoT) devices with three elements: Android-based embedded OS, core platform services, and a developer kit. Google Brillo is about the smart home, which comes hand-in-hand with Google's new communications protocol called Google Wave Federation Protocol[6]. Googles Brillo OS will run on devices with 64 or 32 MB of RAM and that it will launch under the Android brand. The data storage and processing center for this IoT service can be the Google cloud, including the Google Compute Engine (GCE), the Google App Engine (GAE).
- Azure IoT Suite is a set of cloud-based services built on the flexible and scalable Microsoft Azure Cloud Platform, which is about the business. The Azure IoT Suite is designed to integrate with the existing processes, devices, and systems to enable users to analyze and mine disparate data with worldwide availability of the Microsoft Cloud Platform, which including Azure's Linux virtual machine, Azure's new "cloud services".

These two CloudIoT offers both provide the official, publicly available security documentations so that we can find the related evidences, explaining how these providers address the concern related to each indicator. Some examples of the evidences are listed in Table VII and the whole list is in the link [7]. Finally, we can generate the ranking for these indicators for each solution, which is shown in Table VIII. It can be seen that:

- The indicators at software defined network layer rank the top, which is consistent with the learning results present in Section IV. The average score shows that the eight indicators in the Perception layer (A1) and the "Network Socket(A2-C4-I9)" occupy the bottom 9 positions. Goolge Brillo contains 4 bottom indicators and Azure IoT Suite has five. However, for Google Brillo, it can be seen that the "Authentication" (A1-C3-I6) has a related top position. This indicates that at the perception layer, neither of these two solutions pays many attentions while Google Brillo may have a better security level than the Azure IoT Suite.
- Comparing the two solution in the cloud-based application layer, it is obviously that the Azure CloudIoT has a better security-related performance: four indicators in "Data Security" except the "Data Locality" gain the top positions while these indicators have a high importance. However, for the same level, all the indicators for Google Brillo are lower than top 8. It indicates that for the security level in the "Data security" criterion in the Cloud-based application layer, Azure CloudIot has a better performance than Google Brillo. Actually, Azure CloudIoT has a higher overall score than the Google Brillo. The Pearson correlation testing shows that the ranking of the indicators for Azure has a significant positive correlation with the indicator importance ranking, $r = 0.574, p = 0.004$. However, the correlation between Google Brillo and the indicator importance ranking cannot pass the testing. Hence, we can conclude that overall, Azure IoT Suite has a better security level than Google Brillo. This is consistency with our previous work on assessing cloud security [55].
- Comparing the two solutions with the indicator importance ranking, Azure IoT has a related weakness in "Port Security", "Virtual Switch Security" and "DNS Server Security" as it has a significant gap between

[6]www.waveprotocol.org/

[7]https://www.overleaf.com/6848614vxbfhcbddfyb

TABLE VII
PRIORITY WEIGHTS AND EVIDENCE ANALYSIS FOR CASE STUDIES

Index	Google Brillo	Azure IoT Suite
I_1	Google Brillo is embedded in Android which has gotten Verified (or secure) boot feature that originally appeared in the Android 4.4.	Azure IoT Hub provides monitoring information like connection status (connected/disconnected) and last activity time.
I_2	Google plan to encrypt user data on Android devices by default. Android 6.0, the Android Compatibility Definition Document (CDD) lists full-disk encryption as a requirement.	Azure IoT Hub has an identity registry where it stores all information about provisioned devices.
I_3	Users can install a firewall manually.	Azure SQL server uses firewall rules to allow connections to user devices.

TABLE VIII
ASSESSMENT BASED ON GOOGLE BRILLO AND AZURE IOT SUITE.

ID	Indicators	Ranking Results		
		Google Brillo	Azure IoT	Average
A1-C1-I1	Secure Booting	11	18	23
A1-C1-I2	Device Hardware Physical Security	10	19	22
A1-C1-I3	Firewall and IPS	22	20	21
A1-C2-I4	Antivirus and Antimalware	23	22	20
A1-C2-I5	Software Updates and Patches	20	11	18
A1-C3-I6	Authentication	8	12	19
A1-C3-I7	Access Control	14	17	15
A1-C3-I8	Security Audit	17	10	17
A2-C4-I9	Network Socket	5	2	16
A2-C4-I10	Web Interface Security	3	3	10
A2-C4-I11	Port Security	4	13	5
A2-C5-I12	Data Transfer Protocol	2	8	1
A2-C5-I13	Transport Encryption	1	1	2
A3-C6-I14	VM Image Repository Security	16	9	12
A3-C6-I15	VM Boundaries	13	15	14
A3-C7-I16	DNS Server Security	7	21	13
A3-C7-I17	Virtual Switch Security	18	23	11
A3-C7-I18	Malicious Network Attack	6	16	9
A3-C8-I19	Data Locality	15	14	8
A3-C8-I20	Data Integrity	9	5	6
A3-C8-I21	Data Isolation	19	4	4
A3-C8-I22	Data Confidentiality	21	6	3
A3-C8-I23	Post-termination Data Management	12	7	7
	Overall Score	27.0441	27.7753	

