Enhancing IoT Security through Hardware Security Modules (HSMs)

Mansoor Khan*, Muhammad Ilyas†, Oguz BAYAT§
*Electrical and Computer Engineering, Altinbas University, Istanbul, Turkiye
Email: mansoor.khan1@ogr.altinbas.edu.tr
†Dept, of Cyber Security , Al ain University, Al ain, UAE
Email: muhammad.ilyas@aau.ac.ae
†Electrical and Computer Engineering, Altinbas University, Istanbul, Turkiye
Email: muhammad.ilyas@altinbas.edu.tr
§ Electrical and Computer Engineering, Altinbas University, Istanbul, Turkiye
Email: oguz.bayat@altinbas.edu.tr

***Abstract*—Strong security measures must be integrated in an era where data security is critical, particularly for sensitive data handled by IoT devices. In order to strengthen Internet of Things security, the use of Hardware Security Modules (HSMs) is investigated in this research. We examine the development and effectiveness of HSMs in boosting IoT security through a thorough study of the literature. Our results demonstrate the vital role that HSMs play in protecting cryptographic keys and thwarting any attacks. We explore the difficulties of incorporating HSMs into IoT environments and suggest practical approaches. This research concludes by highlighting the role that HSMs play in strengthening IoT security architecture.**

Keywords—HSMs, IoT, security, Hardware Security Modules

I. INTRODUCTION

In particular, it is of the utmost importance for customers who deal with sensitive data or who operate in highly regulated industries to have both operational and data security in place. Customers of the Internet of Things face an additional obstacle when it comes to the issue of allowing rigorous security standards for connectivity of the Internet of Things to cloud platforms (Crestini, n.d.). Two prominent examples of techniques that are widely employed for the goal of assuring the security of communication traffic are cryptographic keys and asymmetric data encryption methods. Both of these approaches are used to encrypt data or data transmissions.

According to (Crestini, n.d.), the most crucial requirement for Internet of Things devices is the secure storage of cryptographic keys. This is because it prevents malicious users from having direct access to the device. An adversarial user may assume the identity of an Internet of Things device in the case that a private key was obtained (Yu, 2021). This would allow the adversary to gain access to private company information technology resources or to transmit fraudulent data, both of which could have repercussions that could be disastrous.

Hardware Security Modules, which are often referred to as HSMs, are a solution that is utilized by a large number of customers that are enthusiastic about protecting their digital keys and certificates. When it comes to concealing private keys, high-security modules (HSMs) provide a hardware-based method that is both effective and efficient. However, according to Saidov et al. (2017), the process of integrating them into the software stack of an Internet of Things device is not a simple, easy procedure.

Core Contribution

The paper titled, 'Enhancing IoT Security through Hardware Security Modules (HSMs)' is an important addition to the current literature on IoT security as it best describes the essential aspect of how the IoT system's security hinges a lot on HSMs when it comes to safeguarding cryptographic keys and enabling secure communication within the IoT domain. The paper also contains a description of the problem associated with the implementation of HSMs into IoT devices, as well as the advantages of their usage for protection of devices and information from unauthorized users and attacks. In addition to identifying the role of HSMs in improving IoT security this paper presents actionable solutions of the challenges of deploying HSMs. In so doing, the paper enlarges the body of knowledge on how to improve IoT security architectures specifically for organizations such as industries that can handle sensitive data and operating under strict regulatory laws.

Structure of the paper

Literature Review: This section seeks to provide an empirical review of the current literature regarding the involvement of HSM in IoT security.

Methodology: The paper employs technique known as Systematic Literature Review (SLR) in order to conduct data inclusion and analysis from secondary databases. .

Results: The outcome of the study is featured in this section by demonstrating how HSMs contribute to IoT security by storing keys, as well as executing random key creation and cryptographic operations.

Discussion: The discussion section explores the consequences of the outcomes for the work by discussing the difficulties and factors one has to keep in mind for incorporating HSMs into IoT systems.

Conclusion: The paper concludes by restating the findings made in the paper and reemphasizing on the important of HSMs in improving the security of IoT.

