Assigning Trust to Devices in the Context of Consumer IoT Applications

Evandro L. C. Macedo, Flavia C. Delicato, Luís F. M. de Moraes and Giancarlo Fortino

***Abstract*—With the outstanding growth in the number of consumer IoT connected devices, especially boosted by smart home applications and wearables, there is a need to provide such devices with security. If any device in such consumer IoT systems gets compromised, a data leak may cause serious threats to privacy, material losses and even put people's lives at risk. Therefore, in this article, we focus on challenges associated with the trust involving communication between IoT devices, which is a key security-related characteristic in consumer IoT applications. A mathematical trust metric, based on a two-level approach, is used to illustrate how the presented proposal can be useful in the objective assessment of confidence and, consequently, provide better security among IoT devices.**

***Index Terms*—IoT, security, trust, blockchain, entropy**

I. Introduction

The overwhelming growth of devices connected to the Internet of Things (IoT) [1] paves the way to a myriad of consumer IoT applications at homes, offices, factories, cities, and so on, that can significantly impact the current life of society [2]. Such a pervasiveness movement extends the benefits that can be gained in the areas of healthcare, smart cities, smart homes, intelligent transportation systems, and many other IoT systems [3]. The unprecedented data acquisition and exchange among diverse peer devices enables the integration of cyber and physical world, and enhances decision-making processes.

Nevertheless, such benefits also imply providing the involved devices with security. If the security of any component becomes compromised, a data leak may cause serious privacy threats, enable surveillance, bring about material losses, or even jeopardize people's lives. For instance, a smart home equipped with intelligent devices' control (the most common consumer IoT application nowadays [4]), could be compromised and then start switching devices on and off intermittently, which could burn individual components or even short circuit the house, leading to disastrous consequences. Another example would be a tampered control of an autonomous driving car in an intelligent transport system, which can cause vehicles to crash. Besides financial loss, a security flaw can lead to violation of data privacy and, in the worst cases, it may even incur physical damage to living beings. Therefore, there is a need to understand the underpinning security risks and the new requirements and challenges in the design of IoT systems and consumer applications. In particular, the trust aspects of the communication among IoT devices is of a paramount importance [5]–[9], due the challenge of managing each device individually, which are potentially exposed to a variety of risky and compromised networks, especially in the context of applications that present an ultra-reliability requirement.

In accordance with references [6], [10], establishing trust between IoT devices is challenging and includes fundamental aspects such as belief, integrity, reliability, availability, among others. In particular, there are difficulties that still persist for IoT consumers, such as the lack of information about devices management, how their personal data are stored, how their privacy is sustained, and how they can identify security vulnerabilities on their gadgets [4], [11], [12]. All these issues hinder the adoption of IoT and impact the trust about it.

Specifically, in terms of trust, there is a variety of definitions for this concept (as described in [6], [10], [13]), which are inherited from the user's context to IoT devices. In fact, trust is a complex conception yet with no consensus in the community. Meanwhile, we consider that the trust concept for IoT should comprise at least four aspects, namely, identity assurance, network behavior, data integrity, and protection aspects.

In the next coming years, a lot more connected devices are expected to exist than nowadays [1]. Taking into account the potential increase of the attack surface on the Internet, which will result from the huge quantity of connected appliances, the focus of this paper is concentrated on the issues and challenges related to security and trust in the context of consumer IoT applications. In addition, by considering the approach introduced in [14], we propose to measure the trust in IoT devices by using a two-level approach, that is based on information from the network traffic behavior of IoT devices, and from the application layer, which stands for the devices' reputation. One advantage of such a strategy is the use of data obtained from two different perspectives, which provide more information to continuously monitor and establish trust between devices. The characteristics of Low Level (network perspective) and High Level (application perspective) compose a comprehensive trust metric, capable of capturing changes in the acting of devices and isolating those presenting unexpected misbehavior. Another advantage is to stipulate an initial trust value when the communicating devices do not know each

This study was partially funded by Fundação de Amparo à Pesquisa do Estado do Rio de Janeiro (FAPERJ) and Rede-Rio (the state academic backbone network) under the grant 150.134/2010 for Luís F. M de Moraes, by FAPESP under the grant 2015/24144-7 for Flavia C. Delicato, by Italian MIUR PRIN 2017 Project "Fluidware" under the grant CUP H24I17000070001, and in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Finance Code 001.

