ISSN: 0974-5823 Vol. 7 No. 1 January, 2022

International Journal of Mechanical Engineering

Novel Research on Challenges and Directions for Trust Management in Social Internet of Things (SIOT)

Julius Wosowei (Researcher)[1], Prof. Chandrasekar Shastry (Guide)[2]
Affiliation: Computer Science and Engineering, Jain (Deemed to be) University)[1]
Dean, PG Studies, FET, Jain (Deemed to be) University[2]

ABSTRACT

In order for establishing the social networks of the networked smart device, the Internet of Things (IoT) and the social networking concepts were merged for forming the Social Internet of Things (SIoT). As a result of this confluence, both paradigms have been enriched, resulting in new ecologies. The SIoT adds Human-to-Thing (H2T) interaction to the Human-to-Human (H2H) and Thing-to-Thing (T2T) interaction paradigms of the Internet of Things. Socially intelligent "social devices" are now possible because to the Internet of Things (IoT). These social objects (SOs) possess social features that allow them to discover and connect with other SOs in their immediate environment. To find useful services and information, they trawl through social network of things they're interested in. Too far, very little research has been done on the topic of trust & trustworthiness in the Internet of Things (IoT). We have three things to offer in this article. For starters, we'll go over the basics of SIoT and discuss how it differs from the Internet of Things (IoT) in terms of trust. Second, we categorize and assess all of the trust management solutions for SIoT that have been offered in the literature during the last six years. Using comparative analysis of the trust management process, we compare the most recent state-of-the-art SIoT trust management schemes. To round out our discussion, we point out the difficulties in building confidence and measuring trustworthiness among SOs that are engaging in the new wave of SIoT. More advanced than ever before, electrical and technological devices of today are a wonder to behold. We can't imagine our life without sensors, actuators, and RFID tags. Things like social media and the Internet of Things (SIoT) are nothing new. Human-tohuman and human-to-human communication have both increased as pervasiveness has increased. It's not uncommon to hear people refer to the "Social Internet of Things"as the new paradigm that combines IoT with the social networks. It's a kind of social network for smart objects called the Internet of Things (IoT). SIoT is strongly reliant on trust for devices to interact independently. It is our hope that the findings of this study will help readers to better understanding the shortcomings of present trust models and to direct towards future studies that will help to design new models that can manage any and all possible and apparent risks. The study focuses on SIOTs' trust management challenges and opportunities in the future.

Keywords: SIOT, Trust management, Security issues, Future Directions

1. INTRODUCTION

There is an increase within the independent studies which looked into possibilities in merging the social networking concepts with Internet-of-things (SIoT) technologies in recent times. New SIoT applications and networking services can be supported more effectively and efficiently by adopting the SIoT paradigm. The four-layer IoT architecture defines all the applications wherein the IoT is applied and offers the interface between the network and end IoT devices. Services are enabled for different uses at this layer based upon sensor data. The data processing received through a perception layer,data processing layers verifies that the information has come from an authentic user and that the data has been safeguarded from threats. It's also known as the transmission layer, or the network layer. Network communication networks can communicate with each other through it, since it serves as a conduit for data received by sensors. Perception or sensor layers are in charge of identifying and collecting data from IoT devices. There are a variety of sensor types on the network, as well as the perception layer needs to be able to distinguish between them. The data transmissions and the measurement among the two items in an Internet of Things (IoT) setting are made easier by the autonomous nature of the data transfer and the measurements among the objects. Interaction of devices in internet with different standards. Architecture of Social Internet of Things consists of 4 layers. User interaction in SIoT applications is ensured by the first layer of applications. The SIoT architecture includes a wide variety of user applications, some of which were highlighted in the preceding section. There is a lot of multimedia input in the upper layer of user interaction from the following techniques: Social relationship graphs, Service Application Programming Interfaces, Participation Model, Relation Control Model, Social Presence in the network (SPN) and Relation Management Structure; Service Discovery; Service Composition Model; and Trustworthiness Management, to name a few examples. SIoT's second layer or composite year determines the type of intermediate devices and communications protocol among the SIoT devices. Object-to-social, Object-to-object and social-to-social interactions are all possible in the SIoT ecosystem. However, the precise meaning of SIoT is reinforced by the need for social interaction in the IoT ecosystem.

Siblings Relationship, the Client Instance Relationship, Possession Instance Relationship, Social Instance Relationship, Neighbors Relationship, the Sentinels Relationship, Drifters Relationship, and Utility Instance Relationship are derived because of this inclusion. This composite layer of SIoT takes care of the mix of the social interaction and the object interaction in ubiquitous environment. As a result of their specific communication interfaces and common languages and procedures, the base layer as well as object layer of SIoT differs based on objects, environments, applications, data in the object. A last commitment is made by a human to communicate with SIoT servers to improve their profile as well as relationship status between the friend in order for discovering the service through the social network.

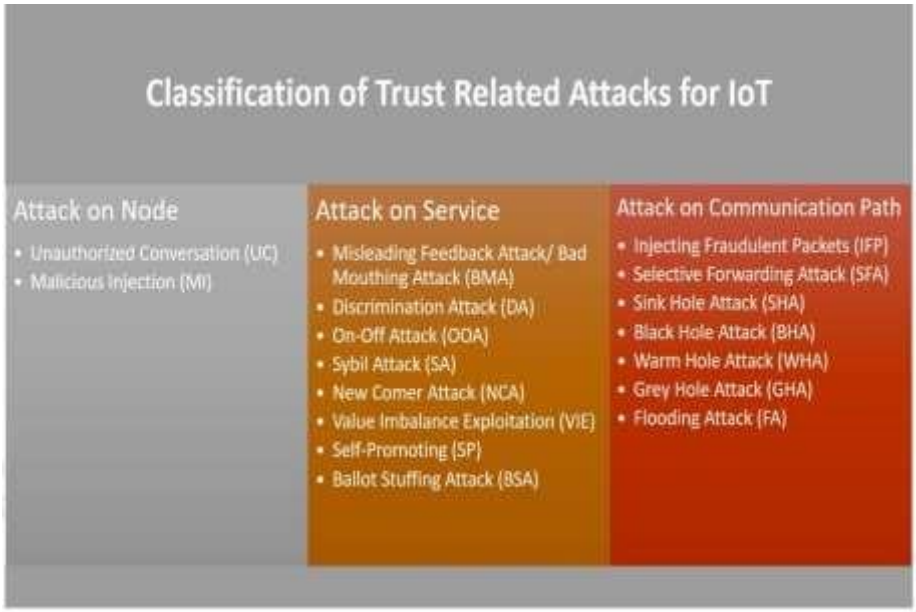

Fig1. Different types of trust attacks

1.1. Badmouth Attack

This attack takes advantage of the trustworthiness of trustworthy nodes [109]. Node A, for example, can be considered to be doing well if all of the nodes that it interacts with provide positive feedback about its performance. This attack occurs when a hacked node takes control and sends negative reports or suggestions to node A to harm its credibility. Many trust management processes mention this as the most direct attack [110].

1.2. Discrimination Attack

Change the trust value of the nodes through delivering discriminating services through nodes that provides the service (the service provider). Giving group an excellent service while giving group B subpar service is an example of this. As a result, the trustworthiness of group B as a recommendation source may be negatively impacted [109].

1.3. ON- OFF (OOA) Attack

Depending on the fact ,trust is a dynamic occurrence. When a node is engaged in this attack, it can act both as a good node and as a bad one simultaneously to avoid detection [110]. Ex. if the node A is the malicious and compromised, that can authenticated by giving nice behaviour in order to improves the good status and after some time bad behaving merely are safe side. Even if a person's reputation is tarnished, he or she can still have a decent one.

1.4. (NCA) New Comer Attack

A re-entry attack is also known. Because of this vulnerability, the same node can access the network multiple times under different identities without the network being aware of it. When a node A's reputation is terrible and its history of bad behaviour is known, it will quit the network and reenter under a new identity with no previous reputation. A mapping among identity and its characteristics are either the identity providers [113] in order to detect this issue.

1.5. (SP) Self-Promoting Attacks

To be considered as a service provider, every node might provide reports on good status.Despite being of the service provider, it gives poor service quality [29].

