ITC595 Research Project - Emerging Security and Privacy issues in Internet of Things (IoT) & Smart Architectures: A Survey

Robert Shannon

ITC595 MIT, School of Computing & Mathematics, Charles Sturt University

flouride@hotmail.com

***ABSTRACT* – Internet of Things (IoT) is a global meshed architecture of internet connected devices comprising the full spectrum of technological devices. Internet of Things technology is a ubiquitous part of life and the** **entwined security and privacy concerns are perhaps the greatest challenge facing our society, which has become so heavily dependent on these interconnected devices for day to day life. The exponential adoption of these technologies across all sectors but primarily in consumer products, or so called Smart devices requires measures be taken to ensure security and privacy of users is paramount to reduce the potential for malicious activity and unintended consequences. This is a much studied topic and it encompasses a wide variety of research niches. This paper seeks to review the extensive body of knowledge present, while identifying and highlighting any gaps in the current literature on the subject of Internet of Thing and Smart Architectures, focusing on the critical issues. The challenge moving forward, future research needs to look at how to secure these low energy, low computing power devices so that the varied range of educational background of users is not a factor and likewise the architecture that these Internet of Things devices use to connect to the Internet is** **inherently secure.**

Keywords— Internet of Things, Security Challenges, Privacy Challenges.

INTRODUCTION

The Internet of Things (IoT) is still in its infancy stage, since the late 90’s when the term Internet of Things (IoT) was first conceived, though its inception was as early as the start of the 80’s when students at Carnegie Mellon University first connected a vending machine to a network. The IoT has progressively become ubiquitous across across all sectors, smart phones, wearable devices, automotive, smart home products, healthcare monitoring, manufacturing, retail, environmental monitoring, agriculture (Prathibha & Fatima, 2018, p. 673). There are differing estimates on how many IoT devices will be connected to the internet by the year 2020, 20 billion (Shah & Shah, 2018) – 50 billion (Evans, 2011, p. 3) and which sectors will have the highest concentration of devices.

The advent of IPv6 and its 2128 possible addresses coupled with the arrival of 5G and societies eagerness to embrace new technology will make it possible for this to become reality (Victer Paul & Saraswathi, 2017, p. 421) (Gunathilake, Buchanan & Asif, 2019, p. 707). Researchers are unanimously agreed that security and privacy related to this large influx of IoT devices and associated sensors is a large concern. A larger number of devices equals a greater attack surface for malicious activity (Santhosh & Gnanasekaran, 2017 p. 111).

The current mechanisms for security and privacy are insufficient and ill equipped to deal with the exponential growth in number of new devices and are incompatible with the IoT devices limitations of small storage space, short battery life and limited computing power (Gunathilake et al., 2019, p 707). These security mechanisms were originally designed for more robust devices.

There are wide-ranging proposed solutions including different Architectures, Blockchain, Fog/Edge Computing, Lattice-based Cryptography (LBC) and Lightweight Cryptography (LWC) encompassing Elliptical Curve Cryptography (ECC). The literature for this review was selected to highlight the current trends in the areas of cryptographic techniques, architectures, authentication and access control related to securing IoT.

1. Security Goals

The primary security goals for the IoT are the same as any other networked system (Sadkhan & Hamza, 2017, p. 60).

* Confidentiality - data confidentiality and privacy
* Integrity - data integrity and system integrity
* Availablity - avoid disruption of service
* Authentication – establishing trust and authenticity
* non-repudiation (accountability)

1. Cryptographic Systems

Cryptographic algorithms are used to secure data and communications between devices. Shah et al. has proposed an Elliptical Curve Internet of Things protocol (ECIOT) for key pair establishment which has a high efficiency for memory, battery and bandwidth utilization and put forward a strong argument for its adoption in IoT. While Sadkhan et al. provides an indepth analysis of current cryptosystems. Khalid, McCarthy, O’Neill & Liu compare LBC methods and provide a comprehensive analysis, benchmarking memory usage and bandwith in resource constrained devices.

Gunathilake et al. compares a number of lightweight cryptographic (LWC) methods to NIST’s gold standard, Advanced Encryption Standard (AES). Adat et al. agrees that lightweight cryptography should be adopted for IoT as it provides a similar level of security with a shorter length key making it better suited to low energy, low computing power devices.

1. Threats and Controls

Santhos et al. compares a range of existing security methods highlighting the issues that they address and the limitations of these methods.Adat et al. explains in detail the varied threats in Wireless Sensor Networks (WSN) across the physical, data link, network and transport layers. The authors suggest a multi-layered defence approach to IoT security. Using Intrusion Detection Systems (IDS) in between the devices and its border router and compares a number of these technologies.