its ranking to the indicator importance ranking. On the other hand, for the Google Brillo, the weakness locates in "Data Isolation" and "Data Confidentiality". Good news is that Google Brillo has a better performance in "Authentication" in the perception layer. Hence, it can has a related better performance than Azure IoT in defending the cyberattack to the IoT devices.

Therefore, the result from the two cases shows that our framework can finally help the consumer to compare the security level of the offered solution with a overall security score. Also, it can also identify the weaknesses so that the providers can have a guide to improve their solution's security.

A. Discussion

Since our approach aims at providing an overall evaluation result for a given CloudIoT offering in terms of security, we can also help the customer who seeks to use offerings with specific security requirements. In such cases, some indicators from our indication framework are obviously important, while others are obviously irrelevant. The weights learned in Section III are no longer suitable but a customized weights can be generated in the same way as in our approach. A set of survey questions about the specialized use case can be formulated, weights can be assigned to the questions responses according to the security needs, and various analysis approaches can again be adopted to formulate a crowd-reviewed ranking of the responses.

Due to the complexity of the CloudIoT platform, there are numerous indicators affect the security assessment of the CloudIoT offerings besides our indication framework, for example, the number and severity of major security incidences, as well as the number and scale of the CloudIoT deployment. These indicators also provide measures of the readiness of the CloudIoT offering for deployment, as well as the popularity of the offering. However, our approach is data-security-oriented, we design the framework based on a basic thought of ensuring data security during the whole process of data flow and simplify the network control, decision making, and action implementation process.

Additionally, based on our experiment, it can be seen that overall, the security for the perception layer is considered as low priority while two solutions also offer few mechanisms to guarantee this layer's security. However, on October 21, 2016, massive amounts of the Internet in USA have been shut down by the huge DDOS attack. One of the sources of traffic of the attacks came from the Mirai botnet, which consists of millions of infected IoT and smart home devices[8]. This October-21 DDos attack ring the bell for the whole society, including academic and industry, to pay attention to the security of the perception layer. Good new is that our experiment shows that the professor group give a related higher rating for this layer. Google Brillo solution pays a specific attention to the "Authentication" for defending the cyberattack to the IoT devices. However, it is still a far way to go for the security of CloudIoT.

B. Threat to Validity

There are internal and external threats that may potentially affect the validity of our experiments.

1) Threats to internal validity: relate to errors in our experimental dataset and methodology implementation. We avoid such errors by having implementation and experiment results double checked by co-authors. We have also manually checked the statistics data in our interview and the scores by security experts to ensure that they have matched with the right value and values are assigned to the right indicators.

2) Threats to external validity: relate to the generalizability of our results. In this study, we assume that a business consumer can get access to cybersecurity experts who can use the proposed assessment framework to evaluate candidate CloudIoT offerings. We have a small-sized applicants in the

[8]http://www.zonealarm.com/blog/2016/10/how-internet-shut-down-ddos-attack-dyn/

interview and the number of security experts are limited, which may lead to bias. Besides, the reliance on specifications of the CloudIoT offering recovered from the security technical documentation leads to the possibility that vague or incomplete documentation may affect the security assessment. These allows us to perform manual analysis to understand the capability and limitations of our approach. We will reduce this threat by expanding the scope of the interview and introducing semantic analysis into the framework to automatically identify the evidence from the solution description documents to facilitate the assessment process in the future.

VI. Conclusion and Future Work

The integration of cloud computing and Internet of things (IoT) motivate the emergence of the CloudIoT. Since the security has become one important issue for its adoption, how to evaluate the security level of the offered solution is valuable and necessary for consumers. In this paper, based on the analysis about the data flow over the CloudIoT, we propose a SDN-based three-layer indication framework consisting of 23 indicators. To evaluate the importances of these indicators, we construct the online survey research to invite experts from researchers and practitioners to rate the indicators and then three different methodologies to generate the aggregate rating are used to gain the weights. Given the weights for different indicators, taking the two real-world CloudIoT solutions as an example, we identify the evidences for the related security mechanisms so that we can figure out how the solutions offer the security guarantee for customers. Therefore, we can offer the consumer the end-to-end approach to compare the security level of different solutions as well as to identify the weakness for the solution providers.