1.6 (BSA) Ballet Stuffing Attack

Ballot stuffing is the practice of boosting the reputation of harmful users by giving them high ratings. [114][115]. Malicious agents, in particular, promote the reputations and trust scores of other nodes that have been compromised in order to boost their own.

1.7 Selective Forwarding Attack (SFA)

Adversary can selectively forward packets in this attack. The routing layer is targeted in this attack [116]. DoS attacks can be launched from any node in the network. As an example, if node A is only transmitting negative suggestions from node the B, and by not recommending, this node will be subjected to DoS attacks as they aren't evaluated to any services that the network offers to any node.

2. MANAGEMENT OF TRUST IN SIOT

Trust composition

The Quality of service (QoS) and the social trust are known as the two most important factors in determining trust value. To assess the quality of the service, variety of metrics is employed. These include packet delivery ratios, load balance, energy usage, honesty,delay, bandwidth, and so on. Factors such as social interaction, privacy,friendship, community of interest, closeness, centralization, and connection are used to measure social trust. Following properties were used to calculate trust in prior studies [6-8, 11].

- Trust is based on the direct experiences and interactions.
- The recommendation and the comments from other gadgets or contemporaries are used to build trust in a product or service.

The advice is based on the opinions of others and the general public.

- History may influence current trust levels based on previous interactions or experiences.
- Context is a major factor in trust. According to task, span of time and surroundings, trust changes. Changing the circumstances can alter one's perception of trustworthiness.
- When the environment changes, trust becomes more or less non-monotonic.

Propagation of trust in SIoT

The trust rating is calculated in both the direct and indirect observations. The trust propagation process uses both centralized and distributed methods. Devices are connected to a centralized body in order to restore trust. The distributed approaches are the trust observations are stored by SIoT devices in relation to their peers. In this method, a central server is not utilised.

Trust aggregation in SIoT

Belief Theory, Regression Analysis, Fuzzy Logic (FL) and Bayesian Model (BM) are used to collect trust. Changeable behaviour, the membership changes, interaction of the pattern changes, the network topology changes and the location changes are all examples of dynamicity of a device.

3. CHALLENGES IN SIOT

1. *Zapability of Devices*

SIoT devices have varying levels of computing the power, storage capacity, communication standard and I/O channels, so previous trust management methods cannot be applied to all SIoT applications. All of these device needs should be taken into account by the trust management algorithm.

2. *Handling of Large Networks*

Transactions are generated when devices communicate with each other. Existing systems can't handle the volume of data that would be generated by such a vast number of transactions. For the massive number of devices and the communication between them, the trust management algorithm must be extremely powerful

3. *Departure of existing models and arrival of new models*

The SIoT system constantly changes as new devices are added and old ones are removed. In other words, a trust management algorithm should take into account a device's dynamic nature.

4. *Finding a trust worthy model*

There are now so many devices on the market that it's hard to tell which ones are reliable. SIoT improves the quality of life for humans. Much more data is exchanged in today's society via mobile devices. Non-trusted clients/devices may use data supplied with

them for harmful purposes. In order to prevent harmful attacks, an algorithm must be developed which identifies activities of the device that allows sharing of a regulated way.

5. Choosing of trust features

Device of IoT will trust each other in order to transmit data securely. The accuracy and performance of trust systems depend on selecting the right trust features. When it comes to total trust in the SIoT network as indicated in table III they fail to detect assaults perpetrated by malicious devices. Finally, the dynamic change in trust feature criteria is not taken into account when trust calculations in the prior systems [6, 7]. As the importance of each transaction rises, so does the level of trust that may be calculated.

6. Aggregation of trust

Weighted sum aggregation of trust values has been employed in most previous attempts. However, this practice has significant flaws. In order to determine the weighting factor, there are numerous possibilities. Because of weights assigned to the trust feature change the situation next, systems are unable to identify which feature has the greatest impact on trust. This method is unable to distinguish between malicious and non-malicious behaviour on a node. Consequently, this research employs the ML to combines trust scores with the detection of harmful devices.

7. Trust updates

As stated in [6, 24, 25], a trust update score is calculated using the value provided by another node or recommender, i.e., a recommendation. If the node is malicious, what will happen to the user? Nodes' abilities and prior trust scores are taken into account when updating trust in [6, 18, 26, 27]. Gain/damage after task completion; good conduct or poor conduct; successful/unsuccessful communications; packet received and differentiation; etc. are all factors in determining a device's ability. What if the trustor and trustee do not communicate for an extended period of time? When updating trust, it is important to take into account the amount of time since the last engagement. If there is no contact between nodes in [14], the trust decays. It is used to trust features such as recommendations and prior trust values, which are affected by trust decay a person's previous level of trust diminishes with each subsequent interaction. Based on historical trust effectiveness, direct assessment, and recommendation, the overall trust is updated. When calculating trustworthiness over time, the number of interactions in the interval is used. Every time j and I have a new encounter, our faith in each other is re-evaluated. If the node j disappears from the network, what will happen to the other nodes in the network, and how will the other nodes in the network react? In these circumstances, I shall provide the value of my former trust. As a result, our research employs a time-driven trust method.

4. FUTURE DIRECTIONS

1. Right friend selection

Without human interaction, the IoT SO s under the SIoT paradigm can build relationships with other social IoT objects and maintain information about their friends. [76] Social IoT not only improves navigation, but it also supports in the discovery of new jobs. In spite of SIoT's efficiency in locating services, the increasing number of heterogeneous devices has made it more difficult to discover the proper companion, as interactions between SOs become increasingly complex. Relationship manager design and the selection of a good buddy are critical variables in the success of the SIoT platform's performance and reliability. As a result, it is imperative that these items be subjected to a set of rules. It is possible for any social IoT device to integrate functionality such as trustworthiness, which can be used to assess the reliability of a buddy [15]. Because a social IoT object could have a big number of friends (good friends, closest mates, etc.), trust is a crucial factor to consider when selecting a possible buddy or discovering new services [77]. When two items become friends, the level of confidence they have in one other increases significantly. In spite of the fact that trust has been extensively studied and addressed as a factor that assists in forming social links between the objects, an extensive research is required to define friendship, the proper selection of friends, and the sorts of jobs or activities that may be done by different kinds of friends It's possible that service composition might be used as a component that selects the appropriate objects or friends for a certain task, activity, or situation. In other words, it is still difficult to find a better way to select and evaluate an ideal and possible friend based on the tasks or circumstances in which they will be used.

2. Different user acceptance models of SIoT

Social networking and IoT integration has created a new generation of SIoT computing in which every object provides intelligence and awareness to support social navigation and to interact based on common interests or shared contexts. SIoT's sociality notion can lead to substantial dangers of information leakage, violating both the privacy of the owners of these SOs and those with whom these objects have interactions or connectivity. Confidentiality and data anonymity, integrity, and access controls that manage authentication and authorization are important to meet basic consumer security concerns, and so privacy of consumers or owners of these SOs should be successfully protected. However, the complex SIoT environment still lacks sufficient identity and authentication capabilities. Despite the benefits of the Internet of Things (IoT), customers are reluctant to use SIoT-based systems and apps because of the potential of privacy violations. For every technology, the level of trust that customers have in it influences their decisions and encourages them to use that technology despite unforeseen situations as they overcome their perceptions of danger and uncertainty that is associated with it. TAM has been used extensively to anticipate the adoption and use of IT and IoT [25, 78–81]. No research

has been done in this area for the SIoT paradigm, and academics have thus far failed to pay attention to the views of SIoT users. As a result, the systems and programmes that accept them have changed. Security models for SIoT systems and user acceptance models for these systems are tough to establish.

3. Management of trustworthiness

There must be a reliable linkage between social IoT items and build relationships. Because of the importance of trust in the Internet of Things, ensuring the physical and digital safety of these devices is a major challenge [82–86]. Resource-constrained social IoT objects make it difficult to share an SP's trustworthiness because a large history of interactions can cause communication overhead and scalability concerns. Objects' initial trust values cannot be calculated using the trust models currently in use. In addition, the mathematics required to determine trust may need a large amount of computing power. For limited IoT devices with limited computation capabilities, lightweight and efficient trust management measures are required to compute trust evaluation metrics because it is difficult to calculate trust scores. In an Internet of Things (IoT) setting, trustworthiness management is essential. For the SIoT-based environments, ensuring the trustworthiness of transmissions, sensed data, and computation outputs, as well as boosting trustworthiness among social intelligent devices is a major requirement. Constrained social IoT items also pose a challenge to developing and implementing trust formation algorithms.

