Encryption as a Service: A Review of Architectures and Taxonomies

Amir Javadpour[1][0000−0002−4932−1660], Forough Ja'fari[2][0000−0001−7176−9456], and Tarik Taleb[3][0000−0003−1119−1239]

[1] ICTFICIAL Oy, Espoo, Finland
Corresponding author: a.javadpour87@gmail.com
[2] Department of Computer Engineering, Sharif University of Technology, Iran
[3] Faculty of Electrical Engineering and Information Technology, Ruhr University Bochum, Bochum, Germany

Abstract. Due to the rise of Internet of Things networks, targeting vulnerabilities related to the limitation of resources in devices has increased. Therefore, it is necessary to delegate encryption services to cloud and fog platforms. Encryption as a Service (EaaS) provides all cryptographic services to end-users to help them cope with their limited resources and processing capabilities. This paper reviews the existing research on EaaS platforms and categorizes them based on their underlying encryption algorithm types. We also introduce different EaaS architectures based on the location of the main components. To our knowledge, none of the existing surveys in this field have covered the aforementioned features.

Keywords: Internet of things (IoT), Encryption as a Service (EaaS), Cloud/Edge computing, Full Cloud Fog architecture

1 Introduction

Cyberattacks are growing and improving daily, making researchers design and deploy mitigation activities. One of these activities is cryptography [7, 8, 11]. In previous decades, the cryptography processes were handled by the single remote servers or the end-devices themselves. However, due to the limitations in device resources in Internet of Things (IoT) devices, and the risk of being a single point of failure when single servers are used, the researchers move toward ways of providing cryptography services in a distributed environment [20, 8]. Hence, Encryption as a Service (EaaS) emerged.

several surveys have reviewed the research on EaaS [10, 13]. However, they do not cover recent works as they are relatively old, and none have discussed the advantages and disadvantages of different architectures of EaaS. This paper, first, gives the background concept of EaaS, then explains the various architectures of an EaaS platform, and finally, categorizes the reviewed research based on the underlying encryption type. The paper in question has made several noteworthy contributions to the field of EaaS. Firstly, it has undertaken a review of a broad range of research studies related to EaaS, highlighting and discussing the various challenges faced in the field. Secondly, the authors have identified four general architectures for EaaS, and have categorized the existing research work based on these architectures. This has helped provide a better understanding of the different approaches taken in the field of EaaS. Lastly, the authors have presented a categorization of EaaS platforms based on the types of encryption they utilize. This has been particularly useful in identifying the encryption techniques employed in EaaS platforms and has helped assess their efficacy and suitability for different use cases.

2 Background

Making data only readable by legitimate users is called cryptography. The raw data and a single or a pair of keys are passed to the encryption algorithm, and a ciphertext is obtained. The ciphertext can be converted to the original raw data during decryption only when the related key(s) are available. Therefore, the data owner can share the associated keys for decrypting data with only those permitted to read [1].

Providing cryptography services and all of the main processes as a cloud service is called EaaS. All the EaaS platforms do not have the same components; however, we can say that the main components, which can also be called as crypto components, are (1) general manager, (2) key manager, (3) encryptor, and (4) decryptor. The general manager is responsible for managing a request from when it is received until it is responded to. The processes under its management contain choosing an appropriate key manager, encryptor, or decryptor for a request, and checking users' authorities. The key manager components create appropriate keys and handle all the related processes. Finally, the encryptor and the decryptor components receive related keys and perform encryption and decryption on a given data. The sequence diagram shown in Figure 1 indicates how different components communicate to serve a cryptography request.