1. Access Controls and User Authentication

Prathibha et al. discusses different authentication techniques and has proposed a solid IoT authentication framework. The immense volume of IoT devices makes authenticating each of these a cumbersome task. The authors suggest username, password and biometrics for authentication.

1. Security Policies

Santhos et al. briefly looks at the security policies that can be implemented at the different layers of the security architecture. Adat et al. suggests that well defined guidelines and practices are needed for users. That there should be mandatory education on basic cyber-hygine e.g. password length, changing default passwords to help users devices from trivially becoming part of a botnet. While Gunathilake et al. proposes outlining privacy policies as a solution.

FUTURE RESEARCH DIRECTION

There are differing ideas on the number and composition of the service layers in the IoT architecture. Adat et al., Lin et al. & Prathibha et al. explore both the four layered Service-oriented architecture (SoA) and three layer architectures.

Adat et al. Briefly touches on routing protocols and suggests that Routing Protocol for Low power and lossy networks (RPL) as a proposed solution to the limitations of the existing routing protocols. However it is still vulnerable to a range of common security issues, eavesdropping, resource exhaustion and malformed crafted packet congestion. This is an important topic for future research, to create a specific, robust routing protocol for IoT devices.

Blockchain does is not currently a workable solution for securing IoT devices because of its Consensus and Shared Ledger components. With the computational power of the devices being low for proof of work and the distributed database would put a drain on the limited storage volume. Perhaps future advancements will make it part of the possible solution. Singh et al. agrees that Blockchain technology currently will not be a good fit for the IoT devices themselves but that it could be beneficial for the API’s and cloud platforms.

Further research is required into secure cryptography in a post-Quantum computing world. Lattice-Based, Elliptic Curve and Elliptic curve Diffie-Hellman cryptographic methods are an important research topic moving forward.

CONCLUSION

There is great need to reach a consensus and standardization for security and privacy mechanisms in the IoT as society becomes more reliant on these devices. The challenge is the wide range of devices and associated communication protocols that make up the IoT.

Strong cryptographic methods that are specifically designed for low computing power, low energy and small storage capacity devices are needed that will also maintain a strong level of security in a post-quantum computing world.

Manufactures need to work towards producing devices that are secure by design and concentrate on interoperability.

The varying range of education levels of users is also a concern and efforts must be made to make security and privacy part of the initial design process so that people with limited security knowledge will not be impacted more adversely than more educated members of society.

Efforts must be made to educate end-users on the importance of basic cyber-hygine, however a multi-layered security approach is required as users typically view security as a roadblock to convenience.

REFERENCES

Adat, V. & Gupta, B.B. (2017). *Security in Internet of Things: issues, challenges, taxonomy, and architecture.* Retrieved from Springer.

Evans, D. (2011). The Internet of Things: *How the Next Evolution of the Internet Is Changing Everything.* Retrieved from CISCO.

Gunathilake, N.A., Buchanan & W.J., Asif, R. (2019). *Next Generation Lightweight Cryptography for Smart IoT Devices: Implementation, Challenges and Applications.* Retrieved from IEEE.

Khalid, A., McCarthy, S., O’Neill, M. & Liu, W. (2019) *Lattice-based Cryptography for IoT in A Quantum World: Are We Ready?* Retrieved from IEEE.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H. & Zhao, W. (2017). *A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy and Applications.* Retrieved from IEEE.

Ni, J., Zhang, K., Lin, X. & Shen, X. (2018). *Securing Fog Computing for Internet of Things Applications: Challenges and Solutions.* Retrieved from IEEE.

Prathibha, L. & Kaleem Fatima. (2018). *Exploring Security and Authentication Issues in Internet of Things.* Retrieved from IEEE.

Sadkhan, S.B. & Hamza, Z. (2017) *Cryptosystems used in IoT – Current Status and Challenges.* Retrieved from IEEE.

Samailia, M.G., Neto, M., Fernandes, D.A.B., Freire, M.M. & Inácio, P.R.M. (2018). *Challenges of securing Internet of Things devices: A survey.* Retrieved from Wiley Online.

Santhosh Krishna, B.V. & Gnanasekaran, T. (2017). *A Systematic Study of Security Issues in Internet-of-Things (IoT).* Retrieved from IEEE.

Shah, D.P. & Shah, P.G. (2018). *Revisiting Eliptical Curve Cryptography for Securing Internet of Things (IoT).* Retrieved from IEEE.

Singh, M., Singh, A. & Kim, S. (2018)  *Blockchain: A Game Changer for Securing IoT Data.* Retrieved from IEEE.

Victer Paul, P. & Saraswathi, R. (2017). *The Internet of Things – A Comprehensive Survey.* Retrieved from IEEE.