979-8-3503-5469-0/24/$31.00 ©2024 IEEE

II. LITERATURE REVIEW

According to Sindu et al. (2019), the implementation of Hardware Security Modules is an essential step in enhancing the security of the Internet of Things. They accomplish this by keeping cryptographic certifications and keys in a secure location, which they provide for their customers. Since cryptographic keys serve as the foundation for authentication and encryption methods, they are an indispensable component in the process of ensuring the safety of messages that are transmitted across the Internet of Things (IoT) (Crestini & Palazzi, 2023). Hardware security modules (HSMs) ensure that these keys are protected from being altered and from being accessed by individuals who are not permitted to do so. They do this by providing a secure environment for the generation, administration, and storage of these keys.

According to Sidhu et al. (2019), one of the primary functions of hardware security modules (HSMs) is to generate cryptographic keys through the process of hashing. These keys are usually the target of malicious actors that are attempting to exploit networks and devices connected to the Internet of Things (IoT). Hardware security modules, often known as HSMs, are effective in enhancing the overall security posture of Internet of Things installations because they prevent the storing of keys and the theft of keys. The keys are stored within a specific hardware module, which allows for this to be performed. Hardware security modules (HSMs) contribute to the protection of the confidentiality and integrity of data that is exchanged between cloud platforms and devices connected to the Internet of Things (Williams et al., 2022). This is accomplished by facilitating the secure execution of cryptographic operations such as encryption and decryption, which are examples of cryptographic operations.

Sisavath and Yu, (2021), mentioned that Hardware security modules, also known as HSMs, provide a secured environment for the administration of keys and the control of cryptographic activities. This makes it less likely that they will be compromised or that they will be accessed by unauthorized parties. Crestantini and Palazzi (2023) state that a wide variety of industries, such as the healthcare business, the financial sector, and the government, are subject to severe regulatory requirements that control data security and privacy.

According to Wu, et al., (2020), these policies require that these industries adhere to certain standards. The utilization of hardware security modules (HSMs) for the purpose of safeguarding sensitive data and cryptographic assets enables enterprises to ensure that they are in compliance with both industry standards and legal obligations (Wu, et al., 2020). High-security measures, also known as HSMs, have the ability to reduce the impact of a wide range of cyberthreats, such as unauthorized access, data breaches, and man-in-the-middle attacks. Using strict cryptographic limits, high-security modules (HSMs) are able to assist Internet of Things (IoT) systems in overcoming rising security vulnerabilities (Cabrera-Gutiérrez, et al., 2022).

According to the given Chien, et al., (2020), in order to demonstrate a commitment to robust security procedures, high-security modules (HSMs) are implemented into Internet of Things (IoT) settings. This, in turn, encourages confidence and assurance among users (Chien, et al., 2020). According to Butun et al. (2020), HSMs have the ability to assist businesses in differentiating themselves in oversaturated markets, enhancing the trust of their consumers, and minimizing the risks associated with their reputations. Each of these benefits can be achieved through the use of HSMs. Because it is a process that has the potential to be challenging and resource-intensive, integrating HSMs into pre-existing Internet of Things systems requires meticulous preparation and the participation of stakeholders who are involved in the process. The implementation of HSMs, as stated by Cabrera-Gutiérrez et al. (2022), adds an extra layer of difficulty to the integration process. This is due to the fact that it may be necessary to make adjustments to the hardware, firmware, and software.

According to the findings of a study that was conducted by Butun, et al., (2020), the installation and purchase of hardware security modules can be extremely expensive. This is especially true for companies that have implemented Internet of Things on a broad scale. There is a possibility that certain businesses will be unable to afford the initial expenditures that are associated with the adoption of HSMs, in addition to the ongoing expenses that are associated with maintenance and support. Because of the present standards, protocols, and infrastructure of the Internet of Things, there is a possibility that HSMs will experience difficulties. According to Al-Omary et al. (2018), in order to effectively tackle compatibility concerns, it is necessary to conduct exhaustive testing and validation in order to ensure that the integration with a variety of Internet of Things devices, platforms, and communication protocols is carried out without any problems. It is common for devices that are a part of the Internet of Things to have minimal capacity for memory, power, and CPU. This can have an impact on how well HSMs work and how effectively they scale out. When it comes to integration efforts, the most important priority should be, respectively, the optimization of resource utilization and the minimizing of HSM influence on the functionality of Internet of Things devices. Both of these should be prioritized (Chmiel, et al., 2021).

