Building Trustable Remote Monitoring and Management Systems

Maghsoud Morshedi
University of Oslo and EyeNetworks
Oslo, Norway
Email: mmc@eyenetworks.no

Josef Noll
University of Oslo
Oslo, Norway
Email: josef@jnoll.net

Raheleh Kari
Norwegian University of Science and Technology
Ålesund, Norway
Email: raheleh.kari@ntnu.no

***Abstract*—Internet of Things (IoT) is an emerging technology that expands wireless and mobile networks into heterogeneous network of connected devices. Trustable remote monitoring and management systems are required to establish a controlled environment for new services and devices in order to *(i)* improve the quality of existing services and *(ii)* enable novel services. However, monitoring and remote management can cause security and privacy concerns and thus affect the trust formation between customer and service provider. This paper introduces a trust model considering institutions as mediators to assess trustability of remote monitoring and management systems. The proposed model considers governance as an approach to audit remote monitoring and management systems and accordingly provides institutional assurance in form of certificate or labels in order to facilitate trust decision making and motivate trustworthy behaviors. The proposed model utilized the multi-metric method to measure governance criteria objectively and represent level of trustworthiness with A-F labels. Representing governance criteria with labels accompanied by color coding facilitates trust decision making based on application context or requirements for everyone regardless of level of expertise. Meanwhile, issuing trustworthiness certificate or A-F labels will encourage service providers to improve trustability of their remote monitoring and management approaches, which improve acceptability and efficiency of managed services.**

***Index Terms*—trust, cloud computing, remote monitoring and management, IoT, wireless networks, privacy, security.**

I. Introduction

The Internet of Things (IoT) is emerging and extends the IT networks with many new connected devices. The number of connected IoT devices will grow from 27 billion devices in 2017 to nearly 127 billion connected devices in 2030 [1] in various domains such as ehealth, industry applications, entertainment and transportation. However, the deployed devices can malfunction and cannot do what they are intended due to technical problems or malicious activities. In the traditional approach, technicians deployed to customer premises to fix issues, which is a time-consuming and costly approach and it cannot scale to billions of devices. Hence, service providers have been utilized cloud-based remote monitoring and management of services and devices.

The remote monitoring and management is a process of supervising and administration of information systems such as network devices, servers, mobile devices, and sensors. In remote monitoring, service providers enable the endpoint devices to report their operating information such as resource consumption, health checks, measured data of sensors by means of self-reporting or installing an agent on remote devices. In remote management, service providers administer remote devices to perform certain tasks such as software updates (e.g. patches, firmware updates and configuration changes), disable or enable specific services or functionalities, reboot or shut down the device, etc.

The remote monitoring and management have many applications in medical, industry, home, energy, and transportation. For example, health centers can optimize the use of health care resources by means of remote management of heart failure using implantable electronic devices, which downloads sensors data from patients' implanted devices [2], [3]. In case of automotive, the remote monitoring and management system can diagnose engine problems or perform health check as well as remote software update of the internal computer.

Although there are various technology solutions to improve the security and privacy measures comprising proper encryption, authentication, access control, etc [4], [5], remote monitoring and management of device behavior have been announced as a security strategy. However, remote monitoring and management may raise security and privacy concerns in respect with unregulated monitoring and management of services devices and accordingly users become reluctant to use managed devices or enable remote monitoring and management on their services.

However, the key challenge is to build a trustable remote monitoring and management system in order to assure users regarding their security and privacy. In the absence of trust, users will be reluctant to use or enable remote monitoring and management services due to growing security and privacy breaches. The present paper presents existing trust issues in monitoring and management systems and defines objectives in order to build trustable remote monitoring and management systems by motivating trustworthy behaviors from services providers' side.

The paper introduces trust issues that may raise security and privacy concerns due to implementation problem or lack of information. Thus, developing trust objectives consider expected behaviors to encourage service providers to improve trustability of their remote monitoring and management system as well as facilitate trust formation for users to accept and actively use managed services or devices.

Developing trust objectives leads to a trust model, which can boost the acceptability of remote monitoring and management systems. The proposed model considers institutional-based trustability assessment in form of certificates or labeling program in order to motivate trustworthy behaviors as well as facilitates trust formation for end-users and improve acceptability of new managed services. Hence, the proposed trust model utilized the multi-metric method to quantify governance criteria defined for trustability assessment and accordingly represent assessment with certificate and labels. The trust labeling program used in the proposed trust model motivates service providers to improve trustability of their remote monitoring and management approach, meanwhile expedites the trust decision making for end-users. In effect, trustable remote monitoring and management system will improve efficiency and quality of service in terms of performance, cost and user satisfaction.