The authors Evandro L. C. Macedo and Luís F. M. de Moraes are with the Computer Engineering and Systems Program, Universidade Federal do Rio de Janeiro, email: {evandro, moraes}@ravel.ufrj.br

The author Flavia C. Delicato is with the Department of Computer Science, Federal Fluminense University (UFF), email: fdelicato@ic.uff.br

The author Giancarlo Fortino is with the Department of Informatics, Modeling, Electronics and Systems (DIMES), University of Calabria (Unical), email: giancarlo.fortino@unical.it

Evandro L. C. Macedo is the corresponding author.

Digital Object Identifier XXX

other beforehand and, consequently, do not have a history of interactions in order to infer about trust. We envision that our approach is mainly applied in IoT applications in which devices primarily rely on device-to-device communication.

The following is a summary of the main ideas developed and presented in this paper:

- We discuss the concept of trust and its importance in the context of consumer IoT;
- We point out the issues and challenges to provide trust in such environments;
- We argue that trust models should involve more than one level of information gathering to compound a trust metric;
- We outline potential future research works;
- We propose a trust model and show how it correctly captures the intended aspects.

The rest of this paper is organized as follows. In Section II we discourse about related works in the literature, and present a comparison involving them and the proposal in this paper. Section III presents the trust components of our model and its verification. Some open research issues are discussed in Section IV, and Section V concludes the paper.

II. Related Work

The literature presents many proposals to model a trust metric applied to IoT. Authors in [15] propose a Bayesian network-based trust model and a method for building reputation based on recommendations in peer-to-peer networks. They show that systems that communicate according to trust and reputation outperforms systems that do not consider such aspects in terms of the percentage of successful interactions. Fortino *et al.* [16] develop a framework based on software agents able to exploit social attitudes of IoT devices. They use blockchain (BC) to compute the reputation of devices, which can use network services according to their reputation.

In [17], Tang *et al.* use the passport analogy to propose a decentralized trust framework for cross-platform collaborations using BC technology. They use a combination of smart contracts, with each interaction among devices signed by the participants and recorded on the BC. In our approach, we focus on recording the devices' identities in BC to build devices' reputations (initial trust). Authors in [18] focus on wireless sensor network applications and present a trust model using weighted averages considering three types of trust: direct, regional, and historical data trust. Through simulations, authors show that their approach is aware of energy consumption with a significant reduction of resource usage and a higher detection rate in comparison with other approaches.

Hongjun *et al.* [19] use Information Theory to build trust among devices. They represent the relationships with a directional graph and compute the entropy of the capability of a device to perform an action. This way, they can detect malicious devices in the network. We also adopt Information Theory, but with a different perspective focusing on the network level instead of the application level.

Khan *et al.* [20] propose a trust-based approach for managing the reputation of every device of an IoT network based on Routing Protocol for Low Power and Lossy Networks (RPL). The results show the ability to detect and isolate malicious nodes from the network, resulting in better network resilience, as well as less number of misbehaving devices (bad devices) identified in the network after every RPL round, and less number of paths including a bad device. Caminha *et al.* [21] introduce a smart trust management method based on machine learning which automatically assesses the IoT trust by evaluating service provider attributes. They also use an elastic slide window feature that helps to differentiate broken or malfunctioning devices among misbehaving devices.