4. Management of trust based on semantics and context

IoE, IoT, IoV, as well as SIoT are all incorporating context awareness into their architectures. Certain scenarios necessitate a system that is aware of the context in which it is operating, such as automated decision making, notification to the user as well as sensitivity to the context. Those heterogeneous IoT devices pose a problem in terms of safety and reliability in collecting context data. For context data, customers, and providers, trust management is a valuable tool inside the SIoT paradigm to address reliability challenges. Researchers should focus on developing context-aware trust models for SIoT in order to evaluate the trustworthiness of various social IoT objects inside the multi-service environment of SIoT, where context awareness is critical.

5. Self-operational and tolerance of fault management

It's not uncommon for failures to occur owing to battery depletion in resource-constrained smart devices and inadequate connectivity in today's mobile, dynamic SIoT environment, resulting in data loss. That's why a need exists for a new generation of fault-tolerant routing algorithms that use minimal communication energy to ensure connectivity between these SOs and people. Furthermore, making SIoT systems more robust and tolerant of failures would help ensure their long-term success. SIoT environments where objects are socially aware and capable of taking collective decisions by successfully sharing information with each other and verifying the trustworthiness of that information can swiftly find a better and an ideal solution to any problem, therefore enhancing the entire network's reliability. When it comes to successful collaboration, social IoT objects must appropriately measure and communicate their own capabilities to solve the problem. Is it logical to have a single, fixed centre accountable for directing the entire system and manipulating its behaviour in a highly evolved heterogeneous SO? A distributed infrastructure, on the other hand, is better suited to SIoT situations where each node is self-sufficient and capable of collecting, evaluating, and deciding on its own what to do. System-level failure detection and management and recovery from failures becomes increasingly difficult in SIoT scenarios because of the IoT's intrinsic complexity. Human-induced error and failure are more to likely occur in these complex systems, making development more difficult [88, 89]. Due to the heterogeneity of IoT linked devices, troubleshooting require huge quantity of the information source are examined to get knowledge about the failure nodes, the causes of failure, the consequences, the diagnosis, and the repairing systems because of the wide range of local area connections. This necessitates the development of autonomous components that can self-heal, self-organize and self-manage in orders in reducing need for the human intervention, although be single device like smart lock or entire system like smart house. By utilizing a collection of actions and tools to collect failure information created from the heterogeneous connected through device and evaluating the event, fault causes and remedies can be determined, Caporuscio et al. [91] has established the concepts of the smart troubleshooting. Smart troubleshooting would allow the system to self-heal and become more resilient. System and framework which includes repair actions for handling failures whilst also avoiding imperfect maintenance and complex actions for prognostics and restoration of normal system operations that usually requires the co - ordination of both manual and automatic actions, as well as avoiding the faults holistically and the virtual patching are difficult to develop.

6. Decentralized management system of SIOT, based on block chains

Confidential third-party servers are used to implement and preserve results in centralized trust management system but all processing (trust calculations) isn’t accessible for the users, so the Centralized Trust Mechanisms is vulnerable. In addition, this result is much expensive due to the great infrastructures and the cost of maintenance that are associated with big server farms, the Centralized cloud, and network equipment. The researchers are attempting the design trust management systems that are less centralized, but they aren't completely decentralized because they still rely on central servers for the ultimate calculation or management of trust credits. In the case where the other third party is not trusted by the user, a fully decentralized trust management architecture must be implemented. Researchers has been started in the decentralized trust management through introduction of the block chain technology because of block chain has the potential to build the effective trust frameworks for IoT by providing transparent evaluation

procedures and the storage of trust credits that cannot be reversed. The development of the blockchain based decentralized trust management systems for the IOT has yet to be attempted. As a result, that's rise of the SIoTbased environment, the need to design a new trust management prototype employing blockchain technology becomes critical. The decentralization, the privacy protection, and the self-enforcing management remains as primary challenges for the creating trust management systems for SIoT.

FUTURE DIRECTIONS

Challenges	Future Directions
Right Friend Selection	• How many friends are sufficient, acceptable, or manageable and is this figure has a limit or not? • Can having many good friends provide much better services or a balanced is required between good and bad (selfish) friends? • How and which new friendship relations can be established and used for gaining better services or completing context specific tasks? • What are the strategies to develop appropriate friend relationships for specific types of tasks or activities and how trust will change throughout that existing or new relationships?
User acceptance models for SIoT	• What are the useful services and attractive applications that can encourage consumers to adopt SIoT systems? • What are methods for recognizing consumer experience? • How consumer trust upon SIoT based systems can be developed? • What are the behavioral and technological aspects of consumer's perception towards SIoT adoption and the factors that influence consumer trust and their role in the adoption of SIoT technology • What are the frameworks and effective trust models that can guide and elucidate SIoT technology designers and service providers about the requirements of the its consumers and the associated risks?
Trustworthiness Management	• How trust assessment of entities like social IoT agents or SIoT service providers can be accurately achieved in the presence of accuracy-privacy dilemma? • How to determine which second-hand evidence is less reliable and how much to rely on the trust scores that are calculated from second hand evidences as compared to first hand evidences? • How to make Trust management (TM) more resilient to trust related attacks and intelligent to detect misbehaving nodes, dishonest recommendations and misbehaving patterns of social IoT objects in the network? • What are the effective trust Update Mechanisms for Social IoT that can facilitate in updating the trust values computed by the social IoT objects and lead to less computation and processing overheads? • What are effective and robust algorithms for trust decision-making for dynamically changing SIoT environments? • How to determine the initial trust score of each individual object in case if history is not sufficiently established and the number of other social objects connected to that new object are insufficient to establish a pattern for trust score calculation?
Context and Semantics based Trust Management	• How context-based information that is exchanged between the social IoT objects can be protected? • How to develop innovative context-aware trust models for the extraction of comprehensive contextual information produced by smart social IoT objects that are capable of collecting diverse types of data? • How to overcome context sharing problems in order to provide an inter-domain context interoperability? • How to correctly manage the current context in the trust models so that the performance of the system can be improved? • How semantics/ontology based trusts models can be developed that can provide unambiguous access and data interpretation while facilitating the interoperability among all components?
Fault Tolerance and Self Operations Management	• What are the fault tolerance techniques for IoT that can be applied in SIoT environment? • What are the faults that can occur in the context changing environment of SIoT and their patterns, severity and effects on the SIoT based applications or systems? • How to deal with challenges of SIoT environment like failures in service provision, changes in sensor location and device faults, and what are the methods to anticipate and to mitigate the problems before they occur? • Why troubleshooting is an essential requirement for SIoT based systems and How anomalies in heterogeneous connected devices of SIoT based systems can be recognized promptly? • What are the appropriate troubleshooting solutions based on available information derived by leveraging social relationships in SIoT systems that can be automatically applied by the social objects for the restoration of the correct system operation and scaling down the probability of maintenance mistakes and time to time repairing? • What are the methodologies, tools and opportunities in the area of smart-troubleshooting for SIoT based systems?
Blockchain based Trust Management System for SIoT environment	• How privacy of Opinions or Trust scores given by an object regarding other objects stored in the blocks of a blockchain can be preserved which is public and can be seen by all the participants? • How to counter Bad Mouthing and Ballot Stuffing attacks on Trust Management Systems based on blockchain where 51 % attack can be launched on bitcoins? • How Scalability can be handled when increasing number of social objects are involved in a Blockchain? • How storage issues can be managed due ato the increased number SIoT objects?

