Faculty of Sciences and Bio-Engineering Sciences
Arthur Chomé

Security within the Internet Of things: A Literature Review

The Internet of Things is an emerging technology(Atzori, Iera, & Morabito, 2010) stemming from the increase in our environment of smart devices able to connect to other devices and generate and broadcast data to each other. It has grown to also encompass surrounding "things" of a human's living space such as home appliances, machines, transportation, business storage, etc. Fortino's book(Fortino & Trunfio, 2014) offers a clear overview on the matter in terms of technology, middleware and applications. The Internet of Things has also seen use as a way of improving businesses' supply chain(Ben-Daya, Hassini, & Bahroun, 2019) by analysing the raw data streams to extract useful information. As to work properly, one of its most important requirements is security in terms of data provenance, authentication, access control and secure communication. With the Internet of Things becoming more and more present in every day life, security has become more important than ever.

IoT's main characteristics(Oh & Kim, 2017) are its heterogeneity, resource constraints and dynamic nature. Having a diverse range of connected devices means they individually have different used protocols(Sethi & Sarangi, 2017), abstractions, performances and specifications with an absence of common security services. Its dynamic nature also brings difficulties in terms of key management and where to store them.

The dynamic nature of the Internet of Things adds challenges when generating keys(Roman, Alcaraz, Lopez, & Sklavos, 2011) and distributing them to nodes in the network. To encode data, one can go for a symmetric(Gomes, da Rosa Righi, & da Costa, 2014) or asymmetric key encryption scheme. The choice depends on the situation at hand and the trade-offs to be made involving management of the limited device resources(Katagi, Moriai, et al., 2008) and the scalability of the IoT network(Gomes et al., 2014).

Encryption prevents unauthorized third parties to access sent data. Before a secure communication can be established however, the sender must have a way to verify the identity of a network node before sending anything. Using certificate-based handshakes(Hummen, Shafagh, Raza, Voig, & Wehrle, 2014) is a possibility but it has been proven to be infeasible for a wide range of constrained device that comprise the Internet of Things. Researcher Rene Hummen from

Aachen University therefore proposes 3 alternate design approaches(Hummen, Ziegeldorf, Shafagh, Raza, & Wehrle, 2013) to reduce the overheads of the DTLS handshake. One way in doing so involves coding a node's identity in certificates and using them to authorize communication between two parties. A centralised approach involves using Registration Authorities(Liu, Xiao, & Chen, 2012) to recognize network players, they are access points in which other nodes can pre-register as to be identified on the network later on. Aside from guaranteeing authentication, they serve as bookkeeper the access request information of each node. Another paper(Jan, Nanda, He, Tan, & Liu, 2014) appears to have developed a light-weight authentication protocol to manage devices' resources based on Liu's paper.

When multiple devices interchange data in a network, one must be able to verify the integrity and correctness of data processed by the application. Researcher Muhammad Aman focuses on leveraging Physically Unclonable Functions (Aman, Chua, & Sikdar, 2017) to uniquely identify devices within a network. These are 'digital fingerprints' based on a microprocessor's unique physical variations from production. Blockchain(*Blockchain - Wikipedia*, n.d.) is a also a technique to be leveraged to ensure data provenance. Another of Aman's papers(Javaid, Aman, & Sikdar, 2018) proposes the combination of a blockchain variant and physically unclonable functions as to guarantee secure data provenance. Another way would be using a hash chain scheme(Suhail et al., 2018) to encode provenance where the hash of data would be prolonged for every new node that the data passes allowing for a checksum to be made in the end. Furthermore, data provenance can be secured using a mutual agreement scheme(Rangwala, Liang, Peng, Zou, & Li, 2016) between sender and receiver.

Certain resources ought to be used sparingly by authorised network nodes and this requires mechanisms to restrict access. One way to do it would be a centralised approach(Hernández-Ramos, Jara, Marin, & Skarmeta, 2013) with one node filtering access requests based on the policies at hand. A centralised access controls scheme like this brings considerable drawbacks(Ouaddah, Elkalam, & Ouahman, 2017) such a lowered scalability and a compromise in end-to-end security properties. An important researcher in the field of access control seems to be Aafaf Ouaddah from the Institute Mines-Telecom in Paris. He adapted blockchain(Ouaddah, Abou Elkalam, & Ait Ouahman, 2016) into a decentralized access control manager overcoming the problem of consensus reaching with distributed anonymous participants. Another paper(Ouaddah, Mousannif, Elkalam, & Ouahman, 2017) of Ouaddah proposes a capability-based access control scheme by giving tokens or keys to nodes that would grant them access to some restricted resources.