Authors in [22] use fuzzy logic to provide an end-to-end security solution through a lightweight authorization mechanism and a novel trust model that has been specially devised for IoT environments. Their approach considers four dimensions, i.e., quality of service, reputation, security aspects, and social relationships, to compute trust values about IoT devices. In [23], authors consider an IBE implementation together with a BC implementation. Authors split the devices in the chain to complete user authentication and private key protection. The results show the failure probability is stabilized with the number of cycles during which a device operates. Wei *et al.* [24] employ a BC approach to address the trust management issue in the context of Social IoT. They compute the trustworthiness value of devices according to their service evaluations stored in BC. Different from our approach, they do not consider network aspects that also impact trust values. Authors in [25] propose a decentralized security framework based on BC that could be applied to IoT systems, among several other consumer applications, which provides a new way of managing trust.

Table I shows a comparison between previously discussed works and our approach in terms of the following aspects: (i) which technique is used, (ii) whether a dataset is considered and, if so, what kind of dataset, (iii) whether the approach considers network-level and/or application-level characteristics, (iv) which type of architecture is used, (v) whether the approach is resource-constraint-aware and/or dynamism-aware, and (vi) if the approach offers trust values. Most of the works consider application-level characteristics, and only a couple (including our approach) take into consideration the network level. Out of the 12 presented works, 10 consider a distributed architecture, 6 are resource-constraint-aware, 5 are dynamism-aware, and 5 actually present a trust metric.

The foregoing works emphasize the importance and relevance of building trust-based approaches to provide security in IoT devices communication. In this paper, besides presenting a trust model that combines BC and Information Theory techniques, the key contribution of our work is the double perspective of both application level and network level. Hence, our approach provides a more comprehensive trust metric that can deal with the particularities of consumer IoT devices.

III. Trust Modeling

To model trust for IoT, we need to know which information is necessary to compose a trust metric. First, a receiver IoT device needs to build an initial trust to enable communication, since it does not know the sender IoT device previously. Given the initial trust, the receiver should dynamically adjust its trust

TABLE I
COMPARISON AMONG RELATED TRUST PROPOSALS

Work	Technique	Dataset	Network Level	Application Level	Architecture	Resource-constraint Awareness	Dynamism Awareness	Offers Trust Metric
[15]	Bayesian networks	None	No	Yes	Distributed	No	Yes	No
[16]	Agent-based + Blockchain	None	No	Yes	Distributed	Yes	Yes	No
[17]	Blockchain	None	No	Yes	Distributed	No	No	No
[18]	Weighted Averages + Data Fusion	Synthetic	No	Yes	Decentralized	Yes	Yes	Yes
[19]	Entropy	Synthetic	No	Yes	Distributed	No	No	Yes
[20]	RPL + Subjective Logic	None	Yes	No	Distributed	Yes	No	No
[21]	Machine Learning	Real + Synthetic	No	Yes	Centralized	No	No	No
[22]	Fuzzy Logic	Real	No	Yes	Distributed	Yes	No	Yes
[23]	IBE + Blockchain	None	No	Yes	Distributed	No	No	No
[24]	Agent-based + Blockchain	None	No	Yes	Distributed	No	No	Yes
This proposal	Relative Entropy + Blockchain	Real + Synthetic	Yes	Yes	Distributed	Yes	Yes	Yes

in the sender accordingly to the network behavior of the sender (more trust if the behavior is as estimated, less trust otherwise). Then, the trust value should not last endlessly, but instead, be decreased over time, given that, after the last contact, the receiver does not know if the sender was compromised or if it presents any unexpected (potentially malicious) behavior.

The essential features for trust are the guarantee of the uniqueness, veracity, and authenticity of the device's identity. Therefore, a device must know if a communicating device is indeed the device it supposes it is. This issue raises the need for an IoT device identification mechanism that provides assurance of unique identities as well as protection against tampering, duplication, forgery, and impersonation. A possible strategy to do so is to use the encryption scheme Identity-Based Encryption (IBE). IBE, as its name implies, is based on the unique identities of the communicating parties to generate private and public keys. The advantage of IBE is that, when sending a message, senders do not need to exchange keys with receivers, since receivers' public keys can be generated based on information already known to the senders, such as an IP address or an email. In this way, it is possible to reduce the number of messages exchanged between devices during authentication, which also contributes to devices' energy saving. Energy efficiency is a key requirement in IoT systems since the devices usually are battery powered. Notwithstanding, IBE itself requires a central entity called a Private Key Generator (PKG) which generates devices' private keys. This is required when using IBE because an entity in this scheme (*e.g.*, a device) could generate the private keys of all other entities since it has access to all public information required for doing this. Thus, the PKG adds a random element to each private key and distributes the key to the respective device.