The rest of paper is organized as follows: The definition of trust, distrust, trustor, and trustee presented in Section II. The existing trust issues that may raise user security and privacy concerns appear in Section III. The trust objectives that aim to improve trustworthiness, as well as proposed trust model, appear in Section IV, while trust labeling description appears in Section V. Section VI discusses the objectives and trust model presented in the previous section. Section VII presents related trust models and trust assessment approaches. Finally, Section VIII presents research conclusion and future work.

II. Trust Definition

In dictionaries, trust is defined as "*solid belief in the reliability, truth, or ability of someone or something*". The definition of trust in computer science can be categorized in term of user trust and system trust [6]. The user trust has its root in psychology and sociology, with a common definition as "*a subjective expectation as an entity has about another's future behavior*" [7]. This implies that trust is perceived personally. On the other hand, the system trust is a security perspective and defined as "*the expectation that a device or system will faithfully behave in a particular manner to fulfill its intended purpose*" [6], [8]. For example, a remote management system is trustworthy if it is reliable to perform as expected, such that it can manage remote devices to ensure remote devices are in the desired state exactly the same way as it expected. Therefore, trust can be defined in technology domain particularly monitoring and management systems as allowing other parties to access vulnerabilities based on their positive intention and behavior. In contrast, distrust can be defined as avoiding other parties to access vulnerabilities because of their doubtful intentions and behavior.

A trust relationship has two actors including trustee and trustor. The trustor is an actor who trusts the target entity called trustee [9], [10]. For example, a customer who buys a service or device is a trustor and the service provider who performs remote monitoring and management is a trustee in a system perspective.

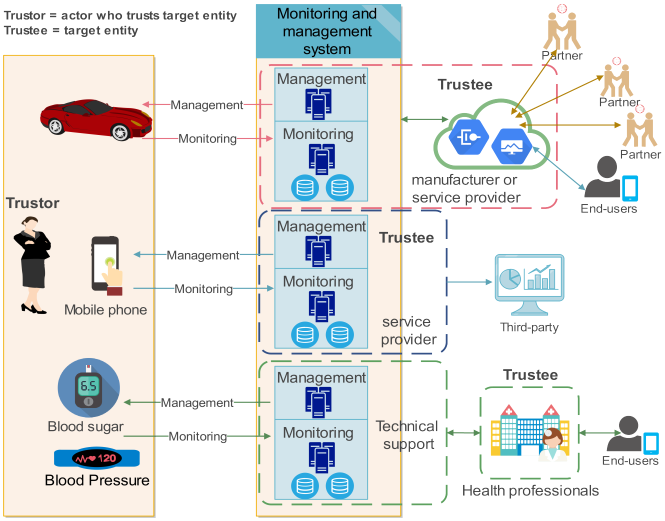

Fig. 1. Remote monitoring and management variables and actors in various use cases.

III. Trust Issues

In each trust relationship, trust issues can affect the trust negatively and result in distrust. Identifying trust issues helps to regulate certain actions such that a trustee demonstrates proper behavior in a trust relationship. Trust issues have been studied in various domains such as wireless sensor networks [11], vehicular communication [12], cloud computing [13], and software-defined networking [14]. Although remote monitoring and management have common trust issues with other technologies, its applications in various domains and distributed cloud-based architecture pose additional trust issues. Trust issues can be categorized into monitoring and configuration attributes and features, access control, technology and law enforcement groups. Figure 1 illustrates various use cases of remote monitoring and management while different parties act as trustee in different use cases. There are various actors in remote monitoring and management system that are not trustee while they can access user data and possibly manage remote devices. The behaviors of these actors can directly influence user trust. The following describes trust issues in various use cases in order to underline the severity of remote monitoring and management issues in different domains.

The monitoring and management attributes and features can become the main cause of trustability concerns such that monitoring attribute containing identifiable information or managing features that are not related to quality improvement can result in severe security and privacy breaches and accordingly user distrust. For example, monitoring driving habits or remote management of car functionalities such as brakes or steering can raise trust issues because if it is manageable then there is a possibility to be hacked and misused. Zhang et al. demonstrated that electronic controller units (ECUs) of cars can be compromised using remote wireless connection so that they could control in-car meter display, car's lock and steering system by sending control messages to car's controller area network (CAN) [15].