Fig 2 Elaborated Future Directions

5. CONCLUSION

Smart devices (things) that can gather and exchange the data through network with less human intimation and decision-making have been provided under the IoT paradigm. Using SIoT as a paradigm, an expanded version of IoT has evolved as a means of enhancing network scalability and thereby addressing SIoT's inherent limitations in terms of scalability, heterogeneity, and trust and resource discovery. According to their owners' connections to other people in online social networks, SIoT social intelligent objects can form friendships with one other (OSNs). SIoT social objects can find new resources to better execute user services. Providing reliable service evaluation in this environment is quite difficult. Trust evaluation in SIoT systems has also become an important issue because of the difficulty of combating trust-related assaults and dishonestly behaved SOs. We compared and contrasted the basic principles of the IoT along with Industrial IoT in this post. The various SIoT designs were evaluated and compared. For the SIoT context, six

years of trust management systems and trust evaluation approaches were studied, categorized, and analysed. Various trust management methods and techniques for the IoT were examined. Later, it was found SIoT would faces a number of issues that require cutting-edge solutions to be developed.

REFERENCES

[1] Azad, M. A., Bag, S., Hao, F., & Shalaginov, A. (2020). Decentralized self-enforcing trust management system for social internet of things. Internet of Things Journal IEEE, 7(4), 2690-2703. https://doi.org/10.1109/JIOT.2019.2962282

[2] S. Verma, Y. Kawamoto, Z. M. Fadlullah, H. Nishiyama, and N. Kato. A survey on network methodologies for real-time analytics of massive IoT data and open research issues. IEEE Communications Surveys Tutorials, 19(3):1457–1477, third quarter 2017. ISSN 1553-877X. Doi: 10.1109/COMST.2017.2694469.

[3] N. C. Luong, D. T. Hoang, P. Wang, D. Niyato, D. I. Kim, and Z. Han. Data collection and wireless communication in internet of things (IoT) using economic analysis and pricing models: A survey. IEEE Communications Surveys Tutorials, 18(4):2546–2590, Fourth quarter 2019. ISSN

1553-877X. doi: 10.1109/COMST.2016.2582841. [4]C. Sobin, "A survey on architecture, protocols and challenges in IoT," Wireless

Pers. Commun., vol. 112, pp. 1383–1429, Jan.

2020

[4] Musa G. Samaila, Miguel Neto, Diogo A.B. Fernandes, M´ario M. Freire, and Pedro R.M. Inacio. Security challenges of the internet of things. 2017.

[5] A. Mosenia and N. K. Jha. A comprehensive study of security of internet of-things. IEEE Transactions on Emerging Topics in Computing, 5(4):586–602, Oct 2017. ISSN 2168-6750. Doi: 10.1109/TETC.2016.2606384.

[6] Chen, I. R., Guo, J., & Bao, F. (2019). Trust management for SOA-based IoT and its application to service composition. IEEE Transactions on Services Computing, 9(3), 482-495. https://doi.org/10.1109/TSC.2014.2365797

[7] S. Singh and N. Singh. Social Internet of things (SIoT): Security challenges, business opportunities amp; reference architecture for e-commerce. In 2015 International Conference on Green Computing and Internet of Things (ICG945 CIoT), pages 1577–1581, Oct 2015. Doi: 10.1109/ICGCIoT.2015.7380718.

[8] Kim, B.-S., Hassan, S., & Khan, M. K. (2018). Trust management techniques for the Social Internet of Things: A survey. IEEE Access, 7, 29763-29787. https://doi.org/10.1109/ACCESS.2018.2880838

[9] Alsharif Abuadbba, Ibrahim Khalil, and Mohammed Atiquzzaman. Ro950 bust privacy preservation and authenticity of the collected data in cognitive radio network-walsh-hadamard based steganographic approach. Pervasive Mob. Compute. 22(C):58– 70, September 2015. ISSN 1574-1192.

Doi: 10.1016/j.pmcj.2015.02.003. URL http://dx.doi.org/10.1016/j.pmcj.2015.02.003.

[10] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash.Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys Tutorials, 17(4):2347–2376, Fourth quarter 2015. ISSN 1553-877X. Doi: 10.1109/COMST.2015.2444095.

[11] Lin, Z. & Dong, L. (2020). Clarifying trust in social Internet of Things. IEEE Transactions on Knowledge and Data Engineering, 30(2). https://doi.org/10.1109/TKDE.2017.2762678

[12] M. Frustaci, P. Pace, G. Aloi, and G. Fortino. Evaluating critical security issues of the IoT world: Present and future challenges. IEEE Internet of Things Journal, 5(4):2483–2495, Aug 2018. ISSN 2327-4662. Doi: 10.1109/JIOT.2017.2767291.

[13] M. R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. A. Grieco,G. Boggia, and M. Dohler. Standardized protocol stack for the internet of (important) things. IEEE Communications Surveys Tutorials, 15(3):1389–1406, Third 2013. ISSN 1553877X. Doi: 10.1109/SURV.2012.111412.00158.

[14] V. Gazis. A survey of standards for machine-to-machine and the internet of things. IEEE Communications Surveys Tutorials, 19(1):482–511, first quarter 2017. ISSN 1553-877X. Doi: 10.1109/COMST.2016.2592948.

[15] Zheng Yan, Peng Zhang, and Athanasios V. Vasilakos. A survey on trust management for internet of things. Journal of Network and Computer Applications, 42:120 – 134, 2014. ISSN 1084-8045. Doi: https://doi.org/10.1016/j.jnca.2014.01.014. URL http://www.sciencedirect.com/

Science/article/pii/S1084804514000575.

[16] A. Arabsorkhi, M. Sayad Haghighi, and R. Ghorbanloo. A conceptual trust model for the internet of things interactions. In 2016 8th International Symposium on Telecommunications (IST), pages 89–93, Sept 2016.doi: 10.1109/ISTEL.2016.7881789.

[17] C. Bormann, M. Ersue, and A. Keranen. Terminology for Constrained Node Networks. RFC, RFC Editor, May 2014. URL https://www.rfc-editor.org/info/rfc7228.

[18] U. Raza, P. Kulkarni, and M. Sooriyabandara. Low power wide area networks: An overview. IEEE Communications Surveys Tutorials, 19(2):855–873, second quarter 2017. ISSN 1553-877X. Doi: 10.1109/COMST.990 2017.2652320.

[19] Laxman Sayana and Bineet Joshi. Security issues in internet of things. April 2016.

[20] M. Z. A. Bhuiyan, G. Wang, W. Tian, M. A. Rahman, and J. Wu.Content-centric event-insensitive big data reduction in internet of things.995 In GLOBECOM 2017 - 2017 IEEE Global Communications Conference, pages 1–6, Dec 2017. Doi: 10.1109/GLOCOM.2017.8254997.

[21] Brian Cusack, Zhuang Tian, and Ar Kar Kyaw. Identifying dos and ddos attack origin: Ip traceback methods comparison and evaluation for iot.In Nathalie Mitton, Hakima Chaouchi, Thomas Noel, Thomas Watteyne,1000 Alban Gabillon, and Patrick Capolsini, editors, Interoperability, Safety and Security in IoT, pages 127–138, Cham, 2017. Springer International Publishing.

[22] M. A. Muhal, X. Luo, Z. Mahmood, and A. Ullah. Physical unclonable function based authentication scheme for smart devices in internet 1005 of things. In 2018 IEEE International Conference on Smart Internet of Things (SmartIoT), pages 160– 165, Aug 2018. Doi: 10.1109/SmartIoT. 2018.00037.

[23] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo. Design of secure user authenticated key management protocol for generic IoT net1010 works. IEEE Internet of Things Journal, 5(1):269–282, Feb 2018. ISSN 2327-4662. Doi: 10.1109/JIOT.2017.2780232. 51

[24] Oualhaj, O. A., Mohamed, A., Guizani, M., and Erbad, A. (2020). Blockchain based decentralized trust management framework. International Wireless Communications and Mobile Computing (IWCMC 2020), Limassol, Cyprus, 2210- 2215. https://doi.org/10.1109/IWCMC48107.2020.9148247

[25] Kowshalya, A. M. & Valarmathi, M. L. (2017). Trust management for reliable decision making among social objects in the Social Internet of Things. IET Networks, 6(4), 75-80. https://doi.org/10.1049/iet-net.2017.0021

[26] He, Y., Han, G., Jiang, J., Wang, H., & Martinez-Garcia, M. (2020). A trust update mechanism based on reinforcement learning in underwater acoustic sensor networks. IEEE Transactions on Mobile Computing. https://doi.org/10.1109/TMC.2020.3020313

[27] Sagar, S., Mahmood, A., Sheng, Q. Z., & Zhang, W. E. (2020). Trust computational heuristic for social internet of things: A machine learning-based approach. IEEE International Conference on Communication. https://doi.org/10.1109/ICC40277.2020.9148767

[28] Dong Chen, Guiran Chang, Dawei Sun, Jiajia Li, Jie Jia, and Xingwei Wang. Trm-iot: A trust management model based on fuzzy reputation for internet of things. 2011.

