Encryption as a Service for IoT: Opportunities, Challenges and Solutions

Amir Javadpour, Forough Ja'fari, Tarik Taleb, Yue Zhao, Yang Bin, and Chafika Benzaïd

***Abstract*—The widespread adoption of Internet of Things (IoT) technology has introduced new cybersecurity challenges. Encryption services are being offloaded to cloud and fog platforms to mitigate these risks. Encryption as a Service (EaaS) emerges as a remedy, offering cryptographic solutions tailored to the resource constraints of IoT devices. This study thoroughly examines existing EaaS platforms, categorizing them based on encryption algorithms and service offerings. Additionally, we outline various EaaS architecture types depending on the placement of key components. Practical implementations of these platforms are explored through different testbeds. A key focus lies in dissecting the challenges that EaaS faces, particularly in the context of IoT, while suggesting potential remedies. This work stands out as an all-encompassing exploration, bridging the gap left by previous surveys.**

***Index Terms*—Encryption as a Service (EaaS), Internet of Things (IoT), Cloud computing, and Fog computing.**

I. Introduction

THE growth in the number of cyberattacks has led to a significant increase in countermeasure activities, such as cryptography. In the past, the cryptography process was performed on the server-side and/or the client-side. However, both of these sides have some weaknesses. Due to resource limitations on processing power-constrained devices (e.g., Internet of Things - IoT - devices such as sensors), it is impossible to expect all clients to be able to run encryption/decryption algorithms, especially the complex and computation-intensive ones. On the other hand, specifying a particular server for running these algorithms may be risky, as it can be a single-point-of-failure in the overall chain of cryptography processes [1]. As a result, the term "Encryption as a Service (EaaS)" has been recently coined to overcome these problems. Researchers, working on this concept, believe that the concept of "Anything as a Service (XaaS)" can also encompass the cryptography process. It is worth noting that EaaS is interchangeably referred to as ”Cryptography as a Service (CaaS)". For the sake of simplicity, we refer to it as EaaS throughout this paper.

Some of the applications used for EaaS by many large companies, such as Google and Microsoft, have features and encryption solutions running in the cloud environment. This approach naturally requires less processing power and memory than encryption solutions on dedicated physical machines. In addition, such an approach enables the provisioning of different security patterns and policies for each part of the organization, and all critical data are securely exchanged through encryption. Some of these applications include online encryption and resource availability in the cloud. With online encryption, all employees of an organization can exchange their data with their colleagues and customers with confidence and security. Using EaaS can meet the security guidelines of organizations and keep important documents, emails, and data safe. Effectively, the use of EaaS can make resources available and secure. Since data in the cloud environment can be stored on different platforms, using EaaS can improve the reliability of data access.

The IoT paradigm has the potential to transform all aspects of human life. However, cybercriminals increasingly target IoT systems and devices to carry out malicious attacks. IoT networks are heterogeneous and contain many resource-constrained devices. Therefore, EaaS is vital for IoT devices to cope with resource limitations. As a result, the objective of this paper is to review the current EaaS platforms and analyze their properties, and that is to investigate their effectiveness and the potential applicability to IoT Wang et al., Kaur et al., Singh et al., Kang et al. [2, 3, 4, 5].

To the authors' best knowledge, only two survey papers have addressed the topic of EaaS. Olanrewaju et al. [6] studied some of the EaaS platforms and compared their functionalities with the Kerberos protocol, which is a network security protocol that protects communications between different network components. Rahimi et al. [7] analyzed EaaS platforms' efficiency, implementation, and possible applications. However, these two studies are relatively old and do not cover recent research in the field of EaaS. Particularly, they do not discuss the different EaaS architectures along with their challenges. They also miss much recent research on EaaS and are deficient in categorizing the EaaS platforms based on their features. To fill this gap, this paper surveys a wide range of research on EaaS, considering the above-mentioned aspects.

In this paper, we embark on a comprehensive exploration of the burgeoning field of Encryption as a Service (EaaS) platforms. Through a meticulous review and analysis of diverse

Amir Javadpour is with ICTFICIAL Oy, Espoo, Finland. He was with the Faculty of Information Technology and Electrical Engineering, University of Oulu when this research work was initiated (e-mail: a.javadpour87@gmail.com). **Forough Ja'fari** is with the Department of Computer Engineering, Sharif University of Technology, Tehran, Iran (e-mail: azadeh.mth@gmail.com). **Tarik Taleb** is with the Faculty of Information Technology and Electrical Engineering, Oulu University, Oulu, 90570 Finland. He is also with the Faculty of Electrical Engineering and Information Technology, Ruhr University Bochum, Bochum Germany (e-mail: talebtarik@gmail.com). **Yue Zhao** is with the Science and Technology on Communication Security Laboratory, Chengdu, China, 610041. (e-mail:yuezhao@foxmail.com) **Yang Bin** is with the School of Computer and Information Engineering, Chuzhou University, China, and also with MOSAIC LAB, Finland.(e-mail: yangbinchi@gmail.com) **Chafika Benzaïd** is with the faculty of Information Technology and Electrical Engineering, Oulu University, Oulu, 90570 Finland. (e-mail: chafika.benzaid@oulu.fi)

Corresponding Author: Amir Javadpour

research endeavors, we delve into the multifaceted realm of EaaS, elucidating its architecture, taxonomy, challenges, and prospects. The pivotal contributions of this study are manifold:

- Offering a systematic framework for understanding the diverse EaaS platforms and their contributions to data security, enabling readers to make informed decisions about adopting and implementing these solutions.
- Highlighting the role of EaaS in addressing the critical security challenges posed by the proliferation of connected devices and cloud services, thereby fostering a safer and more resilient digital ecosystem.
- Advancing the state of the art by not only presenting existing research but also suggesting novel architectural paradigms and approaches to overcome the limitations of current EaaS implementations.
- Emphasizing the practical relevance of EaaS platforms in various industries and sectors, including healthcare, finance, and communication, where data protection and confidentiality are paramount.
- Encouraging interdisciplinary collaborations between researchers in cryptography, cloud computing, IoT, and machine learning, fostering a holistic approach towards enhancing the security and efficiency of EaaS platforms.
- Providing valuable insights for policymakers and industry practitioners, helping them understand the evolving landscape of secure data management and aiding them in making informed decisions regarding adopting and deploying EaaS solutions.
- Ultimately contributing to the advancement of secure digital infrastructures by shedding light on the promising avenues of research, development, and application in Encryption as a Service. By offering a comprehensive view of the existing landscape, challenges, and potential solutions, this paper aims to inspire further research, innovation, and collaboration toward creating robust and scalable EaaS platforms that cater to our interconnected world's evolving data security needs.

A. Motivations

As authors, we are driven by the pressing need to address the escalating security challenges posed by the ever-expanding digital landscape, especially in the Internet of Things (IoT) context. The burgeoning volume of sensitive data being generated, transmitted, and stored demands innovative solutions to safeguard this information against evolving threats. Encryption as a Service (EaaS) emerges as a beacon of hope, offering the potential to revolutionize how we approach data security.

Our motivation lies in comprehensively exploring the intricate tapestry of EaaS platforms, and dissecting their architectures, functionalities, and implementations. By meticulously categorizing these platforms into distinct architectural paradigms, ranging from Full-Cloud to Half-Cloud-Fog, we reveal the nuanced strategies required to meet the diverse security demands of various application domains. But our work doesn't stop at mere categorization; it delves deeper into the heart of the challenges that EaaS platforms confront. In our pursuit of excellence, we unearth EaaS platforms' challenges, ranging from availability concerns to the delicate balancing act between service performance and accommodating many devices. Our paper offers more than a mere identification of these challenges; it presents innovative solutions that have the potential to redefine the landscape of data security. Our proposed architectural designs and the strategic integration of machine learning techniques lay the foundation for a future where EaaS becomes an even more potent shield against emerging threats. As authors, we embark on this journey not just to survey the existing landscape, but to pave the way for future advancements. Our paper is a call to action, a catalyst for fostering collaboration between researchers, practitioners, and technologists. It is a beacon guiding the evolution of Encryption as a Service, inspiring us to collectively rise above challenges, harness innovation, and forge a more secure and resilient digital future.

B. Core objectives

The core objectives of our paper are to provide a comprehensive overview of Encryption as a Service (EaaS) platforms, encompassing their diverse architectures, functionalities, and deployment strategies. Through meticulous categorization into architectural classes like Full-Cloud, Half-Cloud, Half-Fog, and Half-Cloud-Fog, we aim to present a clear roadmap for navigating the intricate landscape of EaaS solutions. By identifying and articulating the challenges confronting EaaS platforms in both general and IoT contexts, we intend to illuminate the complex interplay between security requirements, service performance, scalability, and more. Furthermore, our paper aspires to propose innovative solutions that enhance the efficiency, effectiveness, and resilience of EaaS platforms, fostering new avenues for research and development. We seek to empower stakeholders with actionable insights by exploring real-world testbeds, security analysis, and tailored recommendations for IoT environments. Ultimately, our paper strives to inspire collaboration, motivate future research, and contribute to the collective knowledge base, thereby shaping the evolution of EaaS and data security.

C. Highlighting Detailed Challenges

Recognizing the importance of thoroughly outlining the challenges at the forefront of our paper's focus, we will enhance our introduction section to provide a comprehensive view of the intricate challenges inherent in the problems under scrutiny. Our intent is to offer readers a clear understanding of the complexities that Encryption as a Service (EaaS) architectures must contend with, particularly in the Internet of Things (IoT) context. To address this aspect more effectively, we will delineate the specific challenges that our paper seeks to address. These include:

• Scalability and Resource Constraints: IoT networks comprise many devices with varying resources and processing capabilities. The introduction will emphasize how EaaS platforms must grapple with the challenge of efficiently scaling to accommodate the sheer number of devices while respecting their resource limitations.

• Security and Privacy: Securing IoT data is paramount, considering the potential vulnerabilities in communication and storage. We will elaborate on how EaaS solutions must provide robust encryption and authentication mechanisms to protect sensitive information from unauthorized access or breaches.

• Dynamic Network Characteristics: IoT networks are characterized by their dynamic nature, with devices frequently joining, leaving, or moving within the network. We will highlight how EaaS architectures must adapt to these changes, ensuring seamless encryption services for all devices regardless of network status.

• Availability and Reliability: IoT applications often demand high availability and reliability. The introduction will underscore how EaaS platforms need to ensure consistent and reliable encryption services despite potential network disruptions or component failures. Performance and Latency: IoT devices may have real-time requirements, necessitating low latency in encryption processes. We will elaborate on achieving efficient encryption without compromising the devices' operational performance.

• Attack Resilience: The diverse attack landscape in IoT networks poses a significant challenge to EaaS architectures. The introduction will elucidate how these platforms must incorporate defenses against threats like DDoS attacks, botnets, and various cyber threats. By elucidating these challenges, we will set the stage for the subsequent discussions on EaaS platforms and their categorization, while emphasizing the significance of our survey in addressing the intricate issues within the realm of IoT security. This enhancement will empower readers to grasp the intricate landscape our paper navigates and the subsequent solutions it proposes.

The remainder of this paper is structured as follows. section II gives some background about encryption processes and the general concept of EaaS. In section III, we introduce the different components of an EaaS platform and highlight the proposed architecture types. section IV categorizes the reviewed research work based on the underlying encryption type. The different services that are provided by an EaaS platform are presented in section V. In section VI, we discuss the implementation details and introduce the testbeds that are considered for the EaaS platforms. section VII discusses the pending challenges of EaaS platforms, and section IX accordingly defines future research directions. Finally, the paper concludes in section X.

II. Background

Cryptography, a fundamental component of modern information security, encompasses techniques to safeguard data from unauthorized access or alteration. At its core, cryptography involves three core processes: encryption, decryption, and key generation. Encryption transforms plaintext data into ciphertext, rendering it unreadable to anyone without the appropriate decryption key. Decryption, the reverse process, converts ciphertext back into its original plaintext form. These operations rely on cryptographic keys, which act as the linchpin of data protection. Symmetric encryption methods employ a single key for both encryption and decryption, while asymmetric encryption utilizes a pair of keys: a public key for encryption and a private key for decryption [8]. For example, the widely used Advanced Encryption Standard (AES) is a symmetric algorithm, while the Rivest, Shamir, and Adleman (RSA) algorithm exemplify an asymmetric approach. The security of cryptographic systems hinges on the chosen algorithm and the keys' length. Longer keys enhance security by exponentially increasing the complexity of breaking the encryption. In this era of interconnected systems and relentless cyber threats, selecting appropriate cryptographic algorithms and key lengths is critical in upholding data confidentiality and integrity.

Encryption as a Service (EaaS) represents a forward-looking solution to address the challenges arising from device resource limitations and the demand for robust cryptographic protection. Cryptography, encompassing encryption, decryption, and key generation, is pivotal in safeguarding sensitive data against unauthorized access. Traditionally, encryption tasks were executed either on the server-side or client-side. However, these approaches come with inherent vulnerabilities. Devices with constrained processing power, notably those within the Internet of Things (IoT) landscape, grapple with executing intricate encryption algorithms due to their finite resources. Conversely, relying exclusively on a designated server for cryptographic operations introduces a singular point of failure within the overarching encryption process. In response to these complexities, the EaaS concept emerged. EaaS involves externalizing cryptographic services to cloud and fog platforms, allowing efficient encryption and decryption management while accommodating diverse devices' constraints. Doing so removes the burden of executing resource-intensive algorithms from individual devices, ensuring security without straining them. EaaS platform architectures can be categorized into three layers: the cloud layer, often endowed with robust resources; the fog layer, situated closer to the edge to strike a balance between resources and proximity; and the device layer, where resource-constrained devices reside. While not all EaaS platforms embrace all three layers, a comprehensive understanding of the concept is attained through an illustrative workflow encompassing the cloud, fog, and device layers. The cloud layer undertakes resource-intensive functions, such as key generation, while the fog layer facilitates localized encryption and decryption Wang et al. [9]. Concurrently, the device layer contributes to secure encryption execution on individual devices, culminating in a holistic and resilient data protection approach. This framework empowers organizations and individuals to realize secure data transmission benefits without overtaxing their devices or exclusively relying on centralized servers. Ultimately, EaaS embodies a transformative shift in cryptographic practices, aligning with the evolving digital security landscape. This perspective complements the discussion on EaaS components' location across the cloud, fog, and device layers, enhancing clarity through the exemplified workflow involving these three layers (as depicted in Figure 1). In this scenario, the service manager stationed within the cloud layer is pivotal in orchestrating platform-wide operations. Complementing this, server nodes are strategically situated within the fog layer, adding an edge dimension to

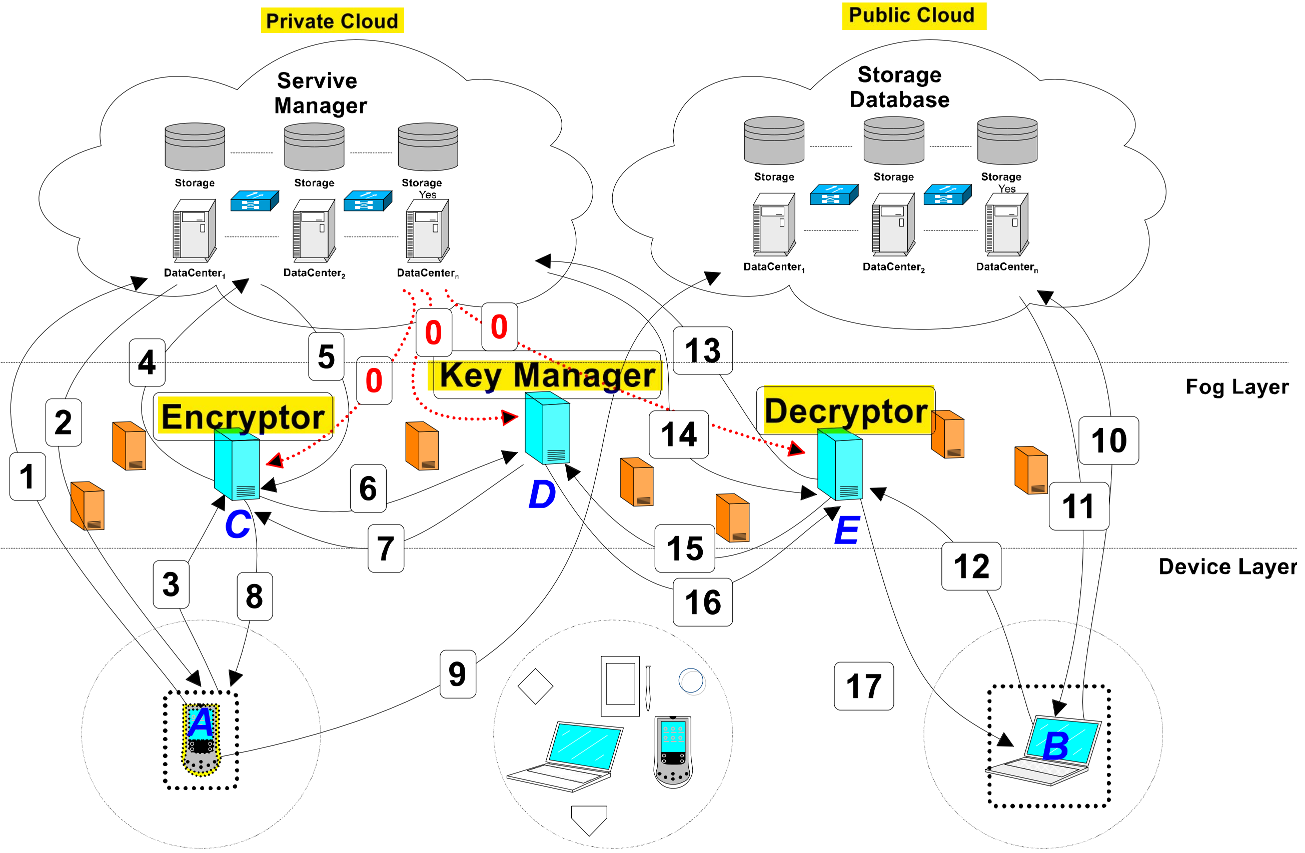

Fig. 1. The workflow of a sample EaaS platform involving the cloud, fog, and device layers: 0) Giving a certificate to a service provider to make it trusted as an encryptor, decryptor, or key manager. 1) Asking for the list of trusted encryption service providers. 2) Responding to the list of trusted encryption service providers. 3) Choose one of the encryptors and send the data to be encrypted together with other required information. 4) Asking for the appropriate encryption configuration. 5) Responding with a suitable encryption configuration. 6) Asking for a pair of keys regarding the encryption configuration. 7) Responding with the required pair of keys. 8) Encrypting the data and sending the encrypted data. 9) Sending the encrypted data to be stored on the public cloud. 10) Requesting encrypted data that is shared on the public cloud. 11) Responding with the requested data. 12) Choose one of the decryptors and send the encrypted data. 13) Asking for the decryption configuration based on the encryption history. 14) Responding with the specific decryption configuration. 15) Asking for a pair of keys regarding the encryption history. 16) Responding with the specific pair of keys. 17) Decrypting the data and sending the decrypted data.

the architecture. The procedural sequence unfolds with the proactive involvement of the service manager, who, in the initial phase (step 0), meticulously designates certain fog servers as eligible recipients of certificates, thus conferring upon them the esteemed status of trusted service providers. This meticulous process marks a foundational step towards ensuring the security and reliability of subsequent cryptographic processes within the EaaS framework.

Let's consider an IoT device, say A, in the device layer that needs to encrypt its data and sends it to the public cloud storage database; so it could be shared with another end-device, say B. First, A asks the service manager for the list of trusted encryption service providers (step 1). The service manager responds with the requested list (step 2). Now A knows the trusted service providers, and selects one of the encryptors, say C, for further communication. In the next step, A sends its raw data, which must be encrypted, to C (step 3). A also sends some extra required information. For example, in some EaaS platforms, the service provider needs to know the resource status of the end devices. This information may be used to select the appropriate encryption algorithm. After receiving the data, C asks the service manager about the appropriate encryption configurations (step 4). For example, C sends the domain of A to the service manager, and the service manager decides which algorithm is preferable for that domain. Hence, in the next step, the service manager responds with the appropriate encryption configuration (step 5). C also requires a pair of keys for encrypting the data. Hence, C asks for a pair of keys from a key manager, say D (step 6). Subsequently, D provides the keys (step 7). After that, C executes the encryption algorithm and sends the encrypted data to A (step 8). After receiving the encrypted data, A sends it to a public cloud server to store it or share it with other users (step 9). Now, it is B's turn to retrieve the data. It is worth noting that B performs the first and second steps, similar to A, for receiving the list of trusted service providers. Then, B connects to the public cloud to get the shared data (step 10). The public cloud responds with the A's encrypted data (step 11). In the next step, B sends the encrypted data to one of the trusted decryptors, say E

TABLE I
THE DESCRIPTION OF THE EAAS COMPONENTS.

Component	Type	Description
Device Node (DN)	Infrastructure	The end devices which ask for a cryptography service.
Cloud Node (CN)	Infrastructure	The powerful machines located on the cloud layer.
Fog Node (FN)	Infrastructure	The intermediary nodes located on the fog layer.
Key management Component (KC)	Crypto	The component responsible for creating and managing the keys.
Encryption Component (EC)	Crypto	The component that encrypts the plaintext.
Decryption Component (DC)	Crypto	The component that decrypts the ciphertext.
General Management Component (GC)	Crypto	The component that performs the other management activities.

to decrypt it (step 12). When the encrypted data is received, E asks the service manager about its history to determine the appropriate decryption configuration (step 13), and the service manager responds (step 14). E also requires the exact pair of keys for decrypting it. Note that in some decryption methods, such as asymmetric encryption algorithms, E only requires the public key. E asks for the appropriate key(s) from D (step 15), and D responds (step 16). Finally, E decrypts the ciphertext and sends the decrypted data to B (step 17). At this time, B can access the original data.

III. EAAS ARCHITECTURES

The perspective of the EaaS platform is multifaceted, encompassing two key dimensions. The first facet pertains to the foundational infrastructure components, encompassing cloud and fog nodes, communication networks, and end devices. Meanwhile, the second facet revolves around the cryptographic components, including entities like encryptors, decryptors, and key managers. Diverse architectural approaches have been put forth to conceptualize EaaS systems, diverging in how they orchestrate the integration of cryptographic components within the broader infrastructure context. In this section, we embark on a comprehensive exploration of these dimensions. We introduce the fundamental components that constitute the EaaS ecosystem, subsequently delving into an examination of the various architectural models that have emerged in the realm of EaaS platforms. Through this exploration, we aim to provide a holistic understanding of the intricate interplay between infrastructure and cryptographic elements within the purview of EaaS.

An EaaS platform consists of different components, with different roles and responsibilities, which are summarized in Table I. The main infrastructure components are as follows:

- **Device Node (DN):** These nodes are the end-devices, most of which have limited resources. Some DNs are IoT devices, smartphones, TVs, wearable devices, smart vehicles, and notebooks. DNs are the clients that request cryptography services.
- **Cloud Node (CN):** These nodes are the physical or virtual machines in the cloud environment, with almost powerful resources to perform complicated tasks and also to give storage space to the clients.

TABLE II
THE DETAILS OF THE CURRENTLY PROPOSED ARCHITECTURES FOR EAAS.

Reference	KC	EC	DC	GC	Architecture
Yang et al. [10]	CN	CN	CN	CN	Full-Cloud
Xu and Joshi [11]	CN	CN/DN	CN/DN	CN	Half-Cloud
Deb et al. [12]	FN	DN	DN	FN	Half-Fog
Zhang et al. [13]	FN	DN	DN	CN	Half-Cloud-Fog
Our suggestion	FN	CN	FN	CN	Full-Cloud-Fog

- **Fog Node (FN):** These nodes are located in the fog layer of the infrastructure, or in other words, on the edge of the network. FNs can be considered as the intermediary layer between DNs and CNs.

Crypto components perform one or some of the cryptography process steps. They are as follows:

- **Key management Component (KC):** This component creates the keys and performs all processes related to the key management step.
- **Encryption Component (EC):** This component is responsible for encrypting a plaintext with a specified key to generate the ciphertext.
- **Decryption Component (DC):** This component performs the decryption by getting the ciphertext and the key, and re-generating the plaintext.
- **General management Component (GC):** The other management activities of a cryptography process, such as choosing the appropriate algorithm and checking the user's authorities, are performed by this component.

Several types of research exist with a proposed architecture for EaaS. The proposed architectures differ in the way of mapping the crypto components onto the network components. The currently proposed architectures can be categorized into four groups: Full-Cloud, Half-Cloud, Half-Fog, and Half-Cloud-Fog. The term ”Full” means that all operations are performed without involving DNs, while the term ”Half” means that DNs perform some of the operations. The selection of the terms ”Cloud” and ”Fog” specifies the location of the components without considering the device's layer. These architectures are described in the remainder of this section.

A. Full-Cloud architecture

In the Full-Cloud architecture, all crypto components are located on CNs, and DNs just perform some simple processes to get the cryptography service. In other words, all the main cryptography processes are performed on the cloud layer. As a result, there is no limitation in getting the encryption services regarding the resource constraints of DNs. Most current EaaS platforms have Full-Cloud architecture, due to its plain implementation. It must be noted that since all crypto components are located on CNs, the whole process may have an extra delay. This architecture is shown in Figure 2.

The architecture proposed by Anenas et al. [10] exemplifies the Full-Cloud approach. In this architecture, all cryptographic components are centralized within the cloud layer. When users initiate encryption services, their data is routed to a proxy residing in the cloud. Subsequently, the data is encrypted and transmitted to its intended destination. This configuration

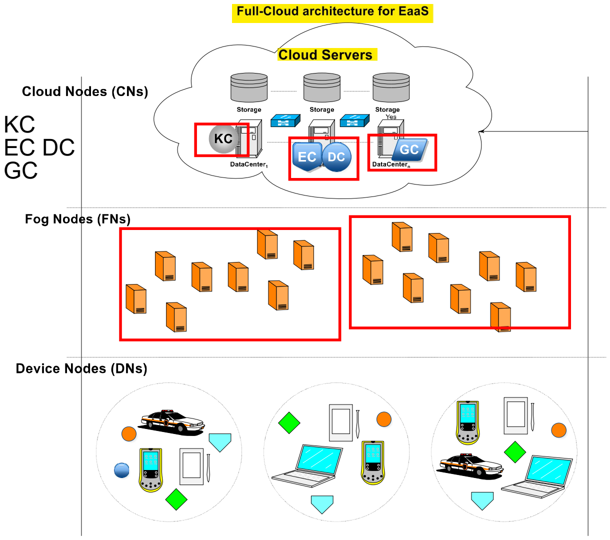

Fig. 2. The Full-Cloud architecture proposed for EaaS.

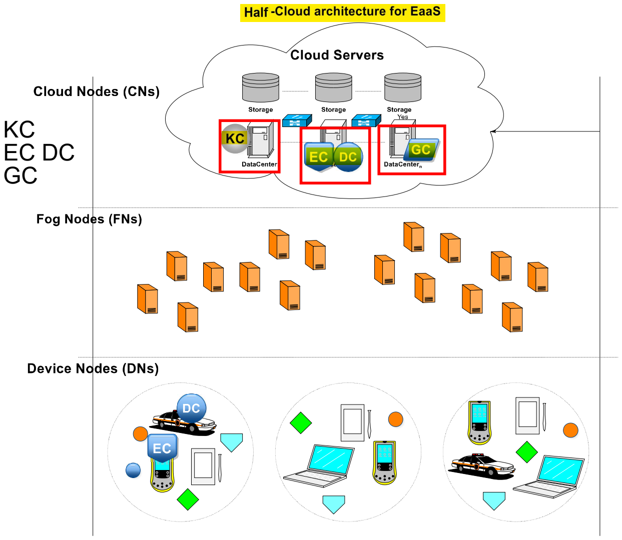

Fig. 3. The Half-Cloud architecture proposed for EaaS.

minimizes the impact of resource limitations on Distributed Nodes (DNs), ensuring efficient and reliable encryption processes. The Full-Cloud architecture's advantage lies in its straightforward implementation and its capacity to overcome DNs' processing constraints. However, it is important to note that the centralized nature of this architecture could introduce potential delays in the overall process due to data transfer between layers.

B. Half-Cloud architecture

In the Half-Cloud architecture, some of the crypto components are located within the cloud layer (i.e., on CNs), and the others are located on DNs. In such architecture, DNs must have the required resources, but, they are not expected to perform complex tasks. They perform some simple computations. The overview of this architecture is shown in Figure 3

The architecture proposed by Xu and Joshi [11] as a Half-Cloud implementation exhibits a distributed configuration comprised of two distinct types of nodes: manager nodes and work nodes, both situated within the cloud layer. One of the manager nodes functions as a backup, enhancing the platform's availability and resilience. These nodes collectively form the backbone of the architecture, with the primary manager node serving as the GC. This pivotal role involves task allocation and process delegation among the designated work nodes, encompassing various cryptographic components like EC, DC, and KC. This distribution of responsibilities provides a scalable and efficient approach to cryptographic processes. In the scenario where a DN necessitates data encryption, it initiates a request to the GC, setting the process in motion. The GC, acting as an orchestrator, intelligently assigns tasks to suitable work nodes. Subsequently, the EC/DC and KC components collaborate to transmit an intermediate ciphertext and a pair of keys to the designated work node. Employing these resources, the work node performs comparatively lightweight computations, utilizing the intermediate ciphertext to encrypt the primary data. This strategically offloads the more resource-intensive processes to the cloud layer while making efficient use of available computational resources. Similarly, in the decryption process, a DN seeking to access encrypted data contacts the KC and GC for the requisite key pair. The GC's authorization check, followed by the delivery of the intermediate ciphertext from EC/DC, ensures that only authorized nodes can access and decrypt the data. This balanced distribution of encryption and decryption operations, coupled with the utilization of cloud resources for computationally intensive tasks, embodies the core principles of the Half-Cloud architecture. By judiciously dividing tasks between the cloud and device layers, this architecture optimizes resource allocation, performance, and security in a comprehensive manner.

C. Half-Fog architecture

The EaaS platforms with the Half-Fog architecture have some crypto components located on FNs, and others located on DNs. As a result, DNs that ask for an encryption service must have the minimum required resources. This architecture is illustrated in Figure 4.

The study presented by Deb et al. [12] introduces a Half-Fog architecture that embraces the distinct roles of Fog Nodes (FNs) and Distributed Nodes (DNs) within an EaaS platform. In this innovative arrangement, FNs are designated with the pivotal tasks of determining the most suitable encryption algorithm and generating the requisite encryption keys. In contrast, the other essential cryptographic components, encompassing tasks executed by entities like Encryption Components (ECs) and Decryption Components (DCs), are strategically positioned on DNs. In this delineation of responsibilities, FNs undertake the management facets of the cryptographic processes, facilitating informed algorithmic choices and key provisioning, while the more resource-constrained DNs take on the central role of executing the fundamental encryption

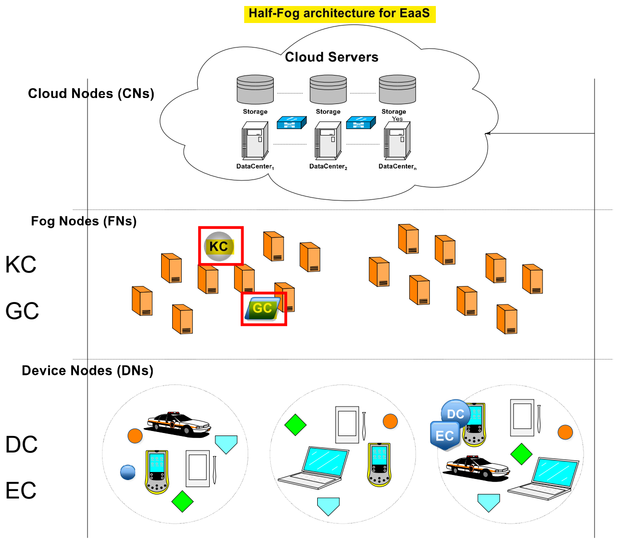

Fig. 4. The Half-Fog architecture proposed for EaaS.

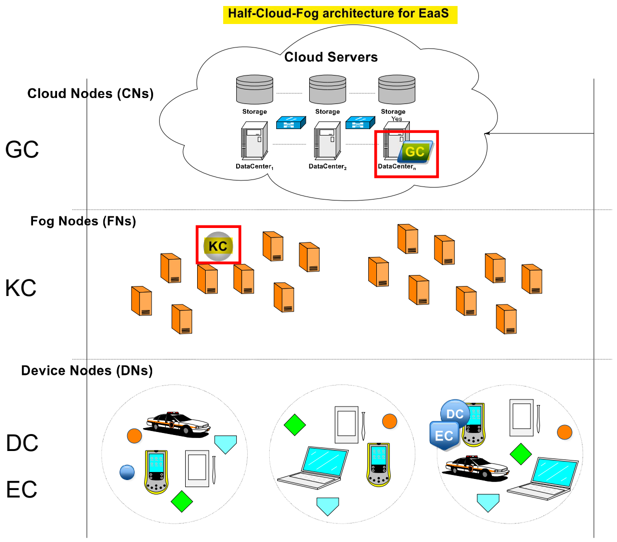

Fig. 5. The Half-Cloud-Fog architecture proposed for EaaS.

and decryption operations. This architectural configuration optimally balances the computational burden between FNs and DNs, ensuring that each node is primed to fulfill its designated function optimally. Notably, the process commences with a DN with data requiring encryption and submitting a request to the Global Coordinator (GC) or Key Coordinator (KC). In response, the GC orchestrates selecting an encryption algorithm, while the KC issues the necessary encryption keys. Armed with this cryptographic data, the source DN performs the encryption process and forwards the encrypted data to another device or even a public cloud storage destination. Noteworthy is the fact that the intricate encryption and decryption processes are fully executed on the DNs, reinforcing the potency of the Half-Fog architecture in accommodating the resource constraints of these nodes while delivering robust cryptographic services.

D. Half-Cloud-Fog architecture

The Half-Cloud-Fog architecture divides the whole crypto components between all network components. In this architecture, all network nodes provide the encryption service. DNs in this architecture must have the required resources. The scheme of this architecture is illustrated in Figure 5.

The architectural proposal detailed in Zhang et al. [13] introduces a Half-Cloud-Fog architecture, a hybrid model that intricately distributes responsibilities among Cloud Nodes (CNs), Fog Nodes (FNs), and Device Nodes (DNs). This architecture capitalizes on the strengths of each component to achieve an optimized EaaS platform. CNs are entrusted with general management operations, while FNs are specialized in the critical task of key management. DNs, the resource-constrained yet essential participants, are responsible for executing the encryption and decryption processes Javadpour et al. [14]. It is important to note that not all DNs are tasked with these cryptographic operations; rather, the architecture identifies the most capable DNs for the task. Consider a scenario in which a DN, labeled as A, aims to transmit data to another DN, denoted as B. The process unfolds as follows: In the initial step, DN A transmits the plaintext to a neighboring DN, say C, which is equipped to perform the encryption process. Subsequently, DN C solicits a pair of encryption keys from an FN. These FNs are intricately connected with CNs, thus possessing the necessary insights into the appropriate encryption configuration. Armed with the requested keys and configuration data, the FN furnishes DN C with the requisite resources. Following this, the ciphertext is conveyed to another DN, say D, which boasts the capacity for decrypting the received data. DN D similarly interfaces with FNs in its decryption endeavor. Ultimately, the decrypted data is conveyed to its intended recipient, DN B. This intricate choreography of interactions between CNs, FNs, and DNs showcases the collaborative synergy of the Half-Cloud-Fog architecture, adeptly leveraging the unique strengths of each component to realize a secure and efficient EaaS platform.

IV. EaaS Encryption Types

An EaaS platform may provide different types of encryption services. Hence, we can categorize them based on the encryption type as follows. These researches are summarized in Table III.

A. Attribute-Based EaaS (ABEaaS)

Attribute-based encryption is a type of cryptography technique, wherein the crypto features vary based on the different attributes of the users or the environment. The ABEaaS platforms provide encryption services that change according to different conditions.

Xu and Joshi [11] proposed a platform for ABEaaS, wherein the attributes of the users are considered in the encryption/decryption operations. When a user asks for an encryption service, the EC/DC gets its attributes and creates an intermediate

TABLE III
A SUMMARY OF THE REVIEWED RESEARCHES BASED ON THEIR ENCRYPTION TYPES.

Ref.	Type	Main Idea	Architecture	Application
[11]	ABEaaS	Generating an intermediate ciphertext based on the attributes.	Half-Cloud	Mobile cloud
[12]		Selecting the appropriate encryption algorithm based on the fuzzy attributes.	Half-Fog	Fog-enabled IoT
[15]		Using key encapsulation to divide the service into multiple sub-services.	Full-Cloud	General enterprises
[16]		Distributing the key management process to reduce the impact of cyber threats.	Full-Cloud	IoT clouds
[17]	HEaaS	Providing homomorphic encryption service for the healthcare systems.	Full-Cloud	Healthcare systems
[18]		Encrypting the images using homomorphic algorithms.	Full-Cloud	Mobile cloud
[19]		Parallelizing the operations performed on fully homomorphic encrypted data.	Full-Cloud	General businesses
[20]		Using a private cloud that provides enough resources for a fully homomorphic algorithm.	Full-Cloud	General companies
[21]	SEaaS	Considering the typographical errors in searching the ciphertexts.	Half-Cloud	Public clouds
[22]		Using multiple threads for handling the search process.	Half-Cloud	Public clouds
[23]	PREaaS	Forwarding emails with an anonymous re-encryption proxy.	Half-Cloud	Smart grid cities
[24]		Locating the proxy on a multi-cloud system for time-efficient re-encrypting operations.	Full-Cloud	Smart grid cities
[25]		Using elliptic curves concept to reduce the key length and the consumed time.	Full-Cloud	General companies
[26]	QEaaS	Considering a middle layer for converting data to photons.	Full-Cloud	UAVs
[27]		Introducing a testbed based on 6G networks providing quantum encryption services.	Full-Fog	Smart houses
[28]	GEaaS	Using parallelism to reduce the encryption service time.	Full-Cloud	General domains
[29]		Providing symmetric algorithms with different key lengths for different situations.	Full-Cloud	General domains
[30]		Providing the ability to define user access policies.	Full-Cloud	General domains
[13]		Utilizing a knapsack algorithm to maximize the security and keep the delay low.	Half-Cloud-Fog	Smart substations
[10]		Considering a proxy server for encrypting/decrypting the traffic.	Full-Cloud	Kubernetes pods
[31]		Considering an agent for managing different encryption configurations for each cloud	Full-Cloud	Multi-clouds

ciphertext based on them. Then, the user encrypts its data with that intermediate ciphertext.

The main focus of the ABEaaS platform proposed by Deb et al. [12] is to handle the heterogeneity of the fog-enabled IoT devices. FNs decide the appropriate encryption algorithm and the keys, based on different features of the devices. They used fuzzy inference systems because the device's features cannot be presented precisely. The device first sends its features to an FN, then the FN suggests an algorithm with specific keys. Three different cryptography algorithms are considered in this approach: AES-128, AES-256, and RSA. The decision is made during a two-level fuzzy technique. The first level specifies the device type, based on its CPU and RAM, and the second level specifies the algorithm, based on the device type, data size, and available network bandwidth.

Blömer et al. [15] proposed an ABEaaS platform based on two different architectures: Full-Cloud and Half-Cloud. However, the main focus is on the Full-Cloud architecture. In this platform, the user provides its attribute, such as its role, and then, a ciphertext is decrypted only if the attributes satisfy the encryption policy. A key encapsulation mechanism is considered in this platform to divide the encryption service into multiple sub-services. An ABEaaS platform is proposed by Unal et al. [16], wherein the attributes that are used for encryption/decryption processes are based on the identity of the users, such as the email addresses or the phone numbers. This IoT-based platform distributes the process of key management between different trusted components. As a result, if one of the parties is compromised by the adversary, it is unable to decrypt the user's data by itself.

B. Homomorphic EaaS (HEaaS)

The foundation of a robust cryptography algorithm lies in its ability to maintain an imperceptible connection between plaintext and ciphertext, rendering decryption nearly impossible without the appropriate keys. This tenet underscores the essence of cryptographic strength. However, certain scenarios necessitate the manipulation of ciphertexts in a manner that mirrors the desired operation on the corresponding plaintexts, achieved by decrypting them. This is where the concept of homomorphic algorithms comes into play. Homomorphic algorithms introduce an innovative facet to cryptography. Unlike traditional encryption methods, which keep the underlying relationship between plaintext and ciphertext deliberately obfuscated, homomorphic algorithms embrace a concealed yet tangible connection between the two. This connection, though inconspicuous, is structured so that specific mathematical operations performed on the ciphertext yield results consistent with the same operations conducted on the decrypted plaintext. In essence, homomorphic algorithms empower encrypted data to be processed in encrypted form, preserving privacy and security while still performing meaningful computations. The beauty of this concept is its subtlety: the underlying relationship between plaintext and ciphertext remains cryptic, thwarting any attempts at unauthorized decryption, yet the ability to perform calculations on encrypted data expands the horizon of cryptography applications. This paradigm shift in cryptographic thinking underscores the ingenious ways in which security and functionality can harmoniously coexist in the digital realm.

The work presented by El Bouchti et al. [17] introduces a noteworthy concept in the realm of healthcare systems, denoted as Homomorphic Encryption as a Service (HEaaS). In this innovative approach, users are bestowed with a level of control over the cryptographic procedures employed, elevating the user-centricity of the encryption process. Tailored specifically for healthcare systems, this platform deploys within the OpenStack infrastructure. A distinctive feature of HEaaS lies in its utilization of homomorphic encryption algorithms to safeguard sensitive patient data. The architectural foundation of HEaaS is built upon the cloud layer, encompassing all cryptographic components within this stratum. This strategic placement aligns with the principle of centralization, facilitating efficient management of the encryption and decryption processes. By housing all crypto components within the cloud, HEaaS achieves a balance between resource-intensive operations and the need for user customization. This platform paves the way for healthcare institutions to harness the power of homomorphic encryption while offering users an element of authority over cryptographic mechanisms. In essence, El Bouchti et al. [17] demonstrates the profound impact of merging homomorphic encryption with the cloud paradigm, thereby enabling healthcare systems to uphold data security while granting users a measure of influence over the encryption landscape. This symbiotic fusion encapsulates the evolving nature of data protection and underscores the pivotal role of user empowerment in shaping the future of cryptographic practices.

Ibtihal et al. [18] proposed a HEaaS for mobile cloud environments. This work focuses on providing the encryption service for images using two cloud components. The first one is for encrypting/decrypting and the second one is for storing the data. The innovative contribution of Ibtihal et al. [18] materializes in the form of HEaaS tailored specifically for the dynamic landscape of mobile cloud environments. With a dedicated emphasis on enhancing data security in the realm of images, this work introduces a novel paradigm to encryption by leveraging cloud infrastructure capabilities. At the core of this approach lies the strategic utilization of homomorphic encryption algorithms, which enable operations to be performed on encrypted data without the need for decryption. By harnessing this unique characteristic, Ibtihal et al. [18] crafts a solution that empowers users to maintain the confidentiality and integrity of their images while engaging with cloud-based services. This HEaaS platform is notably composed of two distinct cloud components, each with a distinct purpose. The first component is tasked with the critical functions of encryption and decryption, ensuring that sensitive image data remains shielded from unauthorized access. The second cloud component is dedicated to storing encrypted image data, further compartmentalizing the process and reinforcing data security. This dual-cloud architecture underscores the modular nature of the solution, enhancing both efficiency and resilience in the encryption process. By addressing the unique challenges posed by the intersection of mobile devices, cloud services, and encryption, this platform represents a significant step forward in redefining data security paradigms for modern computing landscapes.

The groundbreaking work by Zibouh et al. [19] introduces a revolutionary platform that epitomizes the concept of Fully Homomorphic Encryption as a Service (HEaaS). Distinct from traditional encryption methods, fully homomorphic encryption allows users to perform intricate arithmetic operations directly on ciphertexts, without the need for decryption. This transformative platform is designed to operate seamlessly within the OpenStack framework, showcasing its adaptability and integration capabilities within existing cloud infrastructures. The overarching objective of this HEaaS platform is to provide users with a dynamic environment where they can manipulate and process encrypted data with unprecedented flexibility. By enabling arithmetic operations on ciphertexts, users can engage in computations while preserving the confidentiality of the underlying data. This functionality holds immense potential across a multitude of applications, ranging from privacy-preserving data analysis to secure outsourcing of complex computations. Within the architecture of this platform, cloud nodes (CNs) play a pivotal role as computational workhorses. When a user submits a specific operation request, the CNs engage in performing these operations on ciphertexts in a parallelized manner. The result is then delivered back to the user, all without the need for decryption. The platform's robustness lies not only in its ability to perform computations on encrypted data, but also in its strategic parallelization to optimize processing time, acknowledging the inherent computational demands of operating on ciphertexts. In essence, the contribution of Zibouh et al. [19] advances the fusion of fully homomorphic encryption and cloud services, ushering in a new era of secure, privacy-preserving computation. By extending the capabilities of users to perform arithmetic operations on encrypted data through the medium of cloud infrastructure, this platform engenders a paradigm shift in secure computation, offering a glimpse into the transformative potential of cryptographic innovation within modern cloud ecosystems.

In the pursuit of refining and expanding the HEaaS, Zkik et al. [20] presents a pioneering platform that seeks to transcend the inherent limitations of homomorphic algorithms through the judicious utilization of cloud resources. At its core, this platform provides users with a potent toolkit for secure and versatile data manipulation, unencumbered by the conventional constraints posed by fully homomorphic encryption. Central to the architecture of this platform is a meticulously designed authentication mechanism, facilitated by a private cloud server. This authentication step ensures that only authorized users gain access to the transformative capabilities of the HEaaS platform. Once authenticated, users are empowered to issue requests for a spectrum of operations on their pre-encrypted data, effectively ushering in a new dimension of privacy-preserving computation. The technical underpinning of this platform is rooted in the use of the DGHV algorithm, a fully homomorphic encryption scheme that enables computations on encrypted data without requiring decryption. By capitalizing on the strengths of the DGHV algorithm, the platform aligns itself with the broader goals of HEaaS, while simultaneously harnessing the resource-rich environment of cloud servers to mitigate the performance limitations that often accompany fully homomorphic encryption. This platform is a testament to the synergy between cutting-edge cryptographic techniques and the vast computational prowess of cloud infrastructures. By enabling users to interact with their encrypted data in a versatile and seamless manner, Zkik et al. [20] forges a pathway towards realizing the full potential of fully homomorphic encryption. In doing so, it embarks on a journey to bridge the gap between theoretical cryptography and practical utility, thereby enriching the landscape of secure computation within modern cloud ecosystems.

C. Searchable EaaS (SEaaS)

Searchable encryption is a cryptography technique, wherein the data are encrypted while searching for them is also possible. The services that are provided by SEaaS platforms, give the user the ability to search the keywords.

Introducing a unique paradigm in secure computation, Tahir et al. [21] introduces the concept of SEaaS within the dynamic domain of British Telecommunication's public cloud. This innovative platform usher in a novel capability: the user's ability to conduct keyword searches despite typographical errors while preserving the privacy of the underlying data. Orchestrated within a Half-Cloud architecture, the architecture allocates distinct responsibilities to its cloud components. Distributed Network nodes (DNs) emerge as the powerhouses of this SEaaS platform, assuming the integral role of performing the intricate encryption and decryption processes. Their resource-intensive nature and computational capabilities render them apt for the task. In contrast, the cloud's formidable Cloud Nodes (CNs) shift their focus to a more specific role: generating search results based on encrypted data. The synergistic interplay of DNs and CNs manifests within a Half-Cloud architecture, wherein cryptographic and computational functions are meticulously segregated. The continuum of innovation leads to Tahir et al. [22], a noteworthy enhancement of the initial SEaaS framework. This evolution hinges on the astute incorporation of multiple threads to orchestrate the search process. This optimization unfolds as a response to the growing demands of modern users who seek to harness the platform's power to conduct simultaneous searches for multiple keywords. By strategically employing multiple threads, Tahir et al. [22] obviates the delays that could emerge from parallel keyword searches, thus ensuring seamless user experiences without compromising privacy or efficiency.

D. Proxy Re-EaaS (PREaaS)

Proxy re-encryption introduces a profound mechanism in secure data transmission, enabling proxies to mediate encrypted content exchange between distinct entities. This cryptographic technique emerges as a pivotal solution when a party, exemplified by entity A," seeks to unveil the encrypted content to another party, symbolized by entity B," without divulging the closely guarded private key. The strategic application of proxy re-encryption finds utility across diverse scenarios, spanning from secure email communication and law enforcement surveillance to efficient content distribution systems. The mechanism's underlying principle empowers proxies to transform encrypted data in a manner that maintains confidentiality while enabling seamless transfer. When orchestrated, proxy re-encryption augments the versatility and applicability of cryptographic operations. This technique propels secure data sharing without compromising the intricate fabric of cryptographic safeguards. As such, proxy re-encryption stands as a cornerstone in modern cryptographic paradigms, facilitating encrypted data exchange across various domains while upholding the sanctity of privacy and security protocols.

In an innovative endeavor, Zheng et al. [23] unveiled an implementation of PREaaS leveraging the Amazon Elastic Compute Cloud platform. This pioneering system empowers users to forward emails while preserving their anonymity seamlessly. To illustrate, consider a scenario where user A aspires to forward an email to recipient B. The orchestration of this process unfolds through a sequence of intricately coordinated steps. Commencing with user A, the email journey begins with its encrypted transmission to the mail server. At this juncture, the mail server undertakes a pivotal role in generating a re-encryption key, which subsequently assumes a central role in facilitating secure content transfer. The re-encryption key accompanies the encrypted email on its sojourn to the proxy server situated within the cloud infrastructure. In this realm, the proxy server deftly undertakes the task of re-encrypting the email, encapsulating it with an added layer of cryptographic protection. With this enhanced security, the re-encrypted email embarks on its return trajectory to the mail server. The mail server then seamlessly undertakes the responsibility of forwarding the re-encrypted email to the designated recipient B. What distinctly sets this mechanism apart is the covert nature of proxy involvement. Users, such as A and B, remain blissfully unaware of the proxy's presence, effectively shielding its identity from their purview. Notably, a nuanced interplay of cryptographic operations is facilitated within and beyond the cloud layer. This intricate interaction is pivotal in achieving the goals of PREaaS. Notably, the mail server shoulders some of the cryptographic operations, imbuing the platform's architecture with a Half-Cloud configuration. The outcome of this pioneering implementation is a testament to the transformative potential of Proxy Re-Encryption as a Service, bolstering secure and anonymous email forwarding within the contours of modern cloud infrastructures.

Sbai et al. [24] stands as a noteworthy contribution in the realm of Proxy Re-Encryption as a Service (PREaaS), introducing a novel platform tailored for the intricate landscape of smart grid cities. The fundamental objective of this platform is to facilitate secure and encrypted data sharing across diverse entities within these dynamic urban ecosystems. Underpinning this endeavor is the strategic deployment of proxy servers on the cloud, orchestrating the critical re-encryption process. However, what distinguishes this work is the nuanced exploration of different proxy server locations, each yielding distinct implications for efficiency and security. The conceptualization takes shape through three distinctive scenarios, each envisaging the placement of the proxy server at different vantage points within the smart grid city architecture. The first scenario envisions the proxy positioned within the energy side's bank domain. In this arrangement, encrypted data sharing converges at a single focal point, the bank. Yet, this configuration introduces several key management challenges, given the number of parties interacting with this singular entity. Moreover, the single proxy architecture engenders potential delays in data transactions, a concern that demands attention. The second scenario unfolds with the proxy stationed on the network energy manager's side. This scheme endeavors to decentralize key management by enabling each entity to oversee keys within its designated domain. However, this approach invites time-consuming processes, given the intricacies of multiple entities managing keys in tandem. The third and final scenario presents a paradigm shift by situating the proxy within a separate multi-cloud system. This strategic move addresses the challenges posed by the prior scenarios, offering a novel solution to overcome the key management dilemmas and mitigate delays. The distinct advantage lies in decoupling the proxy from any single entity, thus circumventing the pitfalls of centralization and decentralized key management. In essence, the PREaaS platform presented by Sbai et al. [24] symbolizes an astute response to the unique dynamics of smart grid cities. By delving into the intricacies of proxy server placement, this work underscores the profound influence of architecture on key management, latency, and overall system efficiency. Ultimately, this exploration of different proxy server locations exemplifies the innovative spirit driving the evolution of secure data sharing in the context of modern urban ecosystems.

The advancement put forth by Sbai et al. [25] marks a pivotal stride in augmenting the performance of the preceding platform. Central to this enhancement is the strategic incorporation of elliptic curve cryptography, a mathematical construct that yields profound benefits in terms of both security and efficiency. Elliptic curve cryptography is celebrated for its ability to shorten cryptographic keys without compromising their potency, as studies such as [32] affirmed. This pivotal attribute significantly impacts the architecture, ultimately optimizing the platform's performance. The employment of elliptic curves ushers in a twofold advantage, manifesting in the abbreviated length of cryptographic keys and the corresponding reduction in processing time. By leveraging the inherent properties of elliptic curves, Sbai et al. [25] succeeds in crafting a platform that strikes an optimal balance between robust security and operational efficiency. The key length reduction conserves computational resources and contributes to expediting cryptographic operations, culminating in a more streamlined and responsive user experience. Incorporating elliptic curve cryptography in the platform devised by Sbai et al. [25] echoes the synergy between mathematical innovation and practical applicability. This strategic augmentation exemplifies the ongoing pursuit of refining cryptographic paradigms to align with contemporary demands for both security and efficiency. The innovative solution presented by Sbai et al. [33] introduces a PREaaS platform that embodies a novel approach to authentication, prioritizing privacy and security in an interconnected digital landscape. At the core of this concept lies the imperative need to establish user authentication without divulging sensitive credentials to service providers. The architecture of this pioneering platform converges around three primary components: the client, the service provider, and the identity provider, each synergistically contributing to the overarching objective of secure authentication. The platform's dynamics revolve around a strategic interplay between these integral components. Service providers, seeking to uphold the sanctity of user privacy, curate a roster of trusted identity providers. Within this framework, the client is empowered with the autonomy to selectively enroll with any of the pre-approved identity providers, thereby initiating an authentication process devoid of intrusive information sharing. This unique orchestration ensures that users' confidential data remains safeguarded, fostering a heightened sense of trust and privacy assurance in digital interactions. Through this paradigm-shifting PREaaS platform, Sbai et al. [33] encapsulates the evolving ethos of user-centric authentication, mirroring the contemporary imperatives of privacy and security. By circumventing the traditional pitfalls of credential exposure, the platform engenders a transformative narrative where convenience coexists harmoniously with the sanctity of user information, thus charting a course toward a more secure and user-centric digital future.

E. Quantum EaaS (QEaaS)

Quantum cryptography represents a paradigm shift in security mechanisms by harnessing the intricate principles of quantum mechanics for data encryption. In this ingenious approach, the behavior of photons takes center stage as the carriers of information, introducing an inherent capability to detect any unauthorized interception or duplication by a third party. This revolutionary concept stems from the fundamental principle that the state of photons undergoes alteration upon interaction, effectively rendering any unauthorized reading or copying conspicuously detectable. Within the realm of quantum cryptography, the transformative potential is not confined to its security attributes alone; it also paves the way for the emergence of a Quantum Encryption as a Service (QEaaS) platform, as elucidated by Olanrewaju et al. [34]. The underpinning premise of such a platform lies in the exploitation of quantum properties to offer a distinctive form of data protection as a service. The foundation of this notion rests upon the dynamic behavior of photons, which serve as carriers of cryptographic significance, ultimately driving the mechanism that facilitates encryption within the quantum domain. As quantum mechanics and cryptography fields converge, quantum cryptography presents an unprecedented avenue for safeguarding information exchange. By transcending classical encryption paradigms and harnessing the unique attributes of quantum states, QEaaS emerges as an innovative frontier in data protection, poised to revolutionize security paradigms in the digital age.

The advent of quantum cryptography has paved the way for transformative innovations in safeguarding critical communications, as evidenced by the pioneering work of Ralegankar et al. [26]. This trailblazing effort introduces Quantum Encryption as a Service (QEaaS) as a groundbreaking solution to secure communication between Unmanned Aerial Vehicles (UAVs). At the heart of this endeavor lies a meticulously designed five-layer architecture, each layer contributing a distinct facet to the comprehensive protection of UAV communications. The foundational layer of this architecture, aptly named the monitoring layer, assumes the crucial task of capturing data from the surrounding environment and requested locations. Above this, the physical layer, akin to the device layer in conventional cryptographic definitions, plays host to the UAVs themselves. In this layer, UAVs transmit their sensitive data to the succeeding stratum. The third layer, the quantum security layer, emerges as the nucleus of the QEaaS platform. Within this domain, data transforms unparalleled sophistication, transmuted into quantum states represented by photons. This quantum encryption process confers a formidable layer of security, ensuring that data remains impervious to unauthorized access or interception. Once encrypted, the quantum data is propelled into the fourth layer—the Internet layer—where cutting-edge

5G networks usher the quantum-encrypted information across geographically diverse regions. Ultimately, the voyage of the quantum-encrypted data culminates in the central control layer, the fifth and final stratum of the architecture. Here, the data finds its resting place, secure and impregnable, solidifying the overarching aim of safeguarded UAV communications. The multi-layered architecture thus embodies a harmonious interplay of quantum principles and sophisticated networking infrastructure, promising an unparalleled realm of secure data exchange for Unmanned Aerial Vehicles. In this visionary synthesis of quantum mechanics, cryptography, and UAV technology, Ralegankar et al. [26] ushers in an era of enhanced security and trust for UAV communications through the lens of Quantum Encryption as a Service.

The landscape of quantum cryptography's practical implementation takes a substantial leap forward with the pioneering work of Raddo et al. [27], who introduced a groundbreaking testbed for deploying QEaaS. Rooted in the realm of beyond 5G networks, this innovative platform heralds a new era of quantum-secure communication by offering a tangible environment for real-world exploration and validation. Central to this visionary testbed is a pivotal Functional Node (FN) that dons the mantle of traffic classification and slice orchestration. As the nucleus of the QEaaS ecosystem, the FN performs the pivotal task of identifying and classifying various traffic types, thus enabling the strategic orchestration of network slices tailored to distinct communication requirements. This orchestration, facilitated by the FN, ensures the seamless coexistence and optimal allocation of resources across diverse QEaaS applications. Immersed in the cutting-edge realm of beyond 5G networks, the QEaaS testbed introduces a novel paradigm that embraces quantum cryptography's unique challenges and opportunities. Through the ingenious orchestration prowess of the FN and the utilization of advanced networking technologies, Raddo et al. [27] extends an invitation to researchers, practitioners, and enthusiasts to explore, experiment, and validate the transformative potential of QEaaS in a tangible, real-world setting.

F. General EaaS (GEaaS)

The other types of EaaS, which use a general encryption technique, are reviewed in this section.

In a seminal contribution to the field, Rahmani et al. [28] laid the foundation for Encryption as a Service (EaaS) platforms by presenting one of the earliest instances of this transformative paradigm. At the heart of this pioneering work lies a groundbreaking platform that underscores the feasibility of implementing EaaS and unveils its potential to revolutionize data security. With the primary objective of showcasing the practical viability of EaaS, Rahmani et al. [28] ventured into uncharted territory, recognizing the burgeoning need for secure data handling in an increasingly digital landscape. A central hallmark of this platform's innovation lies in its integration of general-type encryption, a crucial step that sets the stage for a wide range of applications across industries and domains. Not content with mere feasibility, the architects of this platform endeavored to optimize its performance by harnessing the power of parallelism. By employing multiple threads spread across multiple virtual machines, they orchestrated an orchestral symphony of computation, drastically reducing service times and enhancing overall efficiency. At the heart of this orchestration lies a guided scheduling algorithm, a sophisticated approach that deftly manages the intricate dance of threads, further enhancing the platform's responsiveness and robustness. In retrospect, Rahmani et al. [28]'s groundbreaking work is a testament to the visionary spirit that drives technological advancement. By planting the seeds of EaaS and nurturing them with innovative techniques such as parallelism and guided scheduling, this seminal research provided the foundational framework upon which subsequent EaaS platforms have been built, forever transforming the landscape of data security and encryption.

Kang et al. [29] presents yet another significant stride in the realm of EaaS with a versatile and user-centric platform that empowers users to tailor their data security according to their specific needs. Central to this innovation is integrating a selection mechanism that allows users to choose from various encryption configurations, each designed to accommodate varying levels of security requirements. Diving deeper, this platform encapsulates the essence of user empowerment by offering a menu of encryption options. Symmetric algorithms, including the formidable AES and the venerable Blowfish, form the backbone of this robust system, reflecting the meticulous consideration given to selecting well-established encryption methods that ensure data integrity and confidentiality. Moreover, Kang et al. [29] highlights the recognition that one size does not fit all regarding security. In a nod to the diverse nature of information and the distinct threat landscapes that various users face, the platform facilitates the customization of encryption strength. This is achieved by provisioning key lengths spanning 128, 192, and 256 bits, enabling users to match their encryption potency to their data's sensitivity and the circumstances' exigency. By offering this versatile platform that lets users easily navigate the intricate terrain of data security, Kang et al. [29] continues the trajectory of EaaS evolution. This dynamic and user-tailored approach embodies a commitment to providing robust encryption and underscores the platform's adaptability to the ever-evolving challenges of the digital realm.

The pioneering work of Vu et al. [30] introduces a novel dimension to the EaaS landscape with a groundbreaking General Encryption as a Service (GEaaS) platform. At the heart of this innovation lies a fundamental shift towards empowering users to dictate access policies, thereby endowing them with unprecedented control over the parties authorized to access their unencrypted data. Intriguingly, Vu et al. [30] goes beyond the conventional confines of encryption by enabling users to wield the power of virtual machines within a cloud-based environment. This virtuosity allows users to orchestrate and oversee the intricacies of cryptographic processes, reflecting a seamless fusion of user-driven data protection and cutting-edge cloud technology. Central to the architecture of this platform is the notion of access policies, affording users the privilege of setting boundaries on data accessibility. This transformative feature translates to the user's ability to shape and define the precise audience permitted to engage with their plaintext data. In doing so, the platform emerges as a bastion of individualized control and customized security, effectively eradicating the one-size-fits-all approach to data protection. The introduction of virtual machines within the cloud framework marks a paradigm shift that empowers users to manage encryption operations with unprecedented dexterity. This dynamic convergence of cloud computing and cryptographic prowess ensures that users are not just passive beneficiaries of security measures, but active architects of their data's protection. Through this pioneering platform, Vu et al. [30] redefines EaaS and revolutionizes the relationship between users and their encrypted data. By placing the reins of data protection squarely in the hands of users, and by leveraging the capabilities of cloud-based virtual machines, this work heralds a new era of user-centric security that is as versatile as it is powerful.