Service providers behavior can cause trust issues such that service provider (trustee) may exploit the vulnerabilities of trustor in a relationship. The service provider can exploit monitored data for marketing purposes, without user permission. Indeed, a user engages in a trusting action (e.g. enabling monitoring of a service), when the user realizes a gain (e.g. improved quality of service) and the trustee does not exploit user's vulnerabilities (e.g. does not exploit monitored data for marketing purposes). There are certain trustee's actions, which result in trust issues and accordingly cause distrust across users of a service. For example, a service provider can monitor data that are not related to the quality of service (e.g. location of device or identity of the owner of a sensor or device), thus monitored data can reveal sensitive information. Likewise, the service provider may share monitored data of a service with third parties or partners in order to gain benefits rather than improving the quality of service. In this case, users may avoid managed services even though they realize a gain by using managed services (e.g. patients may avoid using managed implantable electronic devices).

Another doubtful behavior is that a service provider may delegate the monitoring and management to third-party companies, while they do not define responsibilities and policies about data handling so that this may cause distrust. For example, a customer buys a sensor from vendor X, but the sensor communicates with a third-party company Y for remote monitoring and management features such as quality of service or software updates. Indeed, delegating monitoring and management without determining the responsibilities, access control and data handling policies can establish distrust among customers.

Security and privacy concerns regarding remote monitoring and management technology can also cause distrust. In monitoring and management system, lack of data transmission confidentiality in addition to low level of security may result in information leakage or unauthorized access to remote devices or sensors. For example, implementation of CPE WAN management protocol (CWMP) without security mechanism simplifies communication eavesdropping or performing unauthorized remote procedure calls (RPCs) in the remote device (e.g. home Internet gateways). The CWMP is not inherently insecure, but the improper implementation of TR-069 clients and servers may expose vulnerabilities, which affect many devices. The improper implementation of CWMP practices comprises using HTTP instead of HTTPS, lack of data validation [16] on the parameters used in a configuration, which results in code injection or lack of proper authentication.

The monitoring and management system can be a geographically distributed system so that law and the levels of law enforcement that the system operates can cause trustability concerns. For example, remote monitoring and management system can be geographically distributed and users monitored data can be stored in another country. In this case, which law or levels of law enforcement will assure the privacy and security of user data and managed device. Indeed, monitoring and management system can locate in various region in the world, so that if a sensor or a service has provisioned on monitoring and management system of another region then it can raise distrust even though service provider locates in a country that the sensor is being used.

IV. Trust Objectives

The trust issues can impede trustors enabling remote monitoring and management even though trustors would realize a gain so that trustee can experience business loss. Hence, trust objectives state desired achievements for both trustor and trustee in a relationship in order to maximize gain for both sides of a relationship. Trustee (e.g. service provider) can carry out certain behaviors or practices during information exchange, which improve quality of service and promote trust among trustors (e.g. customers). The trustee should only monitor minimized parameters rather than any data or information relating to identifiable individual or device, whilst the data is the raw material for improving quality of service. The same applies to the remote management such that trustee should only configure minimized functionalities rather than functionalities that compromise the device such as disabling security mechanism remotely. In addition, security and reliability of remote monitoring and management technology increase trustability of the system.

The trustor will either trust the trustee or withdraw from a relationship. In contrary, the trustee may lack the incentive to fulfill trustworthy action and decide to exploit trustors' vulnerabilities. A trust objective is to motivate trustee to carry out trustworthy actions. For example, motivate service provider (trustee) to implement proper security and privacy measures for their monitoring and management system by design. Hence, third-party institutional assurance such as certificates or labeling programs (e.g. from governmental institutions) can motivate trustee (e.g. service providers) to carry out trustworthy actions. The certificate program presents a binary outcome of trust assessment, whereas labeling program can be represented by granular discrete labels such as A-F alphabetical labels, which also helps trustors to make a decision more easily in various situations. Institutions can provide labeling system such that service providers receive trustworthiness label for their remote monitoring and management approaches rather than service-based trust assessment. Assessing service providers trustworthiness minimizes overhead of governance in service development.

The trustor can trust the trustee if trustee complies with certain regulations and policies. Hence, establishing remote monitoring and management governance as a trust objective will increase the confidence of trustor to participate in remote monitoring and management. For example, the remote monitoring and management governance can comprise auditability and accountability of trustee regarding monitored data and managed devices and services. In this regard, *(i)* the purpose of data collection (monitoring) and data processing should be declared *(ii)* data backup and destruction plan for all storage