In the pure IBE architecture, the PKG is a point of vulnerability, given its capacity to open any message from any device, or impersonating a device identity. To address this issue, we propose the use of BC [16], [26], [27] to decentralize the PKG and distribute the responsibility of inferring trust to network members. The nodes that compose the BC, also known as the full nodes, store the identities of devices and keep track of their transactions. Therefore, BC provides the reputation of devices by default (or by design), being transparent to devices, acting as part of the network itself. At this point, it is important to notice that only nodes that take part in an administrative domain can be elected as full nodes since they will be key to the correct and trustful operation of the approach. Hence, we take into account a public-permissioned BC, since the reputation of devices must be available for query by any interested IoT device (public), as well as restricted to allowed full nodes (permissioned). Likewise, full nodes are not meant to be IoT devices, since they are usually resource-constrained. Instead, in a typical three-tiered IoT system, such as described in [28], full nodes can be more resourceful edge devices, located at the Edge tier.

When a device wants to communicate with another device and needs to verify/validate whether the other is in fact whom it claims to be, the identity of that device is verified against the information stored in the BC. Therefore, it is no longer necessary to have a centralized PKG, given that edge nodes will deliver the authorization/authentication service. As a result, security in terms of trust between devices will be provided natively by the network, which has benefits such as denying access to a malicious device, not allowing it even to get into the network, since it does not have a valid identity accepted by most members of the BC.

As commented in [29], blockchain-based identity and access management systems are promising approaches for improving the security of IoT applications. Thus, the High Level of our approach considers a blockchain-based component to improve the security by offering an initial trust while the Low Level is not ready to compute trust values from the network characteristics since there is no communication history. We consider a BC infrastructure that can handle various application requirements and levels, from local applications associated with a local BC to a global application with a BC on large scale. In particular, we consider a consensus protocol based on proof-of-stake, which has the potential to better fit to such a context, since

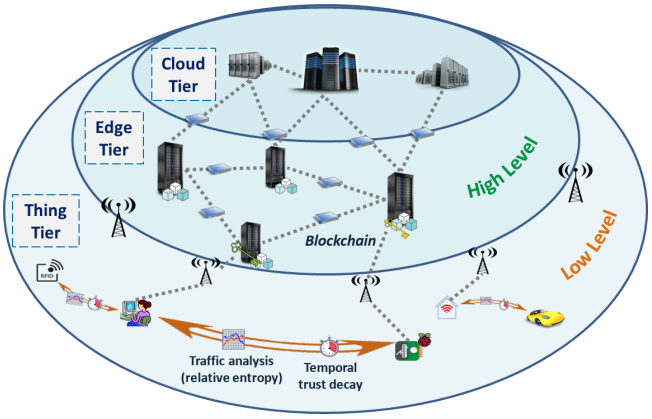

Fig. 1. Trust approach scenario of two-level approach considering a tree-tier architecture

there is no mining in the process requiring less computational power and thus being more cost-effective.

Considering the high dynamism of the IoT, in addition to the initial trust provided by the High Level mechanism, some mechanism is equally necessary to adjust the trust value over the time during which communication between the devices takes place. The Low Level is in charge of it and it comprises two components, namely, the relative entropy (C_2) and the temporal decay (C_3). In C_2 we use Information Theory [30] to model the incoming throughput of a device and compute its respective relative entropy in order to capture changes in the distribution of the traffic behavior of such a device. To deal with the dynamism and opportunistic aspects of IoT, the C_3 decreases the trust value as soon as the devices stop communicating and can no longer be sure about the other device's trustworthiness. Features that consider dynamic aspects are mandatory in IoT because of the frequent topology changes due to devices' battery draining, devices entering and leaving the network, connection disruptions or loss, mobility, scheduled shutdowns, among others.