The applying of Hardware Security Modules (HSMs) in preserving IoT gadgets has lately turned into extolled more as IoT systems progress and become instigate to cybercrimes. HSM, which is designed to store and secure cryptographic keys, play a significant role in ensuring the data protection and security including integrity and confidentiality as well as authenticity across IOT systems. According to Afzal, et al., (2021) a study done it pointed that the HSMs offer an improved security because they incorporate anti-tampering mechanisms thus guaranteeing secure connection in IoT devices.

Furthermore, Merino, et al., (2020) pointed out that HSMs should be incorporated into IoT architectures because of the growing sophistication and networking of IoT devices. Also, pointed out that HSMs are protecting not only the cryptographic processing but also are involved in the firmware upgrade protection and integrity of the device authentication (Merino, et al., 2020). Besides that, Tawalbeh, et al., (2020) investigated productivity-related costs of implementing HSMs for large-scale IoT networks and found that despite higher initial costs, the potential benefits are substantial in achieving enhanced security, and shrinking the data breach risks (Tawalbeh, et al., 2020).

These innovations have also aimed at enhancing the integration of HSMs in different and various IoT systems. A more extensive, presented the prospects and problems, regarding the incorporation of HSMs with other IoT standards

and supports. This situation was explained by the fact that more standardized flexible HSM solutions need to be offered to support the fast changing of IoT.

III. METHODOLOGY

The Systematic Literature Review method is used in the paper which focuses on collecting the data from the secondary sources which includes the published articles, journals, and researches to make the analysis of the data about IoT Security through Hardware Security Modules. In the first phase, the paper focused on selecting 36 papers on the basis of the key search terms included as, “IoT Security”, “Hardware Security Modules”, and “IoT Security through Hardware Security Modules”. The searches were done on Google Scholar, from IEE papers, Scopus Journal, Elsevier and many others to get the most relevant and recent papers in study.

With these key terms, the selection of the first 33 sources was done, to access the impact of IoT Security through Hardware Security Modules, and analysing that how it has evolved over time. In the second phase, the search was more refined by restricting the search with the year. From the selection of the 25 sources, the filter of the years was integrated that made the selection of the most relevant papers that are from the past 5 years. Thus, with both the phases, the final sources for the result and discussion for the study is done with final 19 papers selected. With this, “Enhancing IoT”, was analysed closely to attain the outcomes.

The inclusion criteria included the paper from the recent 5 years, and the relevant papers which are about the IoT and its relevance in enhancing the hardware security across. The criteria of exclusion included no paper previous to 5 years, no paper which was not accessible and was not considered to be published on a renowned page or journal, to maintain the validity and reliability of the study, and deliver authentic outcomes.

IV. RESULTS

An Internet of Things device is provided with a key-pair that consists of both the private key and the public certificate, in addition to a trust-store that contains the server Certificate Authority (CA) chain. This is done in order to guarantee that the communication that takes place between the devices is safe. It is important to have this information in order to enable both client authentication on the server side (by utilising the trust-store) and server authentication on the client side (by utilising the key pair). Both of these authentication methods are necessary in order to provide client authentication. In this particular instance, the identifying mechanism in question is referred to as Mutual TLS authentication, and the figure that follows provides an illustration of it.

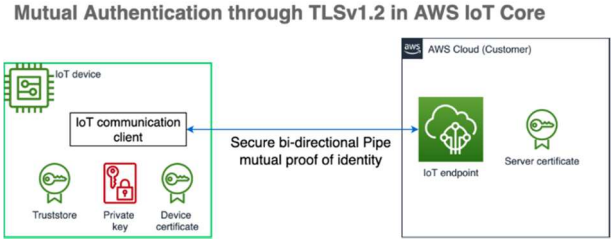

Fig. 1. Mutual Authentication of AWS IoT

In the form of a cryptographic chip, a Hardware Security Module (HSM) is a physical module that is capable of providing security. It is possible to link it to a high-speed bus or just solder it onto the device itself.

The following are the benefits it offers a secure key vault that stores keys and generates random keys based on entropy and other factors (Borgaonkar, et al., 2021). Cryptographic operations are implemented on the semiconductor, without the software stack being exposed to them. The non-volatile memory (NVM) on the chip is the subject of sophisticated anti-tampering measures that provide physical safety (Borgaonkar, et al., 2021).