[29] I. Chen, J. Guo, and F. Bao. Trust management for soa-based IoT and its application to service composition. IEEE Transactions on Services 1035 Computing, 9(3):482–495, May 2016. ISSN 1939-1374. Doi: 10.1109/TSC.2014.2365797.

[30] Zhikui Chen, Ruochuan Ling, Chung-Ming Huang, and Xu Zhu. A scheme of access service recommendation for the social internet of things. International Journal of Communication Systems, 29(4):694–706. Doi: 521040 10.1002/dac.2930. URL https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.2930.

[31] Mauro Conti, Ali Dehghantanha, Katrin Franke, and Steve Watson. Internet of things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78:544 – 546, 2018. ISSN 0167-1045 739X. Doi: https://doi.org/10.1016/j.future.2017.07.060. URL http://www.sciencedirect.com/science/article/pii/S0167739X17316667.

[32] M. Ma, D. He, N. Kumar, K. R. Choo, and J. Chen. Certificateless searchable public key encryption scheme for industrial internet of things .IEEE Transactions on Industrial Informatics, 14(2):759–767, Feb 2018.1050 ISSN 1551-3203. Doi: 10.1109/TII.2017.2703922.

[33] Neetesh Saxena, Santiago Grijalva, and Narendra S. Chaudhari. Authentication protocol for an IoT-enabled lte network. ACM Trans. Internet Technol., 16(4):25:1–25:20, December 2016. ISSN 1533-5399. Doi: 10.1145/2981547. URL http://doi.acm.org/10.1145/2981547.1055

[34] K. Renaud and D. G´alvez-Cruz. Privacy: Aspects, definitions and a multi-faceted privacy preservation approach. In 2010 Information Security for South Africa, pages 1–8, Aug 2010. Doi: 10.1109/ISSA.2010.5588297.

[35] Jin-Hee Cho, Kevin Chan, and Sibel Adali. A survey on trust modeling. ACM Compute. Surv., 48(2):28:1–28:40, October 2015. ISSN 0360-0300. 1060 doi: 10.1145/2815595. URL http://doi.acm.org/10.1145/2815595.

[36] F. D. Hudson. Enabling trust and security: Tippss for IoT. IT Professional, 20(2):15–18, Mar 2018. ISSN 1520-9202. Doi: 10.1109/MITP.2018. 021921646.

[37] Daoxi Xiu and Zhaoyu Liu. A formal definition for trust in distributed 1065 systems. In Jianying Zhou, Javier Lopez, Robert H. Deng, and Feng Bao, editors, Information Security, pages 482–489, Berlin, Heidelberg, 2005.Springer Berlin Heidelberg. ISBN
978-3-540-31930-6.53

[38] M. Nitti, R. Girau, and L. Atzori. Trustworthiness management in the social internet of things. IEEE Transactions on Knowledge and Data 1070 Engineering, 26(5):1253–1266, May 2014. ISSN 1041-4347. Doi: 10.1109/TKDE.2013.105.

[39] Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem, and Faiz Alotaibi. Internet of things security: A survey. Journal of Network and Computer Applications, 88:10 – 28, 2017. ISSN 1084-1075 8045. Doi: https://doi.org/10.1016/j.jnca.2017.04.002. URL http://www.sciencedirect.com/science/article/pii/S1084804517301455.

[40] Javier Lopez, Ruben Rios, Feng Bao, and Guilin Wang. Evolving privacy: From sensors to the internet of things. Future Generation Computer Systems, 75:46 – 57, 2017. ISSN 0167-739X. Doi: https://doi.org/10.1016/1080 j.future.2017.04.045. URL http://www.sciencedirect.com/science/article/pii/S0167739X16306719.

[41] Antonio Kung, Frank Kargl, Santiago Suppan, Jorge Cuellar, Henrich C.P¨ohls, Adam Kapovits, Nicol'as Notario McDonnell, and Yod Samuel Martin. A Privacy Engineering Framework for the Internet of Things, pages1085 163–202. Springer International Publishing, Cham, 2017.

[42] Elisa Bertino, Kim-Kwang Raymond Choo, Dimitrios Georgakopolous, and Surya Nepal. Internet of things (IoT): Smart and secure service delivery. ACM Trans. Internet Technol., 16(4):22:1–22:7, December 2016.ISSN 1533-5399. Doi:
10.1145/3013520. URL http://doi.acm.org/10.1090 1145/3013520.

[43] M. Hassanalieragh, A. Page, T. Soyata, G. Sharma, M. Aktas, G. Mateos,B. Kantarci, and S. Andreescu. Health monitoring and management using internet-of-things (IoT) sensing with cloud-based processing: Opportunities and challenges. In 2015 IEEE International Conference on Services1095 Computing, pages 285–292, June 2015. doi: 10.1109/SCC.2015.47.54

[44] Shahid Raza, Linus Wallgren, and Thiemo Voigt. Svelte: Real-time intrusion detection in the internet of things. Ad Hoc Networks, 11(8):2661 –2674, 2013. ISSN 1570-8705. doi: 04.014. URL http://www.sciencedirect.com/science/article/pii/1100 S1570870513001005.

[45] Z. A. Khan and P. Herrmann. A trust based distributed intrusion detection mechanism for internet of things. In 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), pages 1169–1176, March 2017. Doi: 10.1109/AINA.2017.161.1105

[46] Bruno Bogaz Zarpelo, Rodrigo Sanches Miani, Cludio Toshio Kawakani, and Sean Carlisto de Alvarenga. A survey of intrusion detection in internet of things. J. Netw. Compute. Appl., 84(C):25–37, April 2017. ISSN 1084-8045. Doi: 10.1016/j.jnca.2017.02.009. URL https://doi.org/10.1016/j.jnca.2017.02.009.1110

[47] Yaniv Harel, Irad Ben Gal, and Yuval Elovici. Cyber security and therole of intelligent systems in addressing its challenges. ACM Trans. Intell.Syst. Technol., 8(4):49:1–49:12, May 2017. ISSN 2157-6904. doi: 10.1145/3057729. URL http://doi.acm.org/10.1145/3057729.

[48] Abdallah Makhoul, Christophe Guyeux, Mourad Hakem, and Jacques M.1115 Bahi. Using an epidemiological approach to maximize data survival inthe internet of things. ACM Trans. Internet Technol., 16(1):5:1–5:15,January 2016. ISSN 1533-5399. Doi: 10.1145/2812810. URL http://doi.acm.org/10.1145/2812810.

[49] A. Barki, A. Bouabdallah, S. Gharout, and J. Traor´e. M2m security: 1120 Challenges and solutions. IEEE Communications Surveys Tutorials, 18(2):1241–1254, second quarter 2016. ISSN 1553-877X. Doi: 10.1109/COMST.2016.2515516.

[50] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma, and J. Ott. Security and privacy in device-to-device (d2d) communication: A review. IEEE551125 Communications Surveys Tutorials, 19(2):1054–1079, second quarter 2017.ISSN 1553877X. Doi: 10.1109/COMST.2017.2649687.

[51] Mangement Ge, Jin B. Hong, Walter Guttmann, and Dong Seong Kim. A framework for automating security analysis of the internet of things. Journal of Network and Computer Applications, 83:12 – 27, 2017. ISSN 1084-1130 8045. doi: https://doi.org/10.1016/j.jnca.2017.01.033. URL http://www.sciencedirect.com/science/article/pii/S1084804517300541.