An illustration of how the proposal works can be seen in Figure 1. In the illustrated scenario, initially, two devices at the Thing Tier want to communicate and do not know each other previously. They need to infer an initial trust value since they have little or no information about the other device. Therefore, the operating steps are as follows:

- **Step 1:** Each IoT device queries the other's identity in a BC infrastructure that stores the identities of members;
- **Step 2:** Once a minimum initial trust is established, the communication can normally start;
- **Step 3:** As the communication between the devices happens, the Low Level takes place. Each device calculates the relative entropy of the other device's traffic and uses this information to adjust the respective values of trust. If a device starts behaving abnormally[1], this will negatively affect trust and may cause communication to terminate if it decreases beyond a previously defined threshold. If the communication is over, a temporal component reduces the trust value until it reaches the point where the devices will have to query the BC again and restart the whole process.

[1]In our case, an abnormal behavior means any traffic pattern whose distribution diverges from the expected traffic pattern distribution

Therefore, to perform device trust assignment, we propose a composition of characteristics that can be observed by a particular device during its communication with another device. With such characteristics, the device can calculate how much it trusts in the other device.

We define the trust of a device j in device i as TR_{ji}. The TR_{ji} is initially computed with the first component that is based on the trust of the $i's$ identity, which is obtained from the associated reputation of the stored identity in a public-permissioned BC, expressed by C_1 in Equation 1. In the very beginning of any new devices' communication, the identities of such devices must be stored in the BC. Then, the trust value that C_1 provides is based on the number of confirmations a transaction has on the BC. To cope with the high computational costs commonly found in proof-of-work-based consensus strategies, we envision the implementation of full nodes at the Edge Tier and not at Things Tier given that the IoT devices are known as being resource-constrained.

$$C_1 = \#\text{ of confirmations the } i\text{'s identity has} \tag{1}$$

TR_{ji} is also influenced by a second component C_2 (Equation 2) that is based on the inverse of the relative entropy of the traffic, which changes when the current traffic behavior of the device, represented by $q_{Y_{ji}}(x)$, deviates from the estimated traffic behavior, represented by $p_{X_{ji}}(x)$, due to any type of anomalous condition, where $q_{Y_{ji}}(x)$ and $p_{X_{ji}}(x)$ are non-negative, integer random variables that assume values in the interval $\mathcal{S}_{ji} = [0, \Delta, 2\Delta, ..., R_{ji}^{max}]$, with Δ a positive integer and R_{ji}^{max} the maximum traffic rate. Such component is also based on Kullback-Leibler [31] divergence $D(p||q)$, a type of "distance" between two distributions. The estimated traffic behavior is obtained using a Kalman Filter with $mean = 0$ and $covariance = 1$, since it closely tracks traffic and does not require too many resources.

$$C_2 = \frac{1}{D(p||q)}; \quad D(p||q) = \sum_{x \in \mathcal{S}_{ji}} p_{X_{ji}}(x) \log \frac{p_{X_{ji}}(x)}{q_{Y_{ji}}(x)} \tag{2}$$

The third component (C_3) considered to compute the trust value in our proposal is a temporal component that works like a timeout by decreasing the trust value from the moment devices stop communicating until they reach a threshold. When trust value falls below the threshold, devices will need to return to the first case of trust establishment, i.e., devices will need to obtain a minimum trust from BC again. In our model we consider a proportional temporal decay as described in Equation 3.

$$C_3 = TR_{ji} \times d \tag{3}$$

where d is the decay factor.

Equation 4 presents the proposed composition with all three components together.

$$TR_{ji} = C_1 + C_2 - C_3 \tag{4}$$

Regarding the four aspects that we assume for the IoT trust concept in Section I, in our proposal we incorporate *identity assurance* with the use of IBE for devices identification, *network behavior* is addressed by using the Low Level component, the *data integrity* is incorporated by assuming the successful communications reported by the confirmations of the transactions in BC, and the respective *protection* of devices through communications that are only allowed for licit devices.