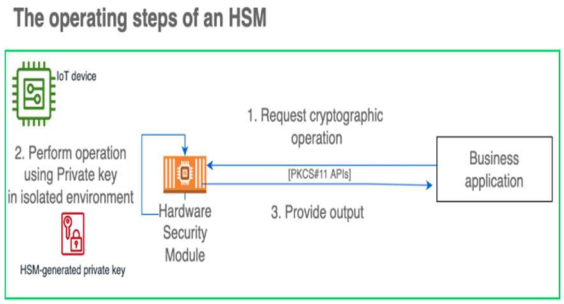

Fig. 2. Steps of HSM Working

From the above figure, it can be inferred that the steps within HSM wokring needs a huge path to follow, which includes the installation of the device, the performance with the isolated network as well, installation of hardware security module, requesting the operation to business application and then receiving the output as well.

V. DISCUSSION

Hardware security modules, often known as HSMs, provide a solid method of protecting cryptographic keys while also taking into consideration all of the security concerns. However, in order for them to function correctly, it is necessary to do thorough installation and maintenance. According to Al-Omary et al. (2018), in order for businesses to properly manage risks, they must first determine the security requirements that they have and then take the appropriate corresponding steps. The importance of ensuring compliance with data privacy standards cannot be overstated, particularly for highly regulated industries such as healthcare and banking. According to Cabrera-Gutiérrez et al. (2022), enterprise security management systems (HSMs) have the capability to assist businesses in demonstrating compliance with industry standards and meeting regulatory obligations.

HSMs in Internet of Things networks confront two integration hurdles: interoperability issues and resource restrictions. Despite the fact that they have numerous built-in advantages, Internet of Things networks face these challenges. The authors Saidov et al. (2017) state that in order for companies to successfully overcome these challenges, they need to conduct a comprehensive analysis of the situation and come up with potential solutions. For the successful installation of Hardware Security Modules in Internet of Things systems, it is vital to adhere to the best practices in the industry and collaborate with a wide variety of stakeholders (Williams et al., 2022). It is necessary to do a comprehensive risk assessment in order to identify the security flaws, threats, and regulatory duties that are specific to the Internet of Things and the environment in which it operates. Utilising the individualised HSM deployment will allow you to effectively

control the risks that have been identified as well as the regulatory requirements.

At the very beginning of the process of creating systems for the Internet of Things, security concerns must to be taken into conscious consideration. When referring to this particular approach, the term "security by design" is the one that is utilised (Tanasiev, et al., 2021). By utilising a security-by-design strategy, you should make the protection of cryptographic keys, the preservation of data integrity, and the preservation of privacy your top priorities for the entirety of the lifecycle of the Internet of Things (Wu, et al., 2020).

Standardisation of industry standards and protocols, as well as encouragement of their use, are required in order to guarantee compatibility across embedded systems and devices connected to the Internet of Things. Ensure that the current security standards and protocols are adhered to at all times (Tanasiev, et al., 2021). This is absolutely necessary in order to facilitate seamless integration and interoperability throughout the system. The implementation of systems that enable continuous HSM monitoring, auditing, and assessment is something that Al-Omary et al. (2018) recommend carrying out. Proactively locating and fixing performance issues as well as security vulnerabilities will be possible as a result of this technology.

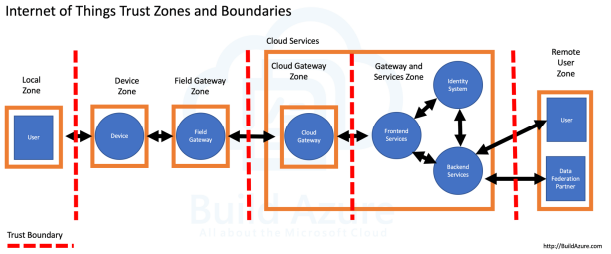

Fig. 3. Iot Security Architecture

It is recommended that you routinely update and fix the firmware and software of your HSM in order to protect it against newly discovered vulnerabilities and threats.

It is of the utmost importance that the different players involved, including manufacturers of the Internet of Things (IoT), professionals working in the security industry, government organisations, and business associations, encourage collaboration and the exchange of information (Tanasiev, et al., 2021). In order to enhance the robustness and efficiency of security systems for the Internet of Things, it is essential to share information security best practices, ideas, and lessons learned with one another.