In the future, we will expand the scope of the interview and the cases, not only to understand the current security status of the CloudIoT ecosystem but also to make the indicator framework more comprehensive. Also, we are intending to introduce the semantic analysis into the framework to automatically identify the evidence from the solution description documents to facilitate the assessment process.

Acknowledgment

This work has partially been sponsored by the National Science Foundation of China (No. 61272106, 61572349). Xiaohong Li is the corresponding author.

References

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013. [Online]. Available: http://dx.doi.org/10.1016/j.future.2013.01.010

[2] M. Armbrust, A. Fox, R. Griffith, A. Joseph, and RH, "Above the clouds: A Berkeley view of cloud computing," *University of California, Berkeley, Tech. Rep. UCB*, pp. 07–013, 2009.

[3] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Computer Systems*, vol. 25, no. June 2009, p. 17, 2009.

[4] A. Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of Cloud computing and Internet of Things: A survey," *Future Generation Computer Systems*, vol. 56, pp. 684–700, 2016.

[5] M. Díaz, C. Martín, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing," *Journal of Network and Computer Applications*, pp. 1–19, 2015.

[6] J. Zhou, T. Leppanen, E. Harjula, M. Ylianttila, T. Ojala, C. Yu, and H. Jin, "CloudThings: A common architecture for integrating the Internet of Things with Cloud Computing," *Proceedings of the 2013 IEEE 17th International Conference on Computer Supported Cooperative Work in Design, CSCWD 2013*, pp. 651–657, 2013.

[7] M. Yun and B. Yuxin, "Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid," in *2010 International Conference on Advances in Energy Engineering, ICAEE 2010*, 2010, pp. 69–72.

[8] I. Podnar Zarko, A. Antonic, and K. Pripužic, "Publish/subscribe middleware for energy-efficient mobile crowdsensing," *Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication - UbiComp '13 Adjunct*, pp. 1099–1110, 2013.

[9] A. Forkan, I. Khalil, and Z. Tari, "CoCaMAAL: A cloud-oriented context-aware middleware in ambient assisted living," *Future Generation Computer Systems*, vol. 35, pp. 114–127, 2014. [Online]. Available: http://dx.doi.org/10.1016/j.future.2013.07.009

[10] G. Fortino, D. Parisi, V. Pirrone, and G. Di Fatta, "BodyCloud: A SaaS approach for community Body Sensor Networks," *Future Generation Computer Systems*, vol. 35, pp. 62–79, 2014. [Online]. Available: http://dx.doi.org/10.1016/j.future.2013.12.015

[11] A. Prati, R. Vezzani, M. Fornaciari, and R. Cucchiara, "Intelligent Video Surveillance as a Service," *Intelligent Multimedia Surveillance: Current Trends and Research*, vol. 9783642415, no. November 2013, pp. 1–16, 2013.

[12] M. T. Lazarescu, "Design of a WSN platform for long-term environmental monitoring for IoT applications," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 3, no. 1, pp. 45–54, 2013.

[13] R. Anderson and T. Moore, "The economics of information security," *Science*, vol. 314, no. 5799, pp. 610–613, 2006.

[14] A. Abuhussein, H. Bedi, and S. Shiva, "Evaluating Security and Privacy in Cloud Computing Services: A Stakeholder's Perspective," *Internet Technology And Secured Transactions*, pp. 388–395, 2012.

[15] M. Sookhak, A. Gani, H. Talebian, A. Akhunzada, S. U. Khan, R. Buyya, and A. Y. Zomaya, "Remote Data Auditing in Cloud Computing Environments: A Survey, Taxonomy, and Open Issues," *ACM Computing Surveys*, vol. 47, no. 4, pp. 65:1–65:34, 2015.

[16] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2014.11.008

[17] H. Yu, J. He, T. Zhang, P. Xiao, and Y. Zhang, "Enabling end-to-end secure communication between wireless sensor networks and the Internet," *World Wide Web*, vol. 16, no. 4, pp. 515–540, 2013.

[18] B. Zhang, Z. Zou, and M. Liu, "Evaluation on security system of internet of things based on Fuzzy-AHP method," in *E-Business and E-Government (ICEE),*, 2011, pp. 2230–2234. [Online]. Available: http://dx.doi.org/10.1109/ICEBEG.2011.5881939

[19] S. Kim and W. Na, "Safe data transmission architecture based on cloud for internet of things," *Wireless Personal Communications*, vol. 86, no. 1, pp. 287–300, 2016.