A. Model Verification

An experimental evaluation of our trust analytic model was developed to analyze the behavior of the model over time. As the model verification evolves, each component of the Equation 4 is computed. For instance, a device i generates traffic to a device j according to some distribution. This means, in each time interval τ (*e.g.*, one second), a value of bytes per τ is generated according to such a distribution. In the same way, device j also sends traffic to device i according to another distribution, but changes its behavior during a certain interval by sending traffic according to a different distribution. What we aim to demonstrate is the dynamism of the trust metric as the traffic behavior changes and verify our model with traffic patterns based on known distributions (not yet realistic).

Figure 2 illustrates the traffic generation of two devices according to a Poisson distribution with parameter $\lambda = 10Bps$. During the interval between the instants 400 and 600 of the experiment, the traffic of device j changes its pattern to another distribution, namely, a Pareto with parameter $\alpha = 10Bps$. Therefore, the trust metric is computed throughout this behavior, taking into consideration the Equation 4.

The trust metric over time is shown in Figure 3. The trust values vary over time, following the variation in traffic behavior (observed in Figure 2). More specifically, it reduces when the traffic pattern changes (between instants 400 and 600), and recovers when the pattern goes back to the expected behavior. The green and red lines represent the thresholds set by each device to decide on the minimum trust value accepted to establish a communication. Threshold values are key to our approach and must be properly set according to the application the devices are associated with, and possibly tuned overtime to cover application changes. Hence, the High Level of our approach makes available application-level information that includes the selected threshold set by the application in question, which can accept lower trust values (less restrict) or only higher trust values (more restrict). In this example, the device i stops trusting in device j as soon as it starts perceiving the anomalous behavior of j. Conversely, device j keeps on trusting in i since its threshold is set really low (0.1), which illustrates a malicious device that easily trusts in any device so as to be able to communicate with anyone.

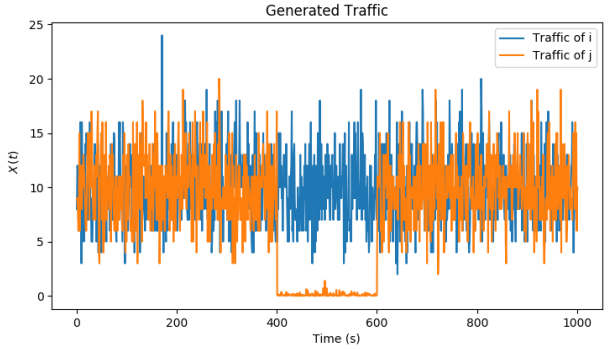

Fig. 2. Generated traffic over time

Fig. 3. Calculated trust over time considering synthetic traffic

During the operation of the network, it is necessary to have mechanisms that allow the adjustment of trust values. Hence, this is done through the relative entropy component, which adjusts the trust based on traffic behavior. Thus, behaviors that deviate from the expected contribute to the variation of the entropy, which consequently impacts the trust value.

IV. Open Research Challenges

With human beings, the concept of trust is related to the behaviors perceived during interactions and experiences with other people (either in the present or in the past). It is also related to the behaviors and attitudes of the person itself who is building trust in others. Thus, cultural aspects and the environment have an influence on people's behaviors, consequently influencing trust placed in others when an interaction occurs.

Different from the human-centric concept, in the IoT context, building trust from one device to another may not consider the behavior and actions of the device itself which is building trust, but only information from other devices. For instance, a compromised device will not consider its malicious history to compute trust in another device. In fact, it will always set its trust in others as high as possible, given that it wants to transmit to whichever device it can. The measure of trust rules whether a device will accept the connection from other devices or not. So, trust for IoT should be built only upon information from other devices and not upon information from the device itself that is building trust. Trust is asymmetric, context-dependent, dynamic, and not necessarily transitive, hence establishing trust between IoT devices is challenging, as its definition is also related to fundamental aspects such as belief, integrity, reliability, verification, among others [6].