The Internet of Things represents a promising technology with a lot of its key requirements yet to be successfully implemented(Borgia, 2014). Ensuring security is a prerequisite to allow its proper functioning.

References

Aman, M. N., Chua, K. C., & Sikdar, B. (2017). Secure data provenance for the internet of things. In *Proceedings of the 3rd acm international workshop on iot privacy, trust, and security* (pp. 11–14).

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787–2805.

Ben-Daya, M., Hassini, E., & Bahroun, Z. (2019). Internet of things and supply chain management: a literature review. *International Journal of Production Research*, *57*(15-16), 4719–4742.

Blockchain - wikipedia. (n.d.). `https://en.wikipedia.org/wiki/Blockchain`. (Accessed on 11/06/2019)

Borgia, E. (2014). The internet of things vision: Key features, applications and open issues. *Computer Communications*, *54*, 1–31.

Fortino, G., & Trunfio, P. (2014). *Internet of things based on smart objects: Technology, middleware and applications.* Springer.

Gomes, M., da Rosa Righi, R., & da Costa, C. A. (2014). Internet of things scalability: Analyzing the bottlenecks and proposing alternatives. In *2014 6th international congress on ultra modern telecommunications and control systems and workshops (icumt)* (pp. 269–276).

Hernández-Ramos, J. L., Jara, A. J., Marin, L., & Skarmeta, A. F. (2013). Distributed capability-based access control for the internet of things. *Journal of Internet Services and Information Security (JISIS)*, *3*(3/4), 1–16.

Hummen, R., Shafagh, H., Raza, S., Voig, T., & Wehrle, K. (2014). Delegation-based authentication and authorization for the ip-based internet of things. In *2014 eleventh annual ieee international conference on sensing, communication, and networking (secon)* (pp. 284–292).

Hummen, R., Ziegeldorf, J. H., Shafagh, H., Raza, S., & Wehrle, K. (2013). Towards viable certificate-based authentication for the internet of things. In *Proceedings of the 2nd acm workshop on hot topics on wireless network security and privacy* (pp. 37–42).

Jan, M. A., Nanda, P., He, X., Tan, Z., & Liu, R. P. (2014). A robust authentication scheme for observing resources in the internet of things environment. In *2014 ieee 13th international conference on trust, security and privacy in computing and communications* (pp. 205–211).

Javaid, U., Aman, M. N., & Sikdar, B. (2018). Blockpro: Blockchain based data provenance and integrity for secure iot environments. In *Proceedings of the 1st workshop on blockchain-enabled networked sensor systems* (pp. 13–18).

Katagi, M., Moriai, S., et al. (2008). Lightweight cryptography for the internet of things. *Sony Corporation*, 7–10.

Liu, J., Xiao, Y., & Chen, C. P. (2012). Authentication and access control in the internet of things. In *2012 32nd international conference on distributed computing systems workshops* (pp. 588–592).

Oh, S.-R., & Kim, Y.-G. (2017). Security requirements analysis for the iot. In

2017 international conference on platform technology and service (platcon) (pp. 1–6).

Ouaddah, A., Abou Elkalam, A., & Ait Ouahman, A. (2016). Fairaccess: a new blockchain-based access control framework for the internet of things. *Security and Communication Networks*, *9*(18), 5943–5964.

Ouaddah, A., Elkalam, A. A., & Ouahman, A. A. (2017). Towards a novel privacy-preserving access control model based on blockchain technology in iot. In *Europe and mena cooperation advances in information and communication technologies* (pp. 523–533). Springer.

Ouaddah, A., Mousannif, H., Elkalam, A. A., & Ouahman, A. A. (2017). Access control in the internet of things: Big challenges and new opportunities. *Computer Networks*, *112*, 237–262.

Rangwala, M., Liang, Z., Peng, W., Zou, X., & Li, F. (2016). A mutual agreement signature scheme for secure data provenance. *environments*, *13*(14).

Roman, R., Alcaraz, C., Lopez, J., & Sklavos, N. (2011). Key management systems for sensor networks in the context of the internet of things. *Computers & Electrical Engineering*, *37*(2), 147–159.

Sethi, P., & Sarangi, S. R. (2017). Internet of things: architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, *2017*.

Suhail, S., Hong, C. S., Lodhi, M. A., Zafar, F., Khan, A., & Bashir, F. (2018). Data trustworthiness in iot. In *2018 international conference on information networking (icoin)* (pp. 414–419).