[52] J. Granjal, E. Monteiro, and J. S´a Silva. Security for the internet of things: A survey of existing protocols and open research issues. IEEE Communications Surveys Tutorials, 17(3):1294–1312, third quarter 2015.1135 ISSN 1553-877X. doi:
10.1109/COMST.2015.2388550.

54] Y. Liu, Z. Chen, F. Xia, X. Lv, and F. Bu. A trust model based on service classification in mobile services. In 2010 IEEE/ACM Int'l Conference on Green Computing and Communications Int'l Conference on Cyber, Physical and Social Computing, pages 572–577, Dec 2010. doi: 1145 10.1109/GreenCom-CPSCom.2010.19.

[55] Rolf H. Weber. Internet of things: Privacy issues revisited. Computer Law & Security Review, 31(5):618 – 627, 2015. ISSN 0267-3649. doi: https://doi.org/10.1016/j.clsr.2015.07.002. URL http://www.sciencedirect.com/science/article/pii/S0267364915001156.1150

[56] S. Sicari, A. Rizzardi, L.A. Grieco, and A. Coen-Porisini. Security, privacy and trust in internet of things: The road ahead. Computer Networks, 76:146 – 164, 2015. ISSN 1389-1286. doi: https://doi.org/10.1016/j.comnet.562014.11.008. URL http://www.sciencedirect.com/science/article/ pii/S1389128614003971.1155

[57] Arbia Riahi Sfar, Enrico Natalizio, Yacine Challal, and Zied Chtourou. A roadmap for security challenges in the internet of things. Digital Communications and Networks, 4(2):118 – 137, 2018. ISSN 2352-8648. doi: https://doi.org/10.1016/j.dcan.2017.04.003. URL http://www.sciencedirect.com/science/article/pii/S2352864817300214.1160

[58] R. Roman, P. Najera, and J. Lopez. Securing the internet of things. Computer, 44(9):51–58, Sept 2011. ISSN 0018-9162. doi: 10.1109/MC.2011.291.

[59] J. Daubert, A. Wiesmaier, and P. Kikiras. A view on privacy amp; trust in IoT. In 2015 IEEE International Conference on Communication Workshop1165 (ICCW), pages 2665–2670, June 2015. doi: 10.1109/ICCW.2015.7247581.

[60] Kai-Di Chang and Jiann-Liang Chen. A survey of trust management in wsns, internet of things and future internet. KSII Transactions on Internet and Information Systems, 6:5 – 23, 2012. doi:10.3837/tiis.2012.01.001.

[61] Sridipta Misra, Muthucumaru Maheswaran, and Salman Hashmi. Vulnerable Features and Threats, chapter 3, pages 19–38. Springer Briefs in Electrical and Computer Engineering, 2017.

[62] A. F. Skarmeta, J. L. Hern´andez-Ramos, and M. V. Moreno. A decentralized approach for security and privacy challenges in the internet of things. In 2014 IEEE World Forum on Internet of Things (WF-IoT),1175 pages 67–72, March 2014. doi: 10.1109/WF-IoT.2014.6803122.

[63] Qiu xin WU and Han LI. Secure solution of trusted internet of things base on tcm. The Journal of China Universities of Posts and Telecommunications, 20:47 – 53, 2013. ISSN 1005-8885. doi: https://doi.org/10.1016/S1005-8885(13)60222-8. URL http://www.sciencedirect.com/

1180 science/article/pii/S1005888513602228.

[64] Carmen Fernandez-Gago, Francisco Moyano, and Javier Lopez. Modelling trust dynamics in the internet of things. Information Sciences, 396:72 – 82, 2017. ISSN 0020-0255. doi: https://doi.org/10.1016/j.ins.2017.02.039. URL http://www.sciencedirect.com/science/article/pii/ 1185 S0020025517305364.

[65] Nguyen B. Truong, Upul Jayasinghe, Tai-Won Um, and Gyu Myoung Lee. A survey on trust computation in the internet of things. The Journal ofThe Korean Institute of Communication Sciences, 33(2):10–27, 2016.

[66] Jia Guo, Ing-Ray Chen, and Jeffrey J.P. Tsai. A survey of trust1190 computation models for service management in internet of things systems. Computer Communications, 97:1 – 14, 2017. ISSN 0140-3664.doi: https://doi.org/10.1016/j.comcom.2016.10.012. URLhttp://www.sciencedirect.com/science/article/pii/S0140366416304959.

[67] V. Suryani, Selo, and Widyawan. A survey on trust in internet of things. In 2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE), pages 1–6, Oct 2016. doi:10.1109/ICITEED.2016.7863238.

[68] C. Shepherd, G. Arfaoui, I. Gurulian, R. P. Lee, K. Markantonakis,R. N. Akram, D. Sauveron, and E. Conchon. Secure and trusted ex1200 ecution: Past, present, and future - a critical review in the context

Of the internet of things and cyber-physical systems. In 2016 IEEE Trustcom/BigDataSE/ISPA, pages 168–177, Aug 2016. Doi: 10.1109/TrustCom.2016.0060.

[69] Pu Wang and Peng Zhang. A review on trust evaluation for internet of things. In Proceedings of the 9th EAI International Conference onMobile Multimedia Communications, MobiMedia '16, pages 34–39, ICST, Brussels, Belgium, Belgium, 2016. ICST (Institute for Computer Sciences,Social-Informatics and Telecommunications Engineering). ISBN 978-581-63190-104-1. URLhttp://dl.acm.org/citation.cfm?id=3021385.1210 3021392.

[70] Wafa Abdelghani, Corinne Amel Zayani, Ikram Amous, and Florence S`edes. Trust management in social internet of things: A survey. In Yogesh K. Dwivedi, Matti M¨antym¨aki, M.N. Ravishankar, Marijn Janssen,Marc Clement, Emma L. Slade, Nripendra P. Rana, Salah Al-Sharhan,1215 and Antonis C. Simintiras, editors, Social Media: The Good, the Bad, and the Ugly, pages 430–441, Cham, 2016. Springer International Publishing. ISBN 978-3-319-45234-0.

[71] P.P. Ray. A survey on internet of things architectures. Journal of King Saud University - Computer and Information Sciences, 30(3):2911220 – 319, 2018. ISSN 1319-1578. doi:https://doi.org/10.1016/j.jksuci.2016.10.003. URL http://www.sciencedirect.com/science/article/pii/ S1319157816300799.

[72] Francisco Moyano, Carmen Fernandez-Gago, and Javier Lopez. A conceptual framework for trust models. In Simone Fischer-H¨ubner, Sokratis Katsikas, and Gerald Quirchmayr, editors, Trust, Privacy and Security in Digital Business, pages 93–104, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg. ISBN 978-3-642-32287-7.

[73] L. Nastase. Security in the internet of things: A survey on application layer protocols. In 2017 21st International Conference on Control Systems and Computer Science (CSCS), pages 659–666, May 2017. doi: 10.1109/CSCS.2017.101.

[74] I. Chen, F. Bao, and J. Guo. Trust-based service management for social internet of things systems. IEEE Transactions on Dependable and Secure Computing, 13(6):684–696, Nov 2016. ISSN 1545-5971. doi: 10.1109/1235 TDSC.2015.2420552.

[75] S. E. A. Rafey, A. Abdel-Hamid, and M. A. El-Nasr. Cbstm-iot: Context based social trust model for the internet of things. In 2016 International Conference on Selected Topics in Mobile Wireless Networking (MoWNeT), pages 1–8, April 2016. doi: 10.1109/MoWNet.2016.7496623.

[76] Q. Nguyen Vu, S. Hassas, F. Armetta, B. Gaudou, and R. Canal. Combining trust and self-organization for robust maintaining of information coherence in disturbed mas. In 2011 IEEE Fifth International Conference on Self-Adaptive and Self-Organizing Systems, pages 178–187, Oct 2011.doi: 10.1109/SASO.2011.29.

[77] M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized trust management. In Proceedings 1996 IEEE Symposium on Security and Privacy, pages164–173, May 1996. doi: 10.1109/SECPRI.1996.502679.