Based on previously presented security aspects on consumer IoT electronics communication, we bring some challenges and opportunities associated with such context. In particular, trust is a fundamental aspect to provide consumer IoT systems with security [11], [12], since the entities of such systems

are inherently widely distributed and dependent on reliable data. Many open issues are still present on the development of consumer IoT applications in terms of trust establishment, mostly due to the characteristics of the respective applications. For instance, the IoT feature of heterogeneity in terms of device types, transmission technologies, and systems involved, poses the challenge to manage such features and make the devices interoperate in a trustful manner. With a huge amount of different technologies involved, the challenge is to provide a comprehensive and common trust metric that could be used by all different devices in a consumer IoT application.

In addition, the scalability factor, with the huge and continuously increasing amount of connected devices, also contributes to hampering trust establishment, which should consider local and global trust metrics. Distributed solutions tend to be more appropriate to inherently distributed IoT systems. In sum, the integrity of data and devices' identity assurance are still challenging, with no convergence for any standard, despite existing proposals (Sections II and III). Hence, we provided a trust definition suggestion through our two-level approach trying to fill the commented gaps and advance the development of consumer IoT systems. We also encourage the development of trust proposals that can deal with the discussed challenges found in consumer IoT applications.

V. Concluding Remarks and Future Work

In general, security aspects are not considered from the beginning of the development of IoT consumer systems. In particular, trust aspects are fundamental to provide IoT devices with security, in which such devices can trustfully establish communication. We discuss strategies to assigning trust in communication between IoT devices considering the model presented in [14]. Nevertheless, we highlight some issues that are still open and that are essential for the development of trustworthy consumer IoT systems.

A possible limitation of our approach is when a device enforces a specific traffic behavior to increase its reputation before others. Nevertheless, even if some devices may get compromised for a while due "fake" traffic behavior, the High Level of our approach is intended to cope with such situation. This component acts by reducing the trust of such devices through their reputation among the devices' community, as soon as the bad behavior of such devices is reported and the malicious devices are contained. In another perspective, a device that changes its network behavior due to licit application modification may have its trustfulness decreased while such new behavior is not updated on other devices.

References

[1] Ericsson, "Internet of Things Forecast," Ericsson, Tech. Rep., 2019.

[2] T. Alladi, V. Chamola, B. Sikdar, and K.-K. R. Choo, "Consumer IoT: Security vulnerability case studies and solutions," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 17–25, 2020.

[3] R. Casadei, G. Fortino, D. Pianini, W. Russo, C. Savaglio, and M. Viroli, "Modelling and simulation of Opportunistic IoT Services with Aggregate Computing," *FGCS*, vol. 91, pp. 252 – 262, 2019.

[4] C. International, "Testing our trust: consumers and the internet of things 2017 review," Consumer Inter., Tech. Rep., 2017.

[5] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146 – 164, 2015.

[6] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *Journal of network and computer applications*, vol. 42, pp. 120–134, 2014.

[7] V. Dedeoglu, R. Jurdak, G. D. Putra, A. Dorri, and S. S. Kanhere, "A trust architecture for blockchain in IoT," in *16th EAI Inter. Conf. on Mobile and Ubiquitous Sys.: Comp., Net. and Serv.*, 2019, pp. 190–199.

[8] E. L. C. Macedo, E. A. R. de Oliveira, F. H. Silva, R. R. Mello, F. M. G. França, F. C. Delicato, J. F. de Rezende, and L. F. M. de Moraes, "On the security aspects of Internet of Things: A systematic literature review," *Journal of Comm. and Networks*, vol. 21, no. 5, pp. 444–457, 2019.

[9] F. M. R. Junior and C. A. Kamienski, "A Survey on Trustworthiness for the Internet of Things," *IEEE Access*, vol. 9, pp. 42 493–42 514, 2021.

[10] A. Arabsorkhi, M. Sayad Haghighi, and R. Ghorbanloo, "A conceptual trust model for the internet of things interactions," in *2016 IST*, 2016, pp. 89–93.

