Security for IoT

Jigar Thakkar[a], Author Two[c], Author Three[a,c]

[a]*Master of IT,The University of Melbourne, Vic - 3010, Australia, thakkarj@student.unimelb.edu.au*
[b]*Address Two*
[c]*Some University*

Abstract

Smart devices which are part of the internet of things becoming an essential part of our lives with as days passing, Network connected devices are replacing many older devices. But some of this new smart device will not easily replaceable in future like body implanted pacemaker to IoT devices installed into space. So, for this kind of devices we have discuss some algorithms which cannot only work in limited resource IoT device but some algorithms are resilient to attack using a quantum computer.

Keywords: Internet of things, Post-quantum cryptography

1. Introduction

During last three decades connecting computers was a major focus, which becomes a global network of computers - the internet. The Internet has enabled us to do all kind of things which was science fiction just three decades ago like group video calling, www, and cryptocurrency. Next revolution which started to shaping is a network of devices like sensors, RFIDs and all kind of things- the internet of things. Imagine one day in the future your car will not only drive itself but downloads all the latest traffic information of that area and choose the best route to go to office from your home, after dropping you at office it'll find parking space by itself, and if car is needed any maintenance it will order parts by itself and goes itself to the manufacturer for repair.[1] When you finish your work in the evening and start going back towards your home, smartwatch or wristband measure your body temperature and send it to smart home/automatic temperature control system, so it starts maintaining temperature. When you go home, your home will know in which part of the home you are and what activity you are doing, Lights will start turning on/ off as you move.[2] When you go to the fridge it will not only show you which items it has but sophisticated algorithms will show you a list of recipes which you can prepare from that items, it also preorders items in case it is running out, and smart internet enabled drones delivers it at your doorstep.[3][4] IoT is not only for making human life easy but also healthy and safer, smart pacemaker directly sends data of heart to the doctor/or some smart AI system, so in case of emergency autonomous ambulance immediately takes the patient to the nearest hospital.[5] IoT is not only things doing smartly but also efficiently, and this is not future it all already started, according to estimate IoT will have more than 30 billion internet connected devices before 2020, If we consider 7 billion population of the world, it is more than 4 devices per person.[6] A huge chunk of this devices currently uses in industry, Australias largest independent oil and gas company Woodside has already deployed 200,000 smart internet-connected sensors for plant monitoring in Perth, Western Australia. IoT is not just helping to manage industries but making them more productive and safer.[7]

But this all shiny promises of IoT turns dark when it got hacked, Security is becoming major issues in IoT, now imagine some malicious blackhat criminals hack your car with you, and force you to pay a ransom, governments start spying you by your smart home. What can be more dangerous than your body implanted device like pacemaker get hack? Industries can be sabotaged in the same way, And this also started happening. Germany recently banned smart doll which was spying, the DDoS attack happened by the network of IP cameras which was used as IoT botnet. Attack by using IoT devices are much more disastrous than an attack on your computer because this can harm you physically, like bad robots of Hollywood movies.

Security is challenging for IoT because devices are itself very small with limited capabilities and resources, Most of the device is embedded devices with few MB of RAM and limited storage capabilities, Most common example is Raspberry Pi, but most industries built device are a custom build. The device resources not only issue for the

[☆]This is only an example

[*]I am corresponding author

Email addresses: author.one@mail.com (Jigar Thakkar), author.two@mail.com (Author Two), author.three@mail.com (Author Three)

URL: author-one-homepage.com (Jigar Thakkar)

[1]I also want to inform about...

[2]Small city

security but nature of the device itself can a problem, For example, some device is hard to replace once installed like devices used in some remote areas, or in space and inside the human body. Encryption algorithm also has a limited lifespan, like RSA, before 10 years even 512-bit key size RSA was hard to break, but nowadays standard is using 2048 bit RSA. As the progress quantum computers, the work of Proos and Zalka shows that using 4096 qubit quantum computer and Shor's algorithm RSA - 2048 bit can be broken. [8] Making key size larger is not the solution of this as computation power of quantum computers double as adding each new qubit, countering this we have to double RSA key size on each qubit, so it is clear that larger key size is an issue here for limited resources of IoT.

Our approach and proposed algorithms not only for making IoT secure today but we also emphasis making IoT secure even in quantum age. We have proposed a cloud-based system using ECC (elliptic curve cryptography) which can be used today. ECC is much powerful compared to RSA with smaller key size. 256bit ECC is equivalent in security compared to 3072bit key size of RSA and 384 bit ECC is equivalent in security compared 7680bit RSA. Because of this properties NSA (National Security Agency) use classified top secret information with 384bit keys.