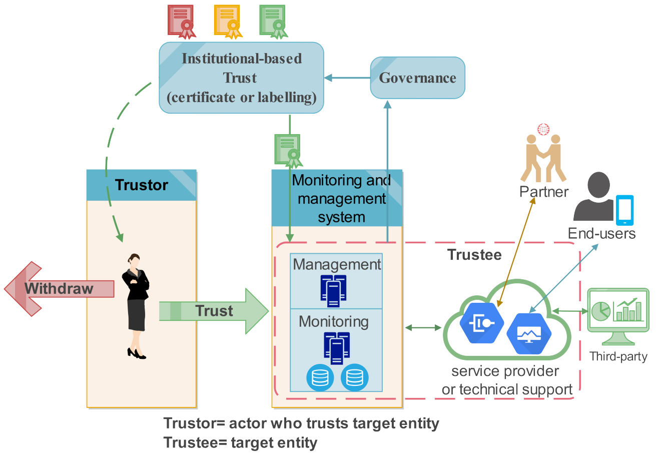

Fig. 2. Proposed trust model for remote monitoring and management systems.

location is necessary *(iii)* the physical location of data need to be recorded from law enforcement perspective *(iv)* data access policies should be performed in order to identify which data is accessible for partners or third-parties *(v)* how sensitive data is safeguarded in storage systems e.g. encryption mechanisms.

The remote monitoring and management are generally implemented as a system of systems so that it is part of a bigger system with various types of interconnections. Although actors' interactions may differ in various use cases, high-level architecture of remote monitoring and management approach will remain identical. In a remote monitoring and management system, identifying roles of actors and their interactions will help to recognize trust issues and form proper trust objective accordingly. This paper introduces a trust model, which considers institutional entities as mediators in order to facilitate trust formation and motivate trustworthy behaviors among trustees. In the proposed model, institutional entities assess trustability of trustees' (e.g. service providers) remote monitoring and management approach by means of governance criteria. This will also help trustors (e.g. users) to make a trust decision with confidence and accept trustable remote monitoring and management services rather than reject services. Figure 2 illustrates the proposed trust model in order to ensure trustworthiness of service providers remote monitoring and management approaches rather than individual service assessment. In the model, institutions as a mediators audit service provider's remote monitoring and management approach by means of governance criteria so that service providers receive trustworthiness certificate or A-F labeling. The certificate or A-F trustworthiness labeling will motivate service providers to improve trustability of remote monitoring and management approaches, meantime will simplify decision making for end-user for accepting managed services or devices.

V. Trust Labeling Program

The trust model proposed in preceding section introduced the essence of governance in building trustable remote monitoring and management systems. However, result of governance can be represented with a certificate or labels in order to facilitate trust formation. The governance can be done by observation or self-declaration approach, which this paper considers self-declaration approach in order to reduce governance overhead for implementing certificate or labeling program. On the other hand, the collected information by governance has to be measurable so that information can be represented by certificate or labels in an automated process.

This paper introduces generic and high-level governance criteria for remote monitoring and management systems by performing a case study in a company, which performs remote monitoring and management of Wi-Fi access points. However, the introduced governance criteria can be generalized to different domains as well. The criteria were selected in a way to identify trust issues in remote monitoring and management system so that criteria reflect trust issues presented in preceding section. In addition, the governance criteria can be extracted from European general data protection regulation (GDPR) [17] as well. Hence, governance criteria provide measures to identify trust issues in monitoring and measurement, which in the simple form can consist of yes/no questions. However, governance criteria can consider application-specific details, which may impede generalization to new services and applications and accordingly challenge the whole certificate or labeling program. Table I presents generic and high-level governance criteria such that service providers can answer questions in form of self-declaration in order to allow trust model to identify existing trust issues in remote monitoring and management approach, regardless of application or service type. The criteria categorized to four groups of trust issues discussed earlier, which can be extended per domain. Indeed, each category can introduce detailed sub-criteria in order to provide granular identification of trust issues. Therefore, each category presents sub-criteria one level further in order to demonstrate the process of providing detailed information for certificate or labeling program. Nonetheless, existing sub-criteria can be detailed into lower level information e.g. encryption algorithms used, cloud credential policies or encryption key sizes sub-criteria.

The governance provides information about trustee's behavior and existing trust issues in the system. However, mapping governance to a labeling program, which everyone can understand easily requires quantifying governance criteria. When the governance outcome became measurable, thus it would be straightforward to issue certificate or label for service provider's remote monitoring and management approach. Hence, this paper utilizes the multi-metric method presented by [18] and [19] in order to quantify governance criteria and accordingly issue certificate or label for trustee's remote monitoring and management approach. The multi-metric method utilizes two parameters: score (X_i) and weight (W_i) or importance of each criterion in order to calculate overall trustability score of an approach or a system. Therefore, overall trustability score can be calculated by a mean square

TABLE I

THE PROPOSED GOVERNANCE CRITERIA FOR REMOTE MONITORING AND MANAGEMENT SYSTEM WITH THEIR COMPUTED SCORE AND WEIGHT FOR WI-FI ACCESS POINTS USE CASE.