[11] C. International, "Securing consumer trust in the internet of things – principles and recommendations," Consumer Inter., Tech. Rep., 2017.

[12] H. Aldowah, S. Ul Rehman, and I. Umar, "Trust in IoT Systems: A Vision on the Current Issues, Challenges, and Recommended Solutions," in *Advances on Smart and Soft Computing*, F. Saeed, T. Al-Hadhrami, F. Mohammed, and E. Mohammed, Eds. Singapore: Springer Singapore, 2021, pp. 329–339.

[13] D. E. Saputra, "Defining trust in computation," in *2020 ICITSI*, 2020, pp. 161–166.

[14] E. L. C. Macedo, R. S. Silva, L. F. M. de Moraes, and G. Fortino, "Trust Aspects of Internet of Things in the Context of 5G and Beyond," in *2020 CIoT*, 2020, pp. 59–66.

[15] Y. Wang and J. Vassileva, "Trust and reputation model in peer-to-peer networks," in *Proceedings Third International Conference on Peer-to-Peer Computing (P2P2003)*, 2003, pp. 150–157.

[16] G. Fortino, F. Messina, D. Rosaci, and G. M. L. Sarne, "Using Blockchain in a Reputation-Based Model for Grouping Agents in the Internet of Things," *IEEE Trans. on Eng. Management*, pp. 1–13, 2019.

[17] B. Tang, H. Kang, J. Fan, Q. Li, and R. Sandhu, "IoT Passport: A Blockchain-Based Trust Framework for Collaborative Internet-of-Things," in *Proceedings of the 24th ACM SACMAT '19*, 2019, p. 83–92.

[18] Z. Chen, L. Tian, and C. Lin, "Trust Model of Wireless Sensor Networks and Its Application in Data Fusion," *Sensors*, vol. 17, no. 4, 2017.

[19] D. Hongjun, J. Zhiping, and D. Xiaona, "An Entropy-based Trust Modeling and Evaluation for Wireless Sensor Networks," in *2008 Inter. Conf. on Embedded Software and Systems*, 2008, pp. 27–34.

[20] Z. A. Khan, J. Ullrich, A. G. Voyiatzis, and P. Herrmann, "A Trust-Based Resilient Routing Mechanism for the Internet of Things," in *Proceedings of the 12th ARES '17*, 2017.

[21] J. Caminha, A. Perkusich, and M. Perkusich, "A Smart Trust Management Method to Detect On-Off Attacks in the Internet of Things," *Security and Communication Networks*, vol. 2018, pp. 1–10, 2018.

[22] J. Bernal Bernabe, J. L. Hernandez Ramos, and A. F. Skarmeta Gomez, "TACIoT: Multidimensional Trust-Aware Access Control System for the Internet of Things," *Soft Comput.*, vol. 20, no. 5, p. 1763–1779, 2016.

[23] B. Zhou, H. Li, and L. Xu, "An Authentication Scheme Using Identity-based Encryption Blockchain," in *IEEE ISCC*, 2018, pp. 00 556–00 561.

[24] L. Wei, J. Wu, and C. Long, "Enhancing trust management via blockchain in social internet of things," in *2020 Chinese Automation Congress*, 2020, pp. 159–164.

[25] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework [future directions]," *IEEE Consumer Electronics Magazine*, vol. 7, no. 2, pp. 18–21, 2018.

[26] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Working Paper*, 2008.

[27] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *FGCS*, vol. 82, pp. 395–411, 2018.

[28] W. Li, I. Santos, F. C. Delicato, P. F. Pires, L. Pirmez, W. Wei, H. Song, A. Zomaya, and S. Khan, "System modelling and performance evaluation of a three-tier Cloud of Things," *FGCS*, vol. 70, pp. 104 – 125, 2017.

[29] N. Kshetri, "Can blockchain strengthen the internet of things?" *IT Professional*, vol. 19, no. 4, pp. 68–72, 2017.

[30] C. E. Shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[31] J. C. Principe, *Information theoretic learning: Renyi's entropy and kernel perspectives*. USA: Springer Science & Business Media, 2010.