[20] K. S. Sahoo, B. Sahoo, and A. Panda, "A secured sdn framework for iot," in *Man and Machine Interfacing (MAMI), 2015 International Conference on*. IEEE, 2015, pp. 1–4.

[21] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "Openflow: enabling innovation in campus networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69–74, 2008.

[22] O. Flauzac, C. González, A. Hachani, and F. Nolot, "Sdn based architecture for iot and improvement of the security," in *Advanced Information Networking and Applications Workshops (WAINA), 2015 IEEE 29th International Conference on*. IEEE, 2015, pp. 688–693.

[23] B.-L. Cai, R.-Q. Zhang, X.-B. Zhou, L.-P. Zhao, and K.-Q. Li, "Experience availability: tail-latency oriented availability in software-defined cloud computing," *Journal of Computer Science and Technology*, vol. 32, no. 2, pp. 250–257, 2017.

[24] K. Sood, S. Yu, and Y. Xiang, "Software-defined wireless networking opportunities and challenges for internet-of-things: A review," *IEEE Internet of Things Journal*, vol. 3, no. 4, pp. 453–463, 2016.

[25] C. Vandana, "Security improvement in iot based on software defined networking (sdn)," *International Journal of Science, Engineering and Technology Research (IJSETR)*, vol. 5, no. 1, 2016.