[78] Min Li, Xiaoxun Sun, Hua Wang, Yanchun Zhang, and Ji Zhang.Privacy-aware access control with trust management in web ser1250 vice. World Wide Web, 14(4):407–430, Jul 2011. ISSN 1573-1413.doi: 10.1007/s11280-011-0114-8. URL https://doi.org/10.1007/s11280-011-0114-8.

[79] Francisco Moyano, Carmen Fernandez-Gago, and Javier Lopez. A model-driven approach for engineering trust and reputation into soft1255 ware services. Journal of Network and Computer Applications, 69:134– 151, 2016. ISSN 1084-8045. doi: https://doi.org/10.1016/j.jnca.2016.04.018. URL http://www.sciencedirect.com/science/article/pii/S1084804516300698.

[80] Francisco Moyano, Carmen Fernandez-Gago, and Javier Lopez. A frame1260 work for enabling trust requirements in social cloud applications. Requirements Engineering, 18(4):321–341, Nov 2013. ISSN 1432-010X.doi: 10.1007/s00766-013-0171-x. URL https://doi.org/10.1007/s00766-013-0171-x.

[81] Francisco Moyano, Carmen Fernandez-Gago, and Javier Lopez. Building 1265 trust and reputation in: A development framework for trust models implementation. In Audun Jøsang, Pierangela Samarati, and Marinella Petrocchi, editors, Security and Trust Management, pages 113–128, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg. ISBN 978-3-642-38004-4.

[82] A. Sharma, E. S. Pilli, A. P. Mazumdar, and M. C. Govil. A framework to manage trust in internet of things. In 2016 International Conferenceon Emerging Trends in Communication Technologies (ETCT), pages 1–5,Nov 2016. doi: 10.1109/ETCT.2016.7882970.

[83] K. Zhao and L. Pan. A machine learning based trust evaluation framework for online social networks. In 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, pages 69–74, Sept 2014. doi: 10.1109/TrustCom.2014.13.

[84] Wenjun Jiang, Guojun Wang, Md Zakirul Alam Bhuiyan, and Jie Wu.Understanding graph-based trust evaluation in online social networks:Methodologies and challenges. ACM Compute. Surv., 49(1):10:1–10:35,1280 May 2016. ISSN 0360-0300. doi: 10.1145/2906151. URL http://doi.acm.org/10.1145/2906151.

[85] Wenjun Jiang, Guojun Wang, Md Zakirul Alam Bhuiyan, and Jie Wu. Understanding graph-based rust evaluation in online social networks:Methodologies and challenges. ACM Compute. Surv., 49(1):10:1–10:35,1285 May 2016. ISSN 0360-0300. doi: 10.1145/2906151. URL http://doi.acm.org/10.1145/2906151.

[86] N. Kumar, N. Chilamkurti, and S. C. Misra. Bayesian coalition game for the internet of things: an ambient intelligence-based evaluation. IEEE Communications Magazine, 53(1):48–55, January 2015. ISSN 0163-6804.1290 doi: 10.1109/MCOM.2015.7010515.

[87] Randolph W. Hall. Discrete models/continuous models. Omega, 14(3):213– 220, 1986. ISSN 0305-0483. doi: https://doi.org/10.1016/0305-0483(86)90040-X. URL http://www.sciencedirect.com/science/article/pii/030504838690040X.

[88] Yosra Ben Saied, Alexis Olivereau, Djamal Zeghlache, and Maryline Laurent. Trust management system design for the internet of things: A context-aware and multi-service approach. Computers & Security, 39:351 – 365, 2013. ISSN 0167-4048. doi: https://doi.org/10.1016/j.cose.2013.09.001. URL http://www.sciencedirect.com/science/article/1300 pii/S0167404813001302.

[89] Rodrigo Roman, Jianying Zhou, and Javier Lopez. On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10):2266 – 2279, 2013. ISSN 1389-1286.doi: https://doi.org/10.1016/j.comnet.2012.12.018. URL http://www.1305 sciencedirect.com/science/article/pii/S1389128613000054. Towards a Science of Cyber Security Security and Identity Architecture for the Future Internet.

[90] Keyur K Patel and Sunil M Pate. Internet of things-IoT: Definition, characteristics, architecture, enabling technologies, application & future chal1310 lenges. International Journal of Engineering Science and Computing, 6(5), May 2016. ISSN 2321 3361. doi: 10.4010/2016.1482.

[91] N. Kumar, S. Zeadally, and J. J. P. C. Rodrigues. Vehicular delay-tolerant networks for smart grid data management using mobile edge computing. IEEE Communications Magazine, 54(10):60–66, October 2016. ISSN1315 0163-6804. doi: 10.1109/MCOM.2016.7588230.

[92] Fenye Bao and Ing-Ray Chen. Trust management for the internet of things and its application to service composition. In 2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), pages 1–6, June 2012. doi: 10.1109/WoWMoM.2012.1320 6263792.

[93] Fenye Bao and Ing-Ray Chen. Dynamic trust management for internet of things applications. In Proceedings of the 2012 International Workshop on Self-aware Internet of Things, Self-IoT '12, pages 1–6, New York,NY, USA, 2012. ACM. ISBN 9781-4503-1753-5. doi: 10.1145/2378023.1325 2378025. URL http://doi.acm.org/10.1145/2378023.2378025.

[94] Bei Gong, Yu Zhang, and Yubo Wang. A remote attestation mechanism for the sensing layer nodes of the internet of things. Future Gener. Comput.Syst., 78(P3):867–886, January 2018. ISSN 0167-739X. doi: 10.1016/j.future.2017.07.034. URL https://doi.org/10.1016/j.future.2017.1330 07.034.

[95] P. De Meo, F. Messina, M. N. Postorino, D. Rosaci, and G. M. L. Sarn´e. A reputation framework to share resources into IoTbased environments. In 2017 IEEE 14th International Conference on Networking, Sensing and Control (ICNSC), pages 513–518, May 2017. doi: 10.1109/ICNSC.2017.1335 8000145.

[96] Qin Lin and Dewang Ren. Quantitative trust assessment method based on bayesian network. In 2016 IEEE Advanced Information Management,Communicates, Electronic and Automation Control Conference (IMCEC),pages 1861–1864, Oct 2016. doi: 10.1109/IMCEC.2016.7867540.

[97] Carolina V. L. Mendoza and Jo˜ao H. Kleinschmidt. Mitigating on-off attacks in the internet of things using a distributed trust management scheme. International Journal of Distributed Sensor Networks, 11(11):859731, 2015. doi: 10.1155/2015/859731. URL https://doi.org/10.1155/2015/859731.1345

[98] P. N. Mahalle, P. A. Thakre, N. R. Prasad, and R. Prasad. A fuzzy approach to trust based access control in internet of things. In Wireless VITAE 2013, pages 1–5, June 2013. doi:10.1109/VITAE.2013.6617083.

[99] J. Duan, D. Gao, D. Yang, C. H. Foh, and H. Chen. An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications. IEEE Internet of Things Journal, 1(1): 58–69, Feb 2014. ISSN 2327-4662. doi: 10.1109/JIOT.2014.2314132. Gu Lize, Wang Jingpei, and Sun Bin. Trust management mechanism for internet of things. China Communications, 11:148–156, 2014.

[101] W. Li, H. Song, and F. Zeng. Policy-based secure and trustworthy sensing for internet of things in smart cities. IEEE Internet of Things Journal, 5(2):716–723, April 2018. ISSN 2327-4662. doi: 10.1109/JIOT.2017. 2720635.

[102] Borja Bordel, Ram´on Alcarria, and Diego S´anchez-de Rivera. Detecting malicious components in large-scale internet-ofthings systems and architectures. pages 155–165, 2017.

[103] F. Bao, I. Chen, and J. Guo. Scalable, adaptive and survivable trust management for community of interest based internet of things systems. In 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS), pages 1–7, March 2013. doi: 10.1109/ISADS.2013.1365 6513398.

[104] H. Hellaoui, A. Bouabdallah, and M. Koudil. Tas-iot: Trust-based adaptive security in the IoT. In 2016 IEEE 41st Conference on Local Computer Networks (LCN), pages 599–602, Nov 2016. doi: 10.1109/LCN.2016.101.