Score	Weight	Criteria
88	100	Did the service provider have declared features or attributes that service provider can monitor or configure by its remote management platform? And is the declaration accessible to users and certificate issuing institutes?
100	100	Did the service provider declare the purpose of remote monitoring and management?
80	100	Did the monitoring system minimize collecting any information relating to an identifiable individual or device such as MAC address of a device or the personal number of individuals?
90	100	Does the monitoring system collect minimized amount of performance parameters of services or analyze data packets as well?
80	100	What interval does the monitoring system collect data from users device or service? (every second, every minute, every hour, every 12 hours, every day)
89	100	Did the service provider declare the location of data storage and level of law enforcement applied? And is the declaration accessible to users and certificate issuing institutes?
90	70	Did the service provider declare data centers location (country or region) that are responsible of monitoring and configuration of devices or services?
100	70	Does the service provider store data on in-house data center or it stores monitored data on the third-party infrastructure?
100	100	Did the service provider declare what level of law enforcement applies to collected data in each data storage location?
80	100	Did the service provider declare data backup and destruction plan for all storage location?
70	80	Does the service provider use latest data protection methods in the industry (e.g. encryption mechanisms) while storing monitored data in its data center?
73	100	Did the service provider declare who has access to the monitored data or can configure service or device? And is the declaration accessible to users and certificate issuing institutes?
70	100	Does the service provider use an industry-grade access control mechanisms e.g. attribute-based access control (ABAC) to control access? (in-house business, in-house operation or third-party access control)
80	80	Does the service provider records data process activities including collecting data and configuration performed automatically or by the service provider?
70	100	Did the service provider minimize configuring critical features or attributes that may make the remote device or service vulnerable?
65	80	Does the service provider employ the latest security and privacy measures for remote monitoring and management system?
80	100	Does the remote monitoring and management system use latest transmission encryption methods in the industry?
50	60	Does the remote monitoring and management platform perform multi-factor cloud authentication?
50	70	Does the monitoring and configuration platform use PKI to secure devices and communication?

weighted data formula as follows:

$$Score = \sqrt{\sum_{i}^{n} \left(\frac{X_i^2 W_i}{\sum_i^n W_i} \right)}$$

The multi-metric method can quantify governance of complex systems in form of system of systems methodology, which can provide a granular assessment of remote monitoring and management systems. In the multi-metric method, each criterion gets a score in the 0-100 range, which indicates how much each criterion accomplished. Besides, weights indicate the importance of each criterion in the equation such that one criterion may radically affect the overall trust formation, while another may have low impact on building trust.

Table I presents scores and weights of governance criteria for trust assessment of Wi-Fi access point monitoring and management use case. In IoT monitoring and management, retrieving sensor's data is the main goal of monitoring so that weight of corresponding criterion asking whether the monitoring system records data packets is low, whilst in the mobile application services, the weight will be high value due to high risk of data misuse. Indeed, weights are selected based on the impact of criteria in trustworthiness of the system, while each criterion has different impact on trustworthiness. Substituting the use case scores and weights of governance sub-criteria of each category into the multi-metric equation will result in scores of each category presented in Table I. Then, it will require another multi-metric operation in order to calculate overall trustability score of the system, which results in overall trustability score of 80 for remote monitoring and management approach Wi-Fi access point monitoring and management use case presented in Table I.

The next step will map the measured score to respective certificate or label. The certificate or labeling program has to determine limits of labels or certificate threshold per domain. For example, in case of issuing certificate, any trustee that gets a score over 60 can be qualified to receive the trustworthiness certificate. In the labeling program, trustees will be qualified to receive trustworthiness labels according to Table II classification. This classification can be accompanied with coloring in order to facilitate the understanding of level of trustworthiness for everyone regardless of expertise. In case of the Wi-Fi access point use case, the scores and weights result in overall trustability score of 80, which it means the trustee can receive label B according to labeling classification.The labeling program facilitates decision making for trustors in different situations rather than simple yes/no decision.

TABLE II

MAPPING TRUSTABILITY SCORES TO LABELS AND THEIR COLOR REPRESENTATION

Score	Label	Color
90-100	A	🟩
80-90	B	🟩
70-80	C	🟧
60-70	D	🟧
50-60	E	🟧
<50	F	🟥

VI. DISCUSSION

The certificate or labeling program as the tangible outcome of proposed trust model motivates trustees to perform trustworthy behaviors and actions, besides facilitates the decision making for trustors. In addition, representing labels with color scheme simplifies identifying the level of compliance to regulation and policies for everyone.