[26] F. Olivier, G. Carlos, and N. Florent, "New security architecture for iot network," *Procedia Computer Science*, vol. 52, pp. 1028–1033, 2015.
[27] J. Xu and H. Li, "AdaRank: a boosting algorithm for information retrieval," in *Proceedings of the 30th annual international ACM SIGIR conference on Research and development in information retrieval*, no. 49, 2007, pp. 391–398.
[28] Q. Zhang and M. Zhong, "Using multi-level fuzzy comprehensive evaluation to assess reservoir induced seismic risk," *Journal of Computers*, vol. 6, no. 8, pp. 1670–1676, 2011.
[29] N. Pilevari and M. Sanaei, "A Framework for Evaluating Cloud Computing User ' s Satisfaction in Information Technology Management," vol. 1, no. 4, pp. 231–240, 2011.
[30] A. Taha, R. Trapero, J. Luna, and N. Suri, "AHP-based quantitative approach for assessing and comparing cloud security," *Proceedings - 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2014*, pp. 284–291, 2015.
[31] M. Li and M. Bardi, "A risk assessment method of cloud computing based on multi-level fuzzy comprehensive evaluation," in *Cyberspace Technology (CCT 2014), International Conference on*. IET, 2014, pp. 1–4.
[32] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, 2011.
[33] M. U. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A critical analysis on the security concerns of internet of things (iot)," *International Journal of Computer Applications*, vol. 111, no. 7, pp. 1–6, 2015.
[34] C. Qiang, G.-r. Quan, B. Yu, and L. Yang, "Research on security issues of the internet of things," *International Journal of Future Generation Communication and Networking*, vol. 6, no. 6, pp. 1–10, 2013.
[35] J. Sathishkumar and D. R. Patel, "A survey on internet of things: Security and privacy issues," *International Journal of Computer Applications*, vol. 90, no. 11, pp. 20–26, 2014.
[36] S. Sicari, C. Cappiello, F. D. Pellegrini, D. Miorandi, and A. Coen-Porisini, "A security-and quality-aware system architecture for internet of things," *Information Systems Frontiers*, pp. 1–13, 2014.
[37] A. Shipley, "Security in the internet of things: Lessons from the past for the connected future," in *Wind RIver*, 2013, pp. 1–5.
[38] L. Markowsky and G. Markowsky, "Scanning for vulnerable devices in the internet of things," in *Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2015 IEEE 8th International Conference on*, vol. 1. IEEE, 2015, pp. 463–467.
[39] A. Hassanzadeh, S. Modi, and S. Mulchandani, "Towards effective security control assignment in the Industrial Internet of Things," *IEEE World Forum on Internet of Things, WF-IoT 2015 - Proceedings*, pp. 795–800, 2016.
[40] A. Botta, W. de Donato, V. Persico, and A. Pescapé, "N/A - On the Integration of Cloud Computing and Internet of Things," *Future Generation Computer Systems*, vol. 56, pp. 23–30, 2013.
[41] M. Henze, L. Hermerschmidt, D. Kerpen, R. Häußling, B. Rumpe, and K. Wehrle, "A comprehensive approach to privacy in the cloud-based Internet of Things," *Future Generation Computer Systems*, vol. 56, pp. 701–718, 2016. [Online]. Available: http://dx.doi.org/10.1016/j.future.2015.09.016
[42] Y. Jararweh, M. Al-Ayyoub, E. Benkhelifa, M. Vouk, A. Rindos *et al.*, "Sdiot: a software defined based internet of things framework," *Journal of Ambient Intelligence and Humanized Computing*, vol. 6, no. 4, pp. 453–461, 2015.
[43] X. Wang, Y. Zhang, V. Leung, N. Guizani, and T. Jiang, "D2d big data: Content deliveries over wireless device-to-device sharing in realistic large scale mobile networks," *IEEE Wireless Commun.*, vol. 25, no. 1, pp. 1–10, 2018.
[44] X. Wang, Z. Sheng, S. Yang, and V. C. Leung, "Tag-assisted social-aware opportunistic device-to-device sharing for traffic offloading in mobile social networks," *IEEE Wireless Communications*, vol. 23, no. 4, pp. 60–67, 2016.
[45] C. G. W. Group *et al.*, "National information assurance (ia) glossary," *CNSS Instruction*, no. 4009, 2006.
[46] R. Jain and S. Paul, "Network virtualization and software defined networking for cloud computing: a survey," *IEEE Communications Magazine*, vol. 51, no. 11, pp. 24–31, 2013.
[47] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," *Wireless Communications & Mobile Computing*, vol. 13, no. 18, p. 15871611, 2013.
[48] E. B. Fernandez, R. Monge, and K. Hashizume, "Building a security reference architecture for cloud systems," *Requirements Engineering*, pp. 1–25, 2015.
[49] A. B. Y. Ad, A. B. T, M. E. L. Ghazi, A. Bouayad, A. Blilat, N. E. H. Mejhed, and M. El Ghazi, "Cloud computing: Security challenges," *2012 Colloquium in Information Science and Technology*, pp. 26–31, 2012.
[50] R. Bhadauria, R. Chaki, N. Chaki, and S. Sanyal, "A survey on security issues in cloud computing," *International Journal of Engineering & Technology (0975-4024)*, vol. 5, no. 2, 2013.
[51] W. Dawoud, I. Takouna, and C. Meinel, "Infrastructure as a service security: Challenges and solutions," in *Informatics and Systems (INFOS), 2010 The 7th International Conference on*, 2010, pp. 1–8.
[52] M. A. Lubiano, A. Salas, S. D. l. R. de Sáa, M. Montenegro, and M. Á. Gil, "An empirical analysis of the coherence between fuzzy rating scale-and likert scale-based responses to questionnaires," in *Soft Methods for Data Science*. Springer, 2017, pp. 329–337.
[53] T.-Y. Liu, "Learning to rank for information retrieval," *Foundations and Trends in Information Retrieval*, vol. 3, no. 3, pp. 225–331, 2009.
[54] Saaty, "How to make a decision: The Analytic Hierarchy Process," vol. 48, 1980.
[55] Z. Han, X. Li, and E. Stroulia, "A hierarchical security-auditing methodology for cloud computing," in *IEEE International Conference on Services Computing*, 2015, pp. 202–209.

Zhuobing Han received the B.S. degree in computer science from Sichuan Univeristy, Chengdu, China in 2011, and the M.S. degree from Tianjin Univeristy, Tianjin, China in 2013. She is currently working toward the Ph.D degree in the school of computer science and technology, Tianjin University, China. Her research interests include software security assessment, software evolution analysis, and mining software repositories.

Xiaohong Li received the Ph.D. degree from Tianjin University. She is a full tenured professor of the School of Computer Science and Technology, Tianjin University, Tianjin, China. Her current research interests include knowledge engineering, trusted computing, and security software engineering.

Keman Huang received the B.S. degrees from the Department of Automation, School of Economics and Management, Tsinghua University, China, in 2009, and the Ph.D. degree from the Department of Automation, Tsinghua University, China, in 2014. He is currently with the Sloan School of Management, MIT, USA. His research interests include service ecosystem, service recommendation, mobile service, and semantic Web. He received the Best Student Paper Award from the IEEE ICWS 2014 and the ICSS 2013.

Zhiyong Feng received the Ph.D. degree from Tianjin University. He is currently a Full Professor with the School of Computer Software, Tianjin University, China. He has authored one book, over 130 articles, and 39 patents. His research interests include knowledge engineering, service computing, and security software engineering. He is a member of the IEEE Computer Society and ACM.