We can see in Figure 1, that an end-device, which is the data owner, wants to share it on a public cloud, but safely, only specific devices can read. In Step 1, the raw data and the algorithm type are sent to the general manager component. Once received, the general management component checks the status of available key managers, selects one, and sends the algorithm type toward it (Step 2). When the selected key manager receives the algorithm type, the keys are generated based on it and sent back to the general manager (Step 3). Then again, the general manager selects an appropriate encryptor, and sends the raw data and the generated key(s) toward it through step 4. When the encryption process is complete, the encrypted data (i.e., ciphertext) is sent back to the general manager and forwarded to the data owner (Step 5 and Step 6). The data owner can now share the encrypted data on the public cloud in Step 7. When another device attempts to access shared data on the public cloud, the encrypted data is sent to the general manager, which follows similar steps if authorized to access it. The only difference is that a decryptor component is now involved instead of

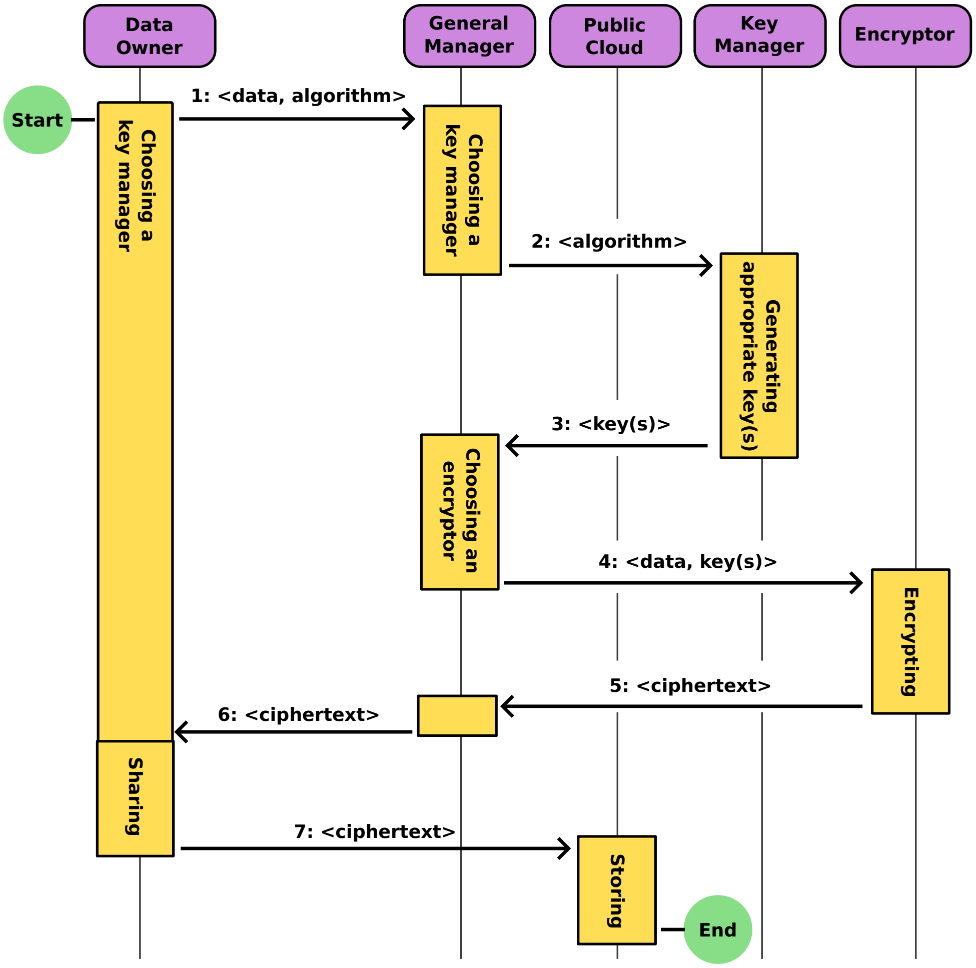


Fig. 1. A diagram illustrating the sequence of events in a simple EaaS system designed for sharing encrypted information.

This Figure shows how different components communicate to serve a cryptography request. The data owner shares the raw data and algorithm type with the general manager, who selects a key manager to generate the keys. Then, an encryptor encrypts the data and sends it back to the owner. Other devices can access the data if they have permission. A decryptor component is involved in the process of reading the encrypted data. Backup crypto components are sometimes used to avoid a single point of failure.

an encryptor. It must be noted that not to have a single point of failure, and some platforms use backup crypto components too [22].

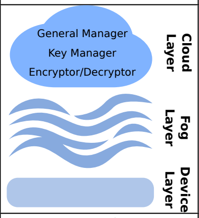
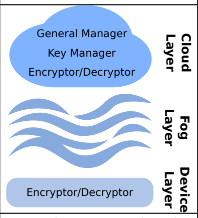
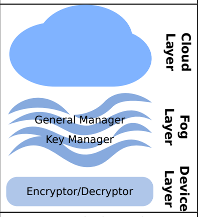
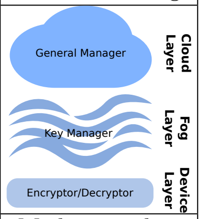
3 EaaS Architectures

Different architectures have been proposed for EaaS platforms. The location of crypto components varies in other architectures. These three layers can host the entities: (1) device layer, (2) cloud layer, and (3) fog layer. The devices on the device layer have limited resources and cannot execute complex processes. The nodes on the cloud layer are physical or virtual systems that function as cloud nodes. These nodes are rich resources, can do complex processes, and offer big storage spaces to users. The nodes on the fog layer are near the edge and are considered intermediary nodes. We can categorize the EaaS architectures currently proposed by the researchers into four categories based on the location of their crypto components. We use the term ”Full” to indicate that none of these components are located on the device layer, and the cloud and fog layers fully handle the processes. And on the other hand, the term ”Half” refers to the architectures that use the end-devices as part of the cryptography process. These categories are as follows [9]:

- **Full-Cloud:** This architecture contains only the cloud layer. This means there is almost no limitation in the resources, and the cryptography service can serve a wide range of end-devices. The EaaS platforms based on the full-cloud architecture are easy to implement, and the request acceptance ratio is high due to having almost no constraints on resources. However, as the included nodes are located on the cloud layer, there may be a significant delay in response.
- **Half-Cloud:** This architecture contains device and cloud layers. The end devices must have the least required resources when a platform works based on the half-cloud architecture. This is because these devices are also involved in some cryptography processes. However, most platforms with the half-cloud architecture do not make end-devices perform complicated tasks. As a result, only simple ones are done by the device layer.
- **Half-Fog:** The half-fog architecture includes two layers, which are the device and the fog layer. The devices that want to be served by EaaS platforms under this architecture must have at least a specific amount of resources. In some platforms, the end-devices under ”Half” architectures, the fog nodes only decide the type of cryptography algorithm, and generate the related key(s). The end-devices perform the other processes by themselves [4].
- **Half-Cloud-Fog architecture:** In this architecture, the EaaS platform's key components are distributed across three layers. This architecture is a hybrid of half-cloud and half-fog. Not all EaaS platforms in the ”Half” category require end-devices to perform cryptographic tasks. Some platforms ask for only powerful devices to do them [24].

A summary of EaaS architectures and the researchers working on them are presented in Table 1.

Table 1. A comparison of different EaaS architectures and the research on each type.

Architecture	Full-Cloud	Half-Cloud	Half-Fog	Half-Cloud-Fog
Scheme	 General Manager Key Manager Encryptor/Decryptor Cloud Layer Fog Layer Device Layer	 General Manager Key Manager Encryptor/Decryptor Cloud Layer Fog Layer Encryptor/Decryptor Device Layer	 Cloud Layer General Manager Key Manager Fog Layer Encryptor/Decryptor Device Layer	 General Manager Cloud Layer Key Manager Fog Layer Encryptor/Decryptor Device Layer
Features	High compatibility but high delay	Medium to high compatibility but medium to high delay	Low delay but medium compatibility	Medium to low delay but medium compatibility
Reference	[3, 23, 21, 5, 17]	[22]	[4, 12]	[24]

4 Categorized EaaS Encryption Types

An EaaS platform can offer various types of cryptographic services, which can be categorized as follows:

- **Attribute-Based EaaS (ABEaaS):** In normal encryption, the cryptography features do not change in different cases. However, ABEaaS provides a way to apply these changes based on user or environment attributes. The ABEaaS platform proposed by [4] tries to cover as much end-devices as possible by suggesting the algorithms that the end-devices can perform.
- **Homomorphic EaaS (HEaaS):** Users may sometimes require specific operations to access encrypted data, but may hesitate to do so due to privacy concerns. Homomorphic Encryption as a Service (HEaaS) is a viable solution. A recent research paper [5] presents an innovative HEaaS offering specializing in cryptography services for encrypting and decrypting images. With this HEaaS solution, users can perform operations on encrypted images without needing to decrypt them, thus ensuring the privacy and security of the data owner's information.
- **Searchable EaaS (SEaaS):** This type of encryption is for situations, where there is a need for searching a keyword in encrypted data without decrypting it. A sample SEaaS is proposed by [18] for British telecommunication cloud, making keywords with typo errors searchable. Searching for a specific keyword within encrypted data may be necessary without decrypting the entire dataset in certain scenarios. This is where a particular type of encryption comes into play. The encryption method allows searching keywords within encrypted data while keeping it secure. An example of such a service is the SEaaS proposed by [18] for the British telecommunication cloud. This service not only enables the searching of keywords within encrypted data, but also allows for typos to be accounted for during the search process. This approach ensures that the data remains secure, allowing for efficient and accurate searchability.

- **Proxy Re-EaaS (PREaaS):** This encryption type is for situations, where two parties want to share encrypted data, but without sharing the keys used for decrypting it. Some examples of these situations are when emails are forwarded to others and when content is distributed. proposes a PREaaS cite2019prasa to protect the data shared between the components of smart grids. In this platform, the location of the proxy is changed to find which one has the best performance. In this scenario, it becomes necessary for two parties to share encrypted data without sharing the keys used for decrypting it. This is where a specific encryption type comes into play. For instance, this encryption type is quite valuable when emails are forwarded to others or when a particular content is distributed. The primary goal of this platform is to safeguard the data shared between the various components of smart grids. To achieve this, the location of the proxy is altered to locate the one with the best performance. This way, the data remains secure while ensuring optimal performance.
- **Quantum EaaS (QEaaS):** In this encryption type, the concepts of quantum mechanics are used for performing cryptography. When data is encrypted using this technique, the receiver can find out if illegal parties read it because the photons are changed when they are read. proposes sample work in this field cite2021qucras, where a QEaaS is designed for applying security to the communications between aerial vehicles. This QEaaS contains five layers, one for gathering data, another for presenting the physical devices, one layer for performing quantum encryption, the fourth one for communications, and the last one as the storing layer. In a recent research paper, [14] proposed a QEaaS system to enhance communication security between aerial vehicles. This QEaaS system comprises five key layers that provide a comprehensive security solution. The first layer gathers the necessary data, while the second is dedicated to the physical devices used in the communication process. The third layer is the quantum encryption layer, which applies advanced encryption techniques to ensure data confidentiality. The fourth layer handles the communication process, and the last layer stores the data securely. Implementing this QEaaS system in aerial vehicles makes it possible to ensure that all communication is secure and protected against any potential threats. This can be especially important when sensitive information must be transmitted between aerial vehicles.

A summary of the research in each category is presented in Table 2. There is another category in this table, called General EaaS (GEaaS) for presenting other types of EaaS than those mentioned.

5 Conclusion

This paper presents an all-inclusive summary of various EaaS platforms suggested by researchers in the respective fields. We have categorized their architecture into four classes, namely, Full-Cloud, Fog, Hybrid, and Edge. Additionally,

Table 2. A summary of Review of Research on Varied Encryption types

Ref.	Type	Year	Architecture	Description
[3]	ABEaaS	2017	Full-Cloud	Splitting ABEaaS into multiple sub-services.
[21]		2021	Full-Cloud	Considering users' identity as the attributes.
[4]		2022	Half-Fog	Covering more devices by selecting optimal features.
[5]	HEaaS	2020	Full-Cloud	Serving cryptography services for images.
[15]		2023	Full-Cloud	Providing role-based HEaaS.
[18]	SEaaS	2019	Half-Cloud	Handling typo errors in SEaaS searches.
[19]		2020	Half-Cloud	Improving SEaaS using multiple threads for searching.
[6]		2023	Full-Cloud	Improving SEaaS by probabilistic encryption.
[16]	PREaaS	2019	Full-Cloud	Improving PREaaS by changing the proxy location.
[17]		2021	Full-Cloud	Using elliptic curves to improve PREaaS.
[12]	QEaaS	2019	Half-Fog	A testbed deploying QEaaS for beyond 5G networks.
[14]		2021	Full-Cloud	A QEaaS platform for protecting aerial vehicles.
[24]	GEaaS	2019	Half-Cloud-Fog	Protecting smart substations with Knapsack algorithm.
[2]		2020	Full-Cloud	Changing encryption configurations using an agent.
[23]		2021	Full-Cloud	Protecting traffic between Kubernetes pods.

we have investigated these platforms based on the encryption type they provide, such as symmetric, asymmetric, and homomorphic encryption. However, EaaS platforms face two significant challenges: the availability of the components and the trade-off between the number of covered devices and the service performance. To address these issues, researchers have proposed various solutions, including implementing a Full-Cloud-Fog architecture that combines the benefits of both centralized and distributed architectures. Furthermore, utilizing machine learning approaches such as deep learning and reinforcement learning can also enhance the performance of EaaS platforms. These approaches can help optimize the encryption algorithms and protocols and predict the components' availability.

Acknowledgment

This research work is partially supported by the European Union's Horizon Europe research and innovation program HORIZON-JU-SNS-2022 under the RIGOUROUS project (Grant No. 101095933). The paper reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains.

Bibliography

[1] Al-Shabi, M.: A survey on symmetric and asymmetric cryptography algorithms in information security. International Journal of Scientific and Research Publications (IJSRP) **9**(3), 576–589 (2019)

[2] Ateeq, K., Pradhan, M.R., Mago, B., Ghazal, T.: Encryption as a service for multi-cloud environment. International Journal of Advanced Research in Engineering and Technology (IJARET) **11**(7), 622–628 (2020)

[3] Blömer, J., Günther, P., Krummel, V., Löken, N.: Attribute-based encryption as a service for access control in large-scale organizations. In: International Symposium on Foundations and Practice of Security, pp. 3–17, Springer (2017)

[4] Deb, P.K., Mukherjee, A., Misra, S.: Ceaas: Constrained encryption-as-a-service in fog-enabled iot. IEEE Internet of Things Journal (2022)

[5] Ibtihal, M., Hassan, N., et al.: Homomorphic encryption as a service for outsourced images in mobile cloud computing environment. In: Cryptography: breakthroughs in research and practice, pp. 316–330, IGI Global (2020)

[6] Ihtesham, M., Tahir, S., Tahir, H., Hasan, A., Sultan, A., Saeed, S., Rana, O.: Privacy preserving and serverless homomorphic-based searchable encryption as a service (seaas). IEEE Access (2023)

[7] Javadpour, A., Ja'fari, F., Taleb, T., Shojafar, M., Benzaïd, C.: A comprehensive survey on cyber deception techniques to improve honeypot performance. Computers & Security p. 103792 (2024)

[8] Javadpour, A., Ja'fari, F., Taleb, T., Shojafar, M., Yang, B.: Scema: an sdn-oriented cost-effective edge-based mtd approach. IEEE Transactions on Information Forensics and Security **18**, 667–682 (2022)

[9] Javadpour, A., Ja'fari, F., Taleb, T., Zhao, Y., Bin, Y., Benzaïd, C.: Encryption as a service for iot: Opportunities, challenges and solutions. IEEE Internet of Things Journal (2023)

[10] Olanrewaju, R.F., Islam, T., Khalifa, O.O., Anwar, F., Pampori, B.R.: Cryptography as a service (caas): quantum cryptography for secure cloud computing. Indian Journal of Science and Technology **10**(7), 1–6 (2017)

[11] Patel, A., Patel, D., Kakkar, R., Oza, P., Agrawal, S., Tanwar, S., Sharma, R., Yamsani, N.: Safeguarding the iot: Taxonomy, security solutions, and future research opportunities. Security and Privacy **7**(2), e354 (2024)

[12] Raddo, T.R., Rommel, S., Land, V., Okonkwo, C., Monroy, I.T.: Quantum data encryption as a service on demand: Eindhoven qkd network testbed. In: 2019 21st International Conference on Transparent Optical Networks (ICTON), pp. 1–5, IEEE (2019)

[13] Rahimi, N., Reed, J.J., Gupta, B.: On the significance of cryptography as a service. Journal of Information Security **9**(4), 242–256 (2018)

[14] Ralegankar, V.K., Bagul, J., Thakkar, B., Gupta, R., Tanwar, S., Sharma, G., Davidson, I.E.: Quantum cryptography-as-a-service for secure uav communication: Applications, challenges, and case study. IEEE Access (2021)

[15] Saxena, U.R., Alam, T.: Role-based access using partial homomorphic encryption for securing cloud data. International Journal of System Assurance Engineering and Management **14**(3), 950–966 (2023)

[16] Sbai, A., Drocourt, C., Dequen, G.: Pre as a service within smart grid city. In: 16th international conference on security and cryptography, pp. 394–401, SCITEPRESS-Science and Technology Publications (2019)

[17] Sbai, A., Drocourt, C., Dequen, G.: Cloud file sharing using preaas. EHEI-Journal of Science & Technology **1**(2), 52–63 (2021)

[18] Tahir, S., Ruj, S., Sajjad, A., Rajarajan, M.: Fuzzy keywords enabled ranked searchable encryption scheme for a public cloud environment. Computer Communications **133**, 102–114 (2019)

[19] Tahir, S., Steponkus, L., Ruj, S., Rajarajan, M., Sajjad, A.: A parallelized disjunctive query based searchable encryption scheme for big data. Future Generation Computer Systems **109**, 583–592 (2020)

[20] Thabit, F., Can, O., Aljahdali, A.O., Al-Gaphari, G.H., Alkhzaimi, H.A.: A comprehensive literature survey of cryptography algorithms for improving the iot security. Internet of Things p. 100759 (2023)

[21] Unal, D., Al-Ali, A., Catak, F.O., Hammoudeh, M.: A secure and efficient internet of things cloud encryption scheme with forensics investigation compatibility based on identity-based encryption. Future Generation Computer Systems **125**, 433–445 (2021)

[22] Xu, R., Joshi, J.B.: Enabling attribute based encryption as an internet service. In: 2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC), pp. 417–425, IEEE (2016)

[23] Yang, B., Zhang, F., Khan, S.U.: An encryption-as-a-service architecture on cloud native platform. In: 2021 International Conference on Computer Communications and Networks (ICCCN), pp. 1–7, IEEE (2021)

[24] Zhang, H., Qin, B., Tu, T., Guo, Z., Gao, F., Wen, Q.: An adaptive encryption-as-a-service architecture based on fog computing for real-time substation communications. IEEE Transactions on Industrial Informatics **16**(1), 658–668 (2019)