However, organizing an institutional assurance is a challenging task and requires governmental and key business actors' support. For example, European GDPR can be a cornerstone to provide privacy governance procedures for technology standardization. On the other hand, definition and updating governance criteria requires active participation of governance bodies and business actors in the same way as technology standardization groups. In this respect, Consensus Assessments Initiative Questionnaire (CAIQ) [20] provided by Cloud Security Alliance (CSA) can be a cornerstone for definition of governance criteria. In addition, the implementation of the multi-metric method requires determining the importance of each criterion. However, the importance of each criterion in the multi-metric method can vary among actors per domain so that machine learning techniques such as neural networks can facilitate weighting process and accomplish a point of agreement among different actors and experts.

VII. Related Work

In recent years, trust models and trust assessment have been investigated in various areas such as wireless sensor networks (WSN), IoT, cloud services and enterprise systems in order to improve reliability of systems.

In WSN domain, trust models have been recommended as an effective mechanism to secure WSN, which extensively considers communication behavior in order to evaluate trust. The [21] classified trust model into centralized, distributed and hybrid in regard to where trust information stored. Authors in [22] classified trust models in WSN into node and data trust models. In node trust models, nodes calculate trust values in order to be able to associate with each other and node trust models can be classified into centralized and distributed. In data trust model, nodes calculate trust values to be able to distinguish data of legal nodes from illegal nodes. Trust models that targeted WSN can also be classified to reputation-based and credential-based model as well. The [23]–[27] presented reputation-based trust models for WSN so that nodes can reliably associate with each other. The [28] presented distributed trust model, which calculated trust according to different aspects including direct trust, recommendation, communication, energy and data trust in order to evaluate trustworthiness of nodes in WSN.

In IoT domain, trust models utilized reputation of devices in order to evaluate trustworthiness. The [29] presented a recommendation and reputation trust model for social IoT devices so that IoT devices associate with each other in trustworthy manner. The [30] presented a trust model based on knowledge, experience and reputation trust metrics in order to assess IoT devices trustworthiness in a network. The [31] presented a trust framework for IoT devices, in which IoT devices use public key in order to ensure trust. The [32] presented IoT trust and reputation model by using distributed probabilistic neural networks in order to distinguish trustworthy nodes from malicious nodes. The [33] presented a challenge-response trust assessment for personal space IoT in order to evaluate trustworthiness of the IoT devices before their association to the personal space.

In cloud environment, trust models utilize different approaches in order to assess security aspect of trust in cloud services. The [34] classified cloud trust models, which are based on customer feedback into applied technology and research models. The applied technology trust models comprises policy and SLA negotiation models in order to control access to cloud and establish trust with customers. The research trust models provide approaches to establish trust in cloud service environments using weighted average, probability, fuzzy logic, statistical analysis and machine learning methods. The [35] presented a trust model to measure security strength and calculate a trust value for only security aspect of cloud services.

In enterprise information systems, trust models almost consider security policies of enterprise. The [36] classified enterprise trust models into credential-based, reputation-based and hybrid trust models.

The most of literature utilized the reputation-based approach in order to evaluate trustworthiness. However, considering only reputation of a service provider does not imply that services and products are trustable because service providers' remote monitoring and management approaches may not comply with security and privacy best practices. Hence, compliance to regulations and best practices can ensure trustability of remote monitoring and management of devices in cloud environment. In addition, implementing trust models in the machine-to-machine communication can not ensure that services are trustworthy and users will trust to service providers. Hence, assessing trustworthiness of service provider's remote monitoring and management approach can complement device-level trust models and accordingly ensure acceptability and trustability of novel services.

VIII. Conclusion

The remote monitoring and management systems are designed to improve efficiency and performance, but they need to be trustworthy so that end-users can accept managed devices and services. This paper presented existing trust issues in remote monitoring and management and accordingly introduced a trust model for maximizing trustability of remote monitoring and management systems. The proposed trust model employed the multi-metric method to quantify governance criteria defined for trustability assessment into trustability scores in order to generate certificate or labels for remote monitoring and management approaches. The introduced trust model and labeling technique can motivate service providers to improve trustability of their monitoring and management approaches, meanwhile it simplifies trust formation decision making for end-users. Indeed, the proposed trust model paves the way for building trustable remote monitoring and management systems. In effect, trustable remote monitoring and management systems will improve acceptability of new managed services and devices, in which enhance performance and user satisfaction.

A. Future Work

The proposed trust model illustrated actors and interactions of a monitoring and management system as well as the essence of an institutional-based trust assessment. The follow-up work will therefore be developing a labeling program application by considering all available regulation for security, privacy, trustability and safety to build a comprehensive governance criteria data set. In addition, the development of labeling program will consider machine-learning techniques in order to automate weighting process and simplify quantifying the governance criteria for trustability assessment.

References

[1] IHS Markit. (2018) The internet of things: a movement, not a market. [retrieved: Sep, 2018]. [Online]. Available: https://cdn.ihs.com/www/pdf/IoT_ebook.pdf

[2] J. M. Morgan, S. Kitt, J. Gill, J. M. McComb, G. A. Ng, J. Raftery, P. Roderick, A. Seed, S. G. Williams, K. K. Witte, D. J. Wright, S. Harris, and M. R. Cowie, "Remote management of heart failure using implantable electronic devices," *European Heart Journal*, vol. 38, no. 30, pp. 2352–2360, 2017. [Online]. Available: +http://dx.doi.org/10.1093/eurheartj/ehx227

[3] G. Boriani, A. Da Costa, A. Quesada, R. P. Ricci, S. Favale, G. Boscolo, N. Clementy, V. Amori, L. Mangoni di S. Stefano, H. Burri, and on behalf of the MORE-CARE Study Investigators, "Effects of remote monitoring on clinical outcomes and use of healthcare resources in heart failure patients with biventricular defibrillators: results of the more-care multicentre randomized controlled trial," *European Journal of Heart Failure*, vol. 19, no. 3, pp. 416–425, 2017. [Online]. Available: http://dx.doi.org/10.1002/ejhf.626

[4] N. Kumar, J. Madhuri, and M. ChanneGowda, "Review on security and privacy concerns in internet of things," in *2017 International Conference on IoT and Application (ICIOT)*, May 2017, pp. 1–5.

[5] V. Beltran, J. A. Martinez, and A. F. Skarmeta, "User-centric access control for efficient security in smart cities," in *2017 Global Internet of Things Summit (GIoTS)*, June 2017, pp. 1–6.

[6] W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in social networks," *ACM Comput. Surv.*, vol. 45, no. 4, pp. 47:1–47:33, Aug. 2013. [Online]. Available: http://doi.acm.org/10.1145/2501654.2501661

[7] L. Mui, "Computational models of trust and reputation : agents, evolutionary games, and social networks," Ph.D. dissertation, Massachusetts Institute of Technology, Massachusetts, 2003. [Online]. Available: http://hdl.handle.net/1721.1/87343

[8] T. W. Um, G. M. Lee, and J. K. Choi, "Strengthening trust in the future social-cyber-physical infrastructure: an itu-t perspective," *IEEE Communications Magazine*, vol. 54, no. 9, pp. 36–42, September 2016.

[9] T. Grandison and M. Sloman, *Specifying and Analysing Trust for Internet Applications*. Boston, MA: Springer US, 2003, pp. 145–157. [Online]. Available: https://doi.org/10.1007/978-0-387-35617-4_10

[10] J. Riegelsberger, M. A. Sasse, and J. D. McCarthy, "The mechanics of trust: A framework for research and design," *International Journal of Human-Computer Studies*, vol. 62, no. 3, pp. 381 – 422, 2005. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1071581905000121

[11] N. Karthik and V. R. S. Dhulipala, "Trust calculation in wireless sensor networks," in *2011 3rd International Conference on Electronics Computer Technology*, vol. 4, April 2011, pp. 376–380.

[12] H. Hu, R. Lu, and Z. Zhang, "Vtrust: A robust trust framework for relay selection in hybrid vehicular communications," in *2015 IEEE Global Communications Conference (GLOBECOM)*, Dec 2015, pp. 1–6.

[13] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, "Trustcloud: A framework for accountability and trust in cloud computing," in *2011 IEEE World Congress on Services*, July 2011, pp. 584–588.

[14] Z. Yan, P. Zhang, and A. V. Vasilakos, "A security and trust framework for virtualized networks and software-defined networking," *Security and Communication Networks*, vol. 9, no. 16, pp. 3059–3069, 2016, sCN-14-0760.R1. [Online]. Available: http://dx.doi.org/10.1002/sec.1243

[15] Y. Zhang, B. Ge, X. Li, B. Shi, and B. Li, "Controlling a car through obd injection," in *2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud)*, June 2016, pp. 26–29.

[16] QA Cafe. (2017) Is your tr-069 implementation vulnerable to code injection attacks? [retrieved: Sep, 2018]. [Online]. Available: https://www.qacafe.com/training/2017-01-12-tr-069-code-injection-attack/

[17] European Parliament. (2016) The european data protection regulation. [retrieved: Sep, 2018]. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

[18] I. Garitano, S. Fayyad, and J. Noll, "Multi-metrics approach for security, privacy and dependability in embedded systems," *Wireless Personal Communications*, vol. 81, no. 4, pp. 1359–1376, 2015.

[19] A. Fiaschetti, *Measurable and Composable Security, Privacy, and Dependability: The Shield Methodology*. Taylor & Francis, a CRC title, part of the Taylor & Francis imprint, a member of the Taylor & Francis Group, the academic division of T&F Informa, plc, 2017. [Online]. Available: https://books.google.no/books?id=fn3ZAQAACAAJ

[20] Cloud Security Alliance (CSA). (2017) Consensus assessments initiative questionnaire (caiq). [retrieved: Oct, 2018]. [Online]. Available: https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v3-0-1/

[21] V. U. Rani and K. S. Sundaram, "Review of trust models in wireless sensor networks," *Int. J. Comput. Inf. Syst. Control Eng*, vol. 8, pp. 371–377, 2014.

[22] G. Han, J. Jiang, L. Shu, J. Niu, and H.-C. Chao, "Management and applications of trust in wireless sensor networks: A survey," *Journal of Computer and System Sciences*, vol. 80, no. 3, pp. 602 – 617, 2014, special Issue on Wireless Network Intrusion. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0022000013001232

[23] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Trans. Sen. Netw.*, vol. 4, no. 3, pp. 15:1–15:37, Jun. 2008. [Online]. Available: http://doi.acm.org/10.1145/1362542.1362546

[24] F. Gómez Mármol and G. Mart´*(i)* nez Pérez, "Providing trust in wireless sensor networks using abio-inspiredtechnique," *Telecommunication Systems*, vol. 46, no. 2, pp. 163–180, Feb 2011. [Online]. Available: https://doi.org/10.1007/s11235-010-9281-7

[25] S. Ozdemir, "Functional reputation based reliable data aggregation and transmission for wireless sensor networks," *Computer Communications*, vol. 31, no. 17, pp. 3941 – 3953, 2008. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366408004301

[26] J. Zhang, R. Shankaran, M. A. Orgun, V. Varadharajan, and A. Sattar, "A dynamic trust establishment and management framework for wireless sensor networks," in *2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, Dec 2010, pp. 484–491.

[27] S. Misra and A. Vaish, "Reputation-based role assignment for role-based access control in wireless sensor networks," *Computer Communications*, vol. 34, no. 3, pp. 281 – 294, 2011, special Issue of Computer Communications on Information and Future Communication Security. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366410000885

[28] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, "An efficient distributed trust model for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 5, pp. 1228–1237, May 2015.

[29] U. Jayasinghe, N. B. Truong, G. M. Lee, and T. W. Um, "Rpr: A trust computation model for social internet of things," in *2016 Intl IEEE Conferences on Ubiquitous Intelligence Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, July 2016, pp. 930–937.

[30] U. Jayasinghe, G. M. Lee, T. W. Um, and Q. Shi, "Machine learning based trust computational model for iot services," *IEEE Transactions on Sustainable Computing*, pp. 1–1, 2018.

[31] K. A. R. Rehiman and S. Veni, "A trust management model for sensor enabled mobile devices in iot," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Feb 2017, pp. 807–810.

[32] S. Asiri and A. Miri, "An iot trust and reputation model based on recommender systems," in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, Dec 2016, pp. 561–568.

[33] T. Nguyen, D. Hoang, and A. Seneviratne, "Challenge-response trust assessment model for personal space iot," in *2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, March 2016, pp. 1–6.

[34] E. F. Rawashdeh, I. I. Abuqaddom, and A. A. Hudaib, "Trust models for services in cloud environment: A survey," in *2018 9th International Conference on Information and Communication Systems (ICICS)*, April 2018, pp. 175–180.

[35] R. Shaikh and M. Sasikumar, "Trust model for measuring security strength of cloud computing service," *Procedia Computer Science*, vol. 45, pp. 380 – 389, 2015, international Conference on Advanced Computing Technologies and Applications (ICACTA). [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050915004081

[36] A. Manna, A. Sengupta, and C. Mazumdar, "A survey of trust models for enterprise information systems," *Procedia Computer Science*, vol. 85, pp. 527 – 534, 2016, international Conference on Computational Modelling and Security (CMS 2016). [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050916305609