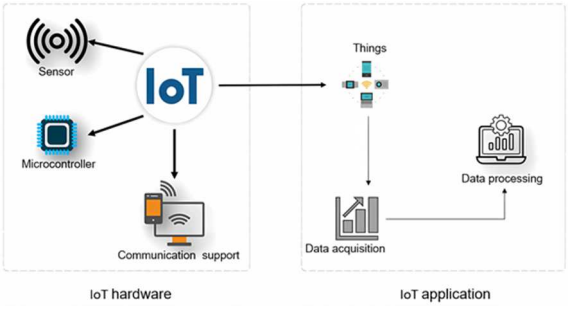

Fig. 4. Hardware Security of IoT

This HSM system is adding to the layer of security by engaging with the more secured storage system, and with the management of the cryptographic keys within. This is helpful in authentication with better modes of encryption and authentication, protecting the system from the unauthorised access. HSMs also contributes with the overall security posture of the system where it mitigates with the risk, ensuring the data integrity and confidentiality. Even the security system HSM bring is helpful with the businesses to get with sensitive data, its protection and overall management of assets and security. An additional layer of security is added with its feature of assurance where it instils with the confidence and assurance and differentiation to enhance the customer trust within.

VI. Conclusion

The significance of Hardware Security Modules in increasing IoT security is highlighted by the outcomes of the systematic literature review. HSMs are crucial for defending IoT networks against unauthorised access and data breaches because they secure cryptographic keys, assure regulatory compliance, and minimise cyber risks. HSM adoption demands thorough preparation, coordination, and adherence to industry best practices, even with integration issues. Going forward, organisations need to put security issues first and deploy HSM technology to develop trustworthy and dependable IoT solutions. HSMs will play a crucial part in guaranteeing security as IoT use develops. Advancements in standards and protocols for secure IoT communications, mitigation of emerging risks, and progress of HSM technology should be the primary areas of future study.

HSMS play a vital role in enhancing security of IoT devices to safeguard the cryptographic keys together with integrity of the data. Because of their fairly strong security measures, organizations dealing with secure data such as the health and financial sectors cannot do without them. Although, they are very effective, there are some drawbacks concerning them these are costly, hard to implement, and sometimes experience interoperability problems. Mitigating such challenges is crucial in the improvement of IoT security across the different sectors.

Research Gap

There is limited research work on analyzing the long-term sustainable architecture of HSMs and their performance in various IoT domains. More research should therefore be carried out in the discovery of cheap solutions to HSM as well as evaluating its flexibility in addressing the changing IoT threats and technologies.

References

[1] Crestini, &. (n.d.). Enhancing IoT device security using Hardware Security Modules and AWS IoT Device SDK. AWS. Retrieved from Amazon: https://aws.amazon.com/blogs/iot/enhancing-iot-device-security-using-hardware-security-modules-and-aws-iot-device-sdk/

[2] Al-Bahri, M., Alkishri, W., Ahmed, F. Y., Alshar'e, M., & Al Maskari, S. (2024). Enhancing IoT Network Security Through Digital Object Architecture-Based Approaches. Qubahan Academic Journal, 4(1), 224-239. **DOI:** https://doi.org/10.48161/qaj.v4n1a413

[3] Al-Omary, A., Othman, A., AlSabbagh, H. M., & Al-Rizzo, H. (2018). Survey of hardware-based security support for IoT/CPS systems. KnE Engineering, 52-70. DOI: 10.18502/keg.v3i7.3072

[4] Borgaonkar, R., Anne Tøndel, I., Zenebe Degefa, M., & Gilje Jaatun, M. (2021). Improving smart grid security through 5G enabled IoT and

edge computing. Concurrency and Computation: Practice and Experience, 33(18), e6466. https://onlinelibrary.wiley.com/doi/pdf/10.1002/cpe.6466

[5] Butun, I., Sari, A., & Österberg, P. (2020). Hardware security of fog end-devices for the internet of things. Sensors, 20(20), 5729. https://www.mdpi.com/1424-8220/20/20/5729

[6] Cabrera-Gutiérrez, A. J., Castillo, E., Escobar-Molero, A., Álvarez-Bermejo, J. A., Morales, D. P., & Parrilla, L. (2022). Integration of hardware security modules and permissioned blockchain in industrial iot networks. IEEE Access, 10, 114331-114345. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9931706

[7] Chien, H. Y., Chen, Y. J., Qiu, G. H., Liao, J. F., Hung, R. W., Lin, P. C., & Su, C. (2020). A MQTT-API-compatible IoT security-enhanced platform. International Journal of Sensor Networks, 32(1), 54-68. https://www.inderscienceonline.com/doi/abs/10.1504/IJSNET.2020.104463