[105] S. Namal, H. Gamaarachchi, G. MyoungLee, and T. Um. Autonomic trust management in cloud-based and highly dynamic IoT applications. In 2015ITU Kaleidoscope: Trust in the Information Society (K-2015), pages 1–8,Dec 2015. doi: 10.1109/Kaleidoscope.2015.7383635.

[106] Y. Ruan, A. Durresi, and L. Alfantoukh. Trust management framework for internet of things. In 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), pages 1013–1019, March 2016. doi: 10.1109/AINA.2016.136.

[107] K. A. R. Rehiman and S. Veni. A trust management model for sensor enabled mobile devices in IoT. In 2017 International Conference on SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pages 1380 807–810, Feb 2017. doi: 10.1109/ISMAC.2017.8058290.

[108] S.V Annlin and JebaB Paramasivan. False data injection attack and its countermeasures in wireless sensor networks. European Journal of Scientific Research, 82(2):248–257, 2012. ISSN 1450-216X.

[109] D. Wang, T. Muller, Y. Liu, and J. Zhang. Towards robust and effective trust management for security: A survey. In 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, pages 511–518, Sept 2014. doi: 10.1109/TrustCom.2014.65.

[110] Y. L. Sun, Z. Han, W. Yu, and K. J. R. Liu. A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks. In Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications, pages 1–13, April 2006. doi:10.1109/INFOCOM.2006.154.

[111] K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan, and M. Rajarajan. Host-based intrusion detection for vanets: A statistical approach to rogue node detection. IEEE Transactions on Vehicular Technology, 65(8):6703–6714, Aug 2016. ISSN 0018-9545. doi: 10.1109/TVT.2015.2480244.

[112] Giseop Noh, Young-Myoung Kang, Hayoung Oh, and Chong-Kwon Kim.Robust sybil attack defense with information level in online recommender systems. Expert Syst. Appl., 41(4):1781–1791, March 2014. ISSN 0957-1400 4174. doi: 10.1016/j.eswa.2013.08.077. URL http://dx.doi.org/10.1016/j.eswa.2013.08.077.

[113] Audun Josang and Jennifer Golbeck. Challenges for robust trust and reputation systems. 2012.

[114] I. Chen and J. Guo. Dynamic hierarchical trust management of mobile groups and its application to misbehaving node detection. In 2014 IEEE28th International Conference on Advanced Information Networking and Applications, pages 49–56, May 2014. doi: 10.1109/AINA.2014.13.

[115] E. Ayday and F. Fekri. Iterative trust and reputation management using belief propagation. IEEE Transactions on Dependable and Secure Com1410 putting, 9(3):375–386, May 2012. ISSN 1545-5971. doi: 10.1109/TDSC.2011.64.

[116] Linus Wallgren, Shahid Raza, and Thiemo Voigt. Routing attacks and countermeasures in the rpl-based internet of things. International Journal of Distributed Sensor Networks, 9(8):794326, 2013. doi: 10.1155/2013/1415 794326. URL https://doi.org/10.1155/2013/794326.

[117] C. Cervantes, D. Poplade, M. Nogueira, and A. Santos. Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet of things. In 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), pages 606– 611, May 2015. doi: 10.1109/1420 INM.2015.7140344.

[118] W. R. Pires, T. H. de Paula Figueiredo, H. C. Wong, and A. A. F.Loureiro. Malicious node detection in wireless sensor networks. In 18th International Parallel and Distributed Processing Symposium, 2004. Proceedings., pages 24–, April 2004. doi: 10.1109/IPDPS.2004.1302934.1425

[119] Pavan Pongle and Gurunath Chavan. Article: Real time intrusion and wormhole attack detection in internet of things. International Journal of Computer Applications, 121(9):1–9, July 2015. Full text available.

[120] P. Deshpande, P. A. Kodeswaran, N. Banerjee, A. A. Nanavati, D. Chhabra, and S. Kapoor. M4m: A model for enabling social network based sharing in the internet of things. In 2015 7th International Conference on Communication Systems and Networks (COMSNETS), pages1–8, Jan 2015. doi: 10.1109/COMSNETS.2015.7098685.

[121] M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito. A subjective model for trustworthiness evaluation in the social internet of things. In 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC), pages 18–23, Sept 2012. doi: 10.1109/PIMRC.2012.6362662.

[122] Z. Lin and L. Dong. Clarifying trust in social internet of things. IEEE Transactions on Knowledge and Data Engineering, 30(2):234–248, Feb 1440 2018. ISSN 1041-4347. doi: 10.1109/TKDE.2017.2762678.

[123] Yan Liu and Kun Wang. Trust control in heterogeneous networks for internet of things. In 2010 International Conference on Computer Application and System Modeling (ICCASM 2010), volume 1, pages V1–632–V1–636,Oct 2010. doi: 10.1109/ICCASM.2010.5620458.

[124] Paolo Massa and Paolo Avesani. Trust-aware recommender systems. In Proceedings of the 2007 ACM Conference on Recommender Systems, RecSys '07, pages 17–24, New York, NY, USA, 2007. ACM. ISBN 978-1-59593-730–8. doi: 10.1145/1297231.1297235. URL http://doi.acm.org/10.1145/1297231.1297235.

[125] Lijun Yang, Chao Ding, Meng Wu, and Kun Wang. Robust detection of false data injection attacks for data aggregation in an internet of things-based environmental surveillance. Computer Networks, 129:410 –428, 2017. ISSN 1389-1286. doi:

https://doi.org/10.1016/j.comnet.2017.05.027. URL http://www.sciencedirect.com/science/article/pii/1455 S1389128617302372. Special Issue on 5G Wireless Networks for IoT andBody Sensors.

[126] R. G. Dutta, X. Guo, and Y. Jin. Quantifying trust in autonomous system under uncertainties. In 2016 29th IEEE International System-on-Chip Conference (SOCC), pages 362–367, Sept 2016. doi: 10.1109/SOCC.2016.1460 7905511.

[127] J. G lowacka, J. Krygier, and M. Amanowicz. A trust-based situation awareness system for military applications of the internet of things. In 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), pages490–495, Dec 2015. doi: 10.1109/WFIoT.2015.7389103.

[128] X. Xu, N. Bessis, and J. Cao. An autonomic agent trust model for IoT systems. Procedia Computer Science, 21:107 – 113, 2013. ISSN 1877-0509. doi: https://doi.org/10.1016/j.procs.2013.09.016. URL http://www.sciencedirect.com/science/article/pii/S1877050913008090. The 4th International Conference on Emerging Ubiquitous Systems and Per1470 vasive Networks (EUSPN-2013) and the 3rd International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH).

[129] Jean Caminha, Angelo Perkusich, and Mirko Perkusich. A smart trust management method to detect on-off attacks in the internet of things. Security and Communication Networks, 2018:10, 2018. URL https://doi.org/10.1155/2018/6063456.

[130] Q. Li, S. Zhu, and G. Cao. Routing in socially selfish delay tolerant networks. In 2010 Proceedings IEEE INFOCOM, pages 1–9, March 2010.doi: 10.1109/INFCOM.2010.5462138.

[131] L. Atzori, A. Iera, and G. Morabito. Siot: Giving a social structure to the internet of things. IEEE Communications Letters, 15(11):1193–1195, November 2011. ISSN 1089-7798. doi:10.1109/LCOMM.2011.090911.111340.

[132] Silke and Holtmanns. Trust modeling and management: from social trust to digital trust. 2007. [132] E. de Matos et al., “Context information sharing for the Internet of Things: A survey,” Comput. Netw., vol. 166, Jan. 2020, Art. no. 106988.

[133] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R. ur Rasool, and W. Dou, “Complementing IoT services through software defined networking and edge computing: A comprehensive survey,” IEEE Commun. Surveys Tuts., vol. 22, no. 3, pp. 1761–1804, 3rd Quart., 2020

[134] M. A. Amanullah et al., “Deep learning and big data technologies for IoT security,” Comput. Commun., vol. 151, pp. 495–517, Feb. 2020.

[135] X. Fan, L. Liu, R. Zhang, Q. Jing, and J. Bi, “Decentralized trust management: Risk analysis and trust aggregation,” ACM Comput. Surveys, vol. 53, no. 1, pp. 1–33, 2020.