After having sufficient Quantum computer ECC we have to replace ECC or make the key size bigger as RSA, according to estimate that it will still be unbreakable until next 15-20 years. Quantum computers cannot break all the encryption they only break encryption for bounded error quantum polynomial time BQP class problems, so NP-complete problems are out of reach for quantum computers. AES and SNOW are resilient to attack by a quantum computer. Another reason for choosing conventional AES and SNOW algorithm is this algorithm is relatively simple to use.

AES/SHA-3 which is block cipher and SNOW which is a stream cipher. [write something about AES] [write something about SNOW]

2. Related work

IoT implementation is pretty new but the potential risk of IoT also introduced in 1990 with the concept of IoT.[9] Unfortunately, most of the device is sold without security measures and old unpatched software and embedded operating systems. Another major problem is users not do the effort to change default passwords, this device can easily use for botnets. (This kind of unsecured devices can be found on www.shodan.io). Another challenge is IoT devices cannot be secure with firewall, anti-malware systems due to a smaller size, limited resources. Also, multilayer security is necessary for achieving any foolproof security measures. From the three perception layer, transportation layer and application layer [10]. Addressing security issues on each different layer is the best way in the direction of achieving a solution to a security issue. [11] application layer- Authentication is only of the scope of the paper.

Many different kinds of security architectures and algorithms proposed over last 2 decades. From that Blockchain and smart contract for IoT is the different and interesting approach for solving trust issues over a peer-to-peer network.[12]

Privacy of the user is also a huge concern, and it is hard to deal than security as various governments have a different view on it, it is more political than a technical issue.[13]

IoT devices often used in large quantity in the industry as internet-connected sensors, Cloud servers are used to integrate and manage them, Data mining and data visualization application runs on top of that. How a large number of IoT device can be managed using ECC, PKC are described in Secure authentication scheme for IoT and cloud servers paper by Sheetal Kalra. in his approach, all heavy work is done at the powerful cloud servers so small IoT embedded devices can only have to store small ECC key. [14]

[Related work of AES] [Related work of SNOW]

3. Authentication schemes

3.1. Elliptic curve cryptography

References

[1] M. Gerla, E.-K. Lee, G. Pau, U. Lee, Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds, in: Internet of Things (WF-IoT), 2014 IEEE World Forum on, IEEE, 2014, pp. 241–246.

[2] D.-M. Han, J.-H. Lim, Smart home energy management system using ieee 802.15. 4 and zigbee, IEEE Transactions on Consumer Electronics 56 (3).

[3] S. Helal, W. Mann, H. El-Zabadani, J. King, Y. Kaddoura, E. Jansen, The gator tech smart house: A programmable pervasive space, Computer 38 (3) (2005) 50–60.

[4] T. T. Zhou, D. T. Zhou, A. H. Zhou, Unmanned drone, robot system for delivering mail, goods, humanoid security, crisis negotiation, mobile payments, smart humanoid mailbox and wearable personal exoskeleton heavy load flying machine, uS Patent App. 14/285,659 (May 23 2014).

[5] A. I. Hernandez, F. Mora, M. Villegas, G. Passariello, G. Carrault, Real-time ecg transmission via internet for nonclinical applications, IEEE Transactions on Information Technology in Biomedicine 5 (3) (2001) 253–257.

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

[7] K. Bloede, G. Mischou, A. Senan, R. Koontz, Silicon Valley London THE INTERNET OF THINGS " Smart " Products Demand a Smart Strategy Using M&A for a Competitive Edge Investment Banking Research.
URL `http://www.woodsidecap.com/wp-content/uploads/2015/03/WCP-I`

[8] D. Beckman, A. N. Chari, S. Devabhaktuni, J. Preskill, Efficient networks for quantum factoring, Physical Review A 54 (2) (1996) 1034–1063. doi:10.1103/PhysRevA.54.1034.
URL `https://link.aps.org/doi/10.1103/PhysRevA.54.1034`

[9] J. Singh, T. Pasquier, J. Bacon, H. Ko, D. Eyers, Twenty security considerations for cloud-supported internet of things, IEEE Internet of Things Journal 3 (3) (2016) 269–284. doi:10.1109/JIOT.2015.2460333.

[10] X. Yang, Z. Li, Z. Geng, H. Zhang, A multi-layer security model for internet of things, Internet of things.

[11] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, D. Qiu, Security of the internet of things: Perspectives and challenges, Wireless Networks (2014) 2481–2501.

[12] K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access 4 (2016) 2292–2303.

[13] R. H. Weber, Internet of Things - New security and privacy challenges, Computer Law and Security Review 26 (1) (2010) 23–30. arXiv:96332259, doi:10.1016/j.clsr.2009.11.008.
URL http://dx.doi.org/10.1016/j.clsr.2009.11.008

[14] S. Kalra, S. K. Sood, Secure authentication scheme for IoT and cloud servers, Pervasive and Mobile Computing 24 (2015) 210–223. doi:10.1016/j.pmcj.2015.08.001.
URL http://dx.doi.org/10.1016/j.pmcj.2015.08.001