[8] Chmiel, M., Korona, M., Kozioł, F., Szczypiorski, K., & Rawski, M. (2021). Discussion on IoT security recommendations against the state-of-the-art solutions. Electronics, 10(15), 1814. https://www.mdpi.com/2079-9292/10/15/1814

[9] Saidov, J., Kim, B. K., Lee, J. H., & Lee, G. (2017). HARDWARE INTERLOCKING SECURITY SYSTEM WITH SECURE KEY UPDATE MECHANISMS IN IOT ENVIRONMENTS. The Journal of the Korea institute of electronic communication sciences, 12(4), 671-678. https://koreascience.kr/article/JAKO201724963131752.pdf

[10] Sidhu, S., Mohd, B. J., & Hayajneh, T. (2019). Hardware security in IoT devices with emphasis on hardware trojans. Journal of Sensor and Actuator Networks, 8(3), 42. **https://doi.org/10.3390/jsan8030042**

[11] Sisavath, C., & Yu, L. (2021). Design and implementation of security system for smart home based on IOT technology. Procedia Computer Science, 183, 4-13. https://doi.org/10.1016/j.procs.2021.02.023

[12] Tanasiev, V., Pătru, G. C., Rosner, D., Sava, G., Necula, H., & Badea, A. (2021). Enhancing environmental and energy monitoring of residential buildings through IoT. Automation in Construction, 126, 103662. https://www.sciencedirect.com/science/article/pii/S0926580521001138

[13] Waraga, O. A., Bettayeb, M., Nasir, Q., & Talib, M. A. (2020). Design and implementation of automated IoT security testbed. Computers & security, 88, 101648. https://e-tarjome.com/storage/panel/fileuploads/2019-11-26/1574771677_gh32.pdf

[14] Williams, P., Dutta, I. K., Daoud, H., & Bayoumi, M. (2022). A survey on security in internet of things with a focus on the impact of emerging technologies. Internet of Things, 19, 100564. https://www.sciencedirect.com/science/article/pii/S2542660522000592

[15] Wu, H., Han, H., Wang, X., & Sun, S. (2020). Research on artificial intelligence enhancing internet of things security: A survey. Ieee Access, 8, 153826-153848. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9172062

[16] Crestini, D. & Palazzi, I. (2023). Enhnacing IoT device security using Hardware Security Modules and AWS IoT Device SDK. AWS. https://aws.amazon.com/blogs/iot/enhancing-iot-device-security-using-hardware-security-modules-and-aws-iot-device-sdk/

[17] Merino, P., Mujica, G., Señor, J., & Portilla, J. (2020). A modular IoT hardware platform for distributed and secured extreme edge computing. *Electronics*, *9*(3), 538. **https://doi.org/10.3390/electronics9030538**

[18] Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), 4102. **https://doi.org/10.3390/app10124102**

[19] Afzal, S., Faisal, A., Siddique, I., & Afzal, M. (2021). Internet of Things (IoT) Security: Issues, Challenges and Solutions. *Int. J. Sci. Eng. Res*, *12*(6), 52. https://d1wqtxts1xzle7.cloudfront.net/67663799/Internet_of_Things_IoT_Security_Issues_Challenges_and_Solutions-libre.pdf?1624002317=&response-content-disposition=inline%3B+filename%3DInternet_of_Things_IoT_Security_Issues_C.pdf&Expires=1723620029&Signature=CcWwzZzXPgW9HmzYe4tZ5T9UmXqVe0FDcwXpkQCff0SxT5Rx8TlJBP1yWQje3rts-lv0LYvV7jVwN1lg01h1ZEpnQWlJDzFJLf-KVxY1PQ3SNRip4NBNFuq-YaeW2Ohu647R2bFX7Di0CVuxD6Gigjc0FTL5sjogBWAHQO27mbujwBDqXUIzeYj6wF9VuUUuSB0hYZ0eJWgEYt3Q7XQ5MZss03M5thKoFXOlYu8t-3pvDnEKZWEZRe8brLXuCiZq~wIGq-NaqFwY~XxHu8Cxg4Sf5Qt7NlMfn8x4k1PL1bUHWrntYkOC7Ph109mb6ETTyfOlpKXPlff1NqW00jCfsA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA