Cryptography Arbitration: Security Complexities of Cloud Enabled IoT in Europe and Beyond

Morgan Eldred, Hassan Alnoon and Sultan AlTamimi
School of Computing, University of Portsmouth, Portsmouth, U.K.

Keywords: Arbitration, Cloud, Cryptography, Data Protection, Internet of Things (IoT).

Abstract: The global nature of the Internet of Things and cloud has and will result in emerging challenges, such as whom is liable for data protection and security breaches of personal data. This paper puts forward the concept of '*cryptography arbitration*' and the need to design and architect legally compliant solutions. As the world becomes more interconnected we are likely to see more example of technology practices sweeping the globe and raising further data protection challenges; much like the fault lines between tectonic plates. This paper provides contribution by capturing some emerging impacts and challenges and how they relate to the internet of things and the need for solutions to have the appropriate cryptography safeguards.

1 INTERNET OF THINGS

There are many definitions of the internet of things (IoT) such as:

A network of items-each embedded with sensors-which are connected to the Internet (IEEE, 2014), "the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment" (Gartner). "The IoT links smart objects to the Internet. It can enable an exchange of data never available before, and bring users information in a more secure way" (Cisco).

For the purposes of this paper the definition of cloud enabled IoT taken is that it is it is a network of physical objects that contain embedded technologies to interact via the cloud with an external environment and uses the below layered three-tiered architecture, which is a modified lightweight version of IEEE P2413 standard for an Architectural Framework for the Internet of Things.

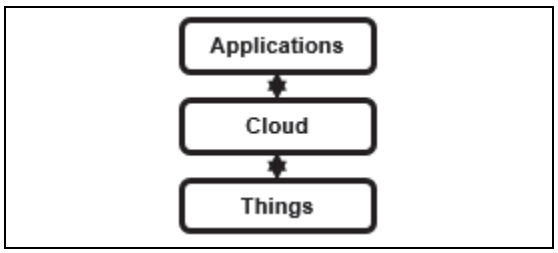

Figure 1: Cloud Enabled IoT.

This architecture consists of three critical layers:

Applications - are the software that controls, monitors and provides the user interface for the IoT application.

Cloud - is the network connectivity between the applications and physical equipment, identified as things.

Things - are the physical objects/device that contain embedded technology to communicate, sense and interact with the external format.

An example of the cloud internet of things, would be a drone that is used by a retailer to deliver purchased items. If the drone was to take a photograph of a facial images or car registration plate and inadvertently delivered that image by accident to a third party, then data protection acts could be breached, whom then would be liable and for what extended would they be liable. Considering that it has been indicated that the security of user's data has the highest priority and concern from users (Chang and Ramachandran, 2016). In such an example, if legal proceedings occurred, it could be beneficial to have a security framework that is verified and vetted by a security/cryptographic specialist. Lessons learned from the cloud computing adoption framework (CCAF) that has security suitable for business clouds, based upon a three major security technologies: firewall, identity management, and encryption based on the development of enterprise file sync and share

Eldred, M., Alnoon, H. and AlTamimi, S.
Cryptography Arbitration: Security Complexities of Cloud Enabled IoT in Europe and Beyond.
DOI: 10.5220/0005922103560361
In *Proceedings of the International Conference on Internet of Things and Big Data (IoTBD 2016)*, pages 356-361
ISBN: 978-989-758-183-0

technologies (Chang, Kuo, and Ramachandran, 2016).

2 CRYPTOGRAPHY

Cryptology is the art and science of making and breaking secret codes. Most people are interested in Cryptography which is the art of making secret codes. Cryptography is required in securing communication lines, whether it is wireless or wired communication lines against leakage of private and confidential information to undesirable individuals or parties while ensuring the basic pillars of information security are met which are confidentiality, integrity and availability of data; and also the authentication and non-repudiation of the individuals involved in the communication are protected.

While using cryptography in IoT the information security basics are important, it ensures that the devices and signals sent over the network are not compromised and ensures the safety and privacy of the user (Ning and Liu, 2012). The confidentiality of a signal being sent to a connected device over the cloud is important and is enforced by making sure that the signal is encrypted. If the signal sent is compromised an adversary can easily understand the type of signals being sent to the connected device, and therefore be able to take control of the device in question. Sending an encrypted signal can't be useful by itself, if an adversary can also change certain values in the encrypted signal without the device having a way of checking the integrity of the signal, an adversary can try random changes until a device reacts different and therefore understands more about how the device mechanism works. However having high security and integrity, with powerful cryptography and protocols used to communicate with the device would certainly cause delay in transmitting the signal to the device and therefore cause an issue with availability of the device mechanism. It is important when building an IoT communication between the different things in the cloud to ensure synergy between the three security pillars (confidentiality, integrity and accessibility) (CIA) (Ning, Liu and Yang, 2013).

Authentication is also another important aspect of information security that needs to be preserved in a cloud IoT environment. Being able to authenticate a device or a user is crucial to the communication that happens in IoT, if the authentication processes is not done in a proper cryptographic fashion using a strong secure protocols then both the devices and the user can be vulnerable. Communication protocols are complicated to build, most of the sophisticated attacks rely on weakness in the mathematical aspect of the protocols, formal verification methods are required to ensure such protocols are secure. Weakness in authentication and integrity of the communication can cause a repudiation of the messages sent, this can cause legal aspects, such as the leaking of personal data and that is why it is important that a protocol is capable of preserving the non-repudiation aspect of the communication. As provided before in the cloud IoT use case, if the image that was taken was not properly secured, what would be the liability of the company that did not properly secure the personal data of customers.

Cryptography Arbitration can be tricky due to the complexity that arises from establishing and implementing a cryptographic algorithm or protocols. To fully understand the underlying aspect of the cryptography a good combination of expertise in the fields of mathematics, computer science, and electrical engineering is required. To understand the complexity of cryptography, it is classified into the following categories:

Symmetric Key Cryptography, involves using the same key for both the encryption and decryption of data. Symmetric key crypto is typically used to create fast stream or block cipher algorithms. Popular symmetric ciphers are AES, 3-DES, TwoFish and RC4 etc.

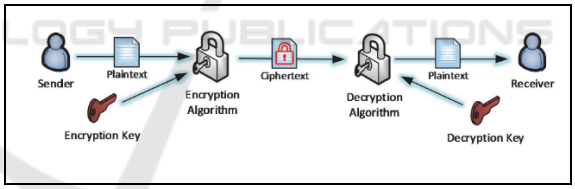

Figure 2: Symmetric Key Cryptography.

Asymmetric Key Cryptography, involves creating two separate keys, one for encryption and one for decryption of data. Asymmetric key crypto is typically used for transferring keys and digital signatures. Popular asymmetric ciphers are RSA, ECC etc.

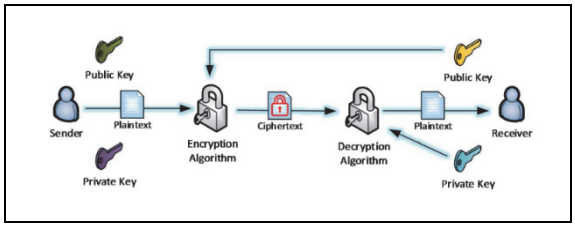

Figure 3: Asymmetric Key Cryptography.

Hashing Algorithm, involves creating techniques where we are able to map data of any size to data of fixed size (Digest). This process should be irreversible Hashing algorithms are typically used for data integrity. Popular hash ciphers are SHA-256, SHA3, MD5 etc.

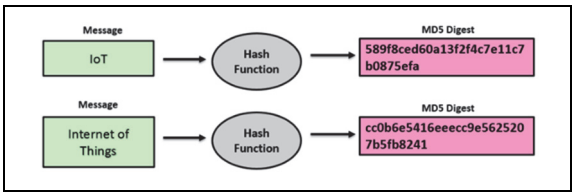

Figure 4: Hashing Algorithm Cryptography.

Message Authentication Code, is similar to a hash algorithm but provides the capability to authenticate the digest. MACs are typically used for Data Integrity and Authenticity. Popular MAC ciphers are HMAC, CMAC, CBC-MAC etc.

Key Management and Key Exchange Protocols, are an extremely important aspect of cryptography (Martin, 2006). Key management basically involves the generation, exchange, storage, use and replacement of keys used in the cryptosystems. The initial suspect in any cryptographic failure of a system would be due to weaknesses in the key management or the key exchange protocols. Most of the algorithms mentioned above have their source code and logic published online, that is mainly because these algorithm have been proven mathematically to be secure with today's available computational power. Though the keys used in any cryptosystem has to be well guarded and never be published publically or to any individual who shouldn't be part of that specific system. Key management even becomes a bigger challenge in IoT and cloud based solutions (NIST, 2013).

To do cryptography arbitration a person has to understand how these different cryptographic classification work together and the proper implementation procedures. Since most of the algorithms are published online, a crypto arbitrator has to understand the different mechanism to implement an algorithm, as a wrong implementation can cause a serious risk to the system. For example, the most used symmetric key cipher is AES, even though AES is a very powerful cipher, its implementation in both software and hardware can cause the overall security of the system to fail. While implementing AES you have to choose a mode-of-operation which is a technique that helps you implement the algorithm and deal with large amount of data to be encrypted. There are several modes-of-operation for example an ECB (Electronic Codebook) mode-of-operation can be very vulnerable whereas Cipher Feedback (CFB) can provide a better implementation security (Eng, 2008). A popular example that is used to generally help understand implementation difference is the following diagram:

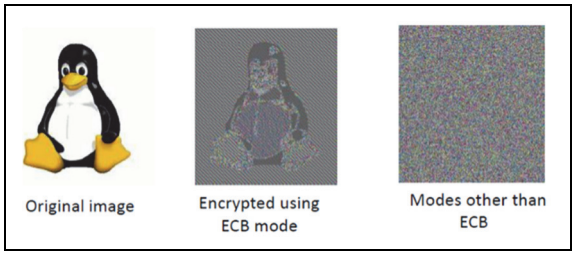

Figure 5: Cryptography differences.

Another attack on AES implementation which would also relate to IoT is a hardware based attack, where even a proper mode-of-operation usage can cause a side-channel attack on the algorithm. A very simple example of such an attack is power analysis attack, where an adversary monitors the power consumption of the device to understand more about the key or the algorithm being used (Gurkaynak, Oswald and Preneel, 2004). In the figure below a person doing a power analysis attack can understand more about the algorithm being used in the device by counting the number sets and how they relate to the inner works of the algorithm (algorithm rounds).

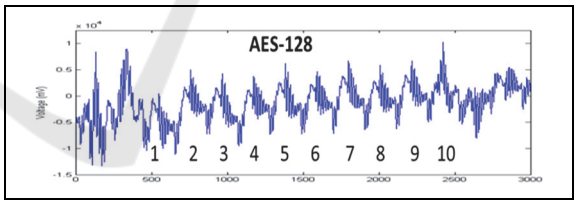

Figure 6: AES Power Consumption.

3 DATA COLLECTION AND ANALYSIS

A short survey was conducted on a sample of 39 IT managing professionals coming from a host of industries such as retail, finance, manufacturing and petrochemicals. The question asked the importance of cryptography in cloud IoT on a rating scale of 1 to 5, with 1 being very low and 5 being very high. The participants selection criteria, was that they needed to be involved with setting up the organisations cloud strategy, substantial management scope (over $5

million budget, and 50 people). The hypothesis was that cryptography would be an importance aspect.

Table 1: Importance of Crytography in Cloud IoT.

Mean	Standard Deviation	P Value
3.33	1.108183277	0.002565532

The mean resulted in an average over neutral in terms of the importance of cryptography, slightly moving towards the importance of cryptography in cloud IoT. The standard deviation was a little over one place, while the p value indicated a null hypothesis.

The participants then answered if they had engaged in a cloud iot project, of which the majority (74.358%) said no and then if they would go to a cryptography arbitrator of which a slight majority (53.846%) indicated they would. The data collection calculated yes as a one and no as a zero.

Table 2: Yes or No Survey Questions.

Question	Response		Mean	Standard Deviation
	Yes	No		
Have you engaged in a cloud iot project	10	29	0.25641	0.538
Is a crypto-arbitrator relevant	21	18	0.538461	0.505035

4 EUROPEAN DATA PROTECTION

The current guiding European directive on the protection of individuals with regard to the processing of personal data and its free movement is the Directive 95/46/EC dated 24th of October 1995. A basic protection level of personal data is explicitly included in the EU's Charter of Fundamental Rights (Article 8), but also in the Treaty on the Functioning of the European Union (Article 16).

According to the Directive 95/46/EC the meaning of personal data is "any information relating to an identified natural person (data subject)." When it comes to the processing of personal data, the Directive 95/46/EC points to "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."

The Directive identifies the subjects involved in the processing of personal data as the controller, processor, third party and the recipient. All subjects refer to a natural or legal person, public authority, agency or any other body, with the controller determining the purpose and means of the processing, the processor being the one that processes the personal data on behalf of the controller, while the recipient is the one to whom data is disclosed. The third party refers to any other subject that is authorized to process the personal data.

Data protection is enforced within the European Union through the principle of applicable national law. Under Article 4, the Directive 95/46/EC specifies that each Member State shall apply the national provisions defined pursuant to the Directive for any controller that has activities of an establishment set on the territory of the Member State. If multiple European establishments exist, the controller must comply with local requirements put forth by each Member State. In the example used for this paper, if the company was European it would be liable under Directive 95/46/EC, and if based in the UK, then it would also be liable under the Data Protection Act, 1998.

5 ARBITRATION & CORPORATE RULES

The current European Directive 95/46/EC on data protection is outdated and does not take the impact of cloud or IoT into consideration as it leaves a gap in the data protection area that cannot easily be covered through legislative efforts. Indeed, the European Commission is actively engaged in reformation processes that target to clarify the missing pieces, while modernizing the legal framework, but this is viewed as a long-term result.

Besides the extended duration of legislative reforms, analyzed proposals could be implemented in a very distinct format than the one when they were initially proposed. Taking all these aspects into consideration, it is imperative that at least a partial clarification and solution be introduced while the more advanced legislative process unfolds. "Binding corporate rules (BCR)" is a term that is increasingly used when it comes to international data transfers that imply third countries. However it would not be difficult to adjust binding corporate rules for external organisations that will have physical devices that

interact with each other via the cloud. In an adjusted manner the approval of the binding corporate rules given by one organization is also enriched with expansion coverage power over all national authorities in the light of the Directive proposal.

After a successful application of binding corporate rules at the level of controllers, the Article 29 Data Protection Working Party advanced to another level by adopting in June 2012 a working document on binding corporate rules for processors, both companies and data protection authorities. BCR are viewed as "internal rules applicable to entities of a multinational company and contain key principles legally covering the transfers of personal data coming from the European Union". They are regarded as an alternative to the Safe Harbor Principles and the European Commission's Standard Contractual Clauses. When transcended at the level of processors, binding corporate rules should be able to provide clients with the security and privacy of their data under European Union data protection regulations. The Article 29 Working Party's working document provides processors with a conditions checklist that must be fulfilled for being granted their adequacy.

The A29 DPWP working paper also came as a response to the industry's numerous requests to move the usage of binding corporate rules at the level of processors, as well. There are also voices that demand BCRs to be included for community cloud, considering that there might be cases when community members that belong to different corporate groups might own similar interests. Even though improvements at the level of binding corporate rules are definitely a step forward, their approval process remains a long and expensive procedure under the current regulations. While Member States grant approval based on diverse conditions, there is still a range of Member States that tends to remain on the safe side requesting an individual approval for each transfer under an already approved BCR.

If applied on a large scale, binding corporate rules could solve one of the main issues implied by both adequacy findings and Safe Harbor compliance – their restrictive geographical reach. In a July 2012 paper on cloud computing adopted by the Article 29 Data Protection Working Party, the organization states that companies that export data should act with increased diligence and question the statement of the data importer that it owns a Safe Harbor certification. Also, cloud clients should verify that standard contractual terms comply with national requirements regarding contractual data processing. Within cloud IoT the same policies could work to include cryptography arbitration. Whereby a third party is engaged to determine if the appropriate technical considerations where conducted in the design and architecture of the system. This would need to be agreed up front and drafted in end user license agreements, to provide the appropriate level of protection. Further challenges would come in the form of determining what type of organization would be certified as a cryptography arbitrator and what standards would be legally sound from a quality perspective, rather than just technical forensic solutions.

6 CONCLUSIONS

This paper has put forward the concept of cryptography arbitration and the need for its inclusion within designing cloud iot solutions. The research itself requires much more analysis to bring the concept out, such as increasing the survey question and sample frame, looking at other legal and cryptography aspects and other use cases. However the paper has put forward the position of the need for cryptography arbitration, and has looked at the security and legal challenges, providing recommendations to learn from lessons learned from existing cloud security frameworks, and in using existing legal frameworks, such as corporate binding rules.

REFERENCES

Chang, V., Kuo, Y.-H. and Ramachandran, M. (2016) 'Cloud computing adoption framework: A security framework for business clouds', Future Generation Computer Systems, 57, pp. 24–41. doi: 10.1016/j.future.2015.09.031.

Chang, V. and Ramachandran, M. (2016) Towards achieving data security with the cloud computing adoption framework. Available at: http://ieeexplore.ieee.org/xpl/abstractMetrics.jsp?arnumber=7299312 (Accessed: 17 March 2016).

Ning, H. and Liu, H. (2012). Cyber-Physical-Social Based Security Architecture for Future Internet of Things. *Advances in Internet of Things*, 02(01), pp.1-7.

Ning, H., Liu, H. and Yang, L. (2013). Cyberentity Security in the Internet of Things. *Computer*, 46(4), pp.46-53.

NIST, (2013). *Cryptographic Key Management Issues & Challenges in Cloud Services (NISTIR 7956)*.

Martin, K. (2006). *Cryptographic Key Management.* Eng, C. (2008). *Cryptography for Penetration Testers*.

Gurkaynak, F., Oswald, E. and Preneel, B. (2004).

Power-Analysis Attack on an ASIC AES Implementation. In: *Information Technology: Coding and Computing*. Leuven, Belgium: IEEE.

IEEE, Retrieved from http://iot.ieee.org/about.html on 05/01/2016.

Gartner, Retreived from http://www.gartner.com/it-glossary/internet-of-things/) on 05/01/2016.

Cisco, Retreived from http://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html on 05/01/2016.