The paradigm-shifting realm of General Encryption as a Service (GEaaS) is further advanced by Zhang et al. [13], who proposes a novel GEaaS platform characterized by a sophisticated three-layer architecture. This groundbreaking platform is fortified by the ingenious MX-SORTS algorithm, a cornerstone in enforcing an optimal security strategy across diverse domains. The core of this innovation lies in the MX-SORTS algorithm's profound ability to navigate the intricate balance between security enhancement and real-time performance. To elucidate, the MX-SORTS algorithm undertakes the formidable task of optimizing security gains while simultaneously ensuring that network delays remain well below a designated threshold. A striking hallmark of this approach is the elegant adoption and customization of the classic knapsack algorithm. The crux of the MX-SORTS algorithm revolves around the ingenious model of item collection, where the weight of each item symbolizes ”delay” and the value represents ”security.” This pivotal conceptualization effectively transforms the complex trade-off between security and real-time performance into a computationally tractable challenge. At the heart of the three-layer architecture lies an intricate interplay of elements that underpin the GEaaS platform's functionality. By seamlessly integrating the MX-SORTS algorithm into this architectural tapestry, Zhang et al. [13] pioneers an approach that transcends traditional encryption paradigms. The strategic deployment of MX-SORTS not only introduces a dynamic equilibrium between security and performance but also ushers in a new era of nuanced encryption strategies that cater to the specific demands of each domain. In essence, the work of Zhang et al. [13] propels the GEaaS concept beyond mere data protection into strategic security orchestration. By ingeniously tailoring the MX-SORTS algorithm and its knapsack-inspired foundation, this research lays the groundwork for a future where security is no longer a static entity but a dynamic and adaptive force that responds quickly to evolving demands and challenges.

Delving deeper into the realm of Encryption as a Service (EaaS), Yang et al. [10] presents a groundbreaking implementation tailored specifically for Kubernetes, a prominent cloud-based container orchestration platform renowned for its dynamic scalability and efficient resource allocation [35, 36]. This innovative proposal harnesses the power of Kubernetes to seamlessly integrate encryption processes, demonstrating a remarkable fusion of modern containerization principles with robust data security practices. At the heart of this cutting-edge approach lies the strategic deployment of a proxy server, discreetly nestled within each pod—a fundamental unit within the Kubernetes framework, housing multiple interconnected containers. The role of this proxy server is nothing short of transformative: it diligently encrypts the incoming traffic originating from within the pod, while adroitly decrypting external traffic directed towards the pod. This proxy-based encryption mechanism serves as a sentinel, tirelessly safeguarding data integrity within the Kubernetes ecosystem's dynamic and often ephemeral confines. The symbiotic relationship between Kubernetes and EaaS is unmistakable. By seamlessly integrating encryption capabilities at the pod level, Yang et al. [10] presents a paradigm shift that aligns with the core tenets of containerization—namely, isolation and resource efficiency. Data encryption becomes an integral aspect of Kubernetes ' containerized landscape by strategically placing proxy servers within each pod. This inventive endeavor not only underscores the potent synergy between cutting-edge cloud-native technologies and robust data security practices but also exemplifies the dynamic evolution of encryption paradigms within the ever-evolving realm of container orchestration. As Yang et al. [10] bridges the worlds of Kubernetes and encryption, a new chapter is written in the narrative of secure and resilient cloud-based ecosystems. This work is a testament to the proactive endeavors that redefine data protection, adapting it to modern cloud infrastructures and architectural philosophies.

Ateeq et al. [31] proposed an EaaS platform for multi-cloud environments. In this platform, a central agent manages the encryption configuration for different cloud providers. After receiving the data from a user, the central agent divides it into multiple fragments. Each fragment is then encrypted with different encryption configurations to be uploaded to each cloud environment.

G. *A summary of the reviewed research based on EaaS types*

The provided references are in Table Table III. Outline various encryption services tailored for specific architectures and applications. ABEaaS (Attribute-Based Encryption as a Service) focuses on generating an intermediate ciphertext based on data attributes optimized for the dynamic environment of a Half-Cloud Mobile Cloud. HEaaS (Homomorphic Encryption as a Service) offers homomorphic encryption designed explicitly for secure healthcare systems within Full-Cloud architecture. SEaaS (Searchable Encryption as a Service) addresses accurate searching within encrypted data, ideal for the context of Half-Cloud Public Clouds. PREaaS (Proxy Re-encryption as a Service) enhances email security through re-encryption proxies, which is significant for secure communication in Half-Cloud Smart grid cities. These services showcase encryption strategies' diverse applications and adaptability in evolving technological landscapes. ABEaaS (Attribute-Based Encryption as a Service): ABEaaS is an innovative cryptographic service that emphasizes generating an intermediate ciphertext based on specific attributes associated with the data being encrypted. Attribute-based encryption (ABE) is a versatile encryption technique that allows access to data based on defined attributes, ensuring that only users with the appropriate attributes or credentials can decrypt and access the data. In the specified architecture of Half-Cloud Mobile cloud, ABEaaS becomes particularly relevant as it caters to the dynamic and mobile nature of data access. Mobile devices frequently connect to cloud services for data processing and storage. By tailoring encryption based on attributes such as user roles, access levels, or other defining features, ABEaaS provides a flexible and secure data access mechanism. It's highly beneficial for scenarios where data security, access control, and mobility are paramount concerns.

- HEaaS (Homomorphic Encryption as a Service): HEaaS is an encryption service that focuses on providing homomorphic encryption capabilities. Homomorphic encryption allows computations to be performed on encrypted data without decrypting it. This is a critical feature, especially in domains like healthcare systems where sensitive data privacy and security are paramount. For instance, in a Full-Cloud architecture, HEaaS encrypts images using homomorphic algorithms, ensuring that computations such as image processing, analytics, or diagnostics can be conducted even while encrypted. By preserving data confidentiality throughout these operations, HEaaS significantly contributes to maintaining the privacy and integrity of sensitive medical information. Its applications extend to any domain where secure processing of encrypted data is essential.

- SEaaS (Searchable Encryption as a Service): SEaaS addresses the challenge of searching within encrypted data. Searchable Encryption allows users to search over encrypted data without revealing any information about the data itself. In the context of Half-Cloud Public clouds, where data privacy and efficient search functionalities are paramount, SEaaS shines. The service considers typographical errors during the search process, enhancing the accuracy and reliability of the search results. By utilizing multiple threads to handle the search process, SEaaS optimizes the search efficiency, enabling faster and more precise searches. This is particularly useful in scenarios where data confidentiality is critical, and precise yet swift data retrieval is a requirement.

- PREaaS (Proxy Re-encryption as a Service): PREaaS facilitates the forwarding of emails with an additional layer of security through anonymous re-encryption proxies. In the context of Half-Cloud Smart grid cities, where secure communication is necessary, PREaaS plays a vital role. Using anonymous re-encryption proxies ensures that emails can be relayed securely while preserving the anonymity and privacy of the sender and receiver. Moreover, integrating PREaaS into a Full-Cloud architecture within smart grid cities, with the proxy located on a multi-cloud system, enhances the efficiency of re-encrypting operations, contributing to robust communication security within the smart grid infrastructure. It's an indispensable service for enhancing secure communication within modern urban infrastructures.

V. EaaS Service Types

Within the expansive realm of Encryption as a Service (EaaS), a diverse array of cryptography services emerges, each catering to distinct security needs and operational contexts. An EaaS platform offers the flexibility to offer one or more cryptography services, tailored to the users' specific requirements. These services encompass a spectrum of functionalities, incorporating data protection and mechanisms for access control, key management, and digital signatures, collectively shaping a robust cryptographic landscape within the EaaS paradigm.

- Secure Storage and Data Protection Services: EaaS platforms extend their protective mantle to encompass secure storage solutions. These services empower users to safeguard their sensitive data within encrypted vaults, ensuring that confidential information remains invulnerable to unauthorized access. By employing encryption, these platforms fortify data privacy, enabling users to entrust their valuable assets to the cloud or fog layers without compromising on security.
- Access Control Services: An integral facet of EaaS service offerings is the domain of access control. These services wield encryption as a tool to enforce granular access policies, granting specific privileges to authorized parties and mitigating the risk of data breaches. Through cryptographic means, users can exercise fine-grained control over who can access their encrypted resources, thus preserving confidentiality even in shared environments.
- Key Management Services: The intricate orchestration of cryptographic keys lies at the core of secure communication and data protection. EaaS platforms rise to this challenge by offering key management services, facilitating the generation, distribution, rotation, and revocation of encryption keys. These services ensure that the cryptographic foundations remain robust, supporting seamless encryption and decryption operations across the diverse layers of the platform.
- Digital Signature Services: In digital transactions and authentication, the assurance of data integrity and origin authenticity is paramount. EaaS platforms amplify their utility by furnishing digital signature services. By employing cryptographic techniques, these services enable users to append digital signatures to their data, validating its origin and ensuring it remains unaltered during transit.
- The versatility of EaaS service types underscores the platform's adaptability to diverse security demands, unveiling a multifaceted ecosystem where cryptography seamlessly intertwines with cloud, fog, and device layers. These services empower users to confidently navigate the intricate landscape of data protection, harnessing the power of encryption to forge secure pathways within the expansive digital realm. As EaaS continues to evolve, its service types stand as a testament to its capacity to align cryptographic practices with the nuanced intricacies of modern data security challenges. A summary of the research, categorized based on their offered service type, is presented in Table IV.

A. *Secure Storage as a Service (SSaaS)*

Secure Storage as a Service (SSaaS) is a cornerstone of Encryption as a Service (EaaS), addressing the need for

TABLE IV
A SUMMARY OF THE REVIEWED RESEARCHES BASED ON THEIR OFFERED ENCRYPTION SERVICE TYPES.

Reference	Service Type	Short Description
Bedi et al. [37]	SSaaS	Storing data on multiple cloud servers and utilizing the fog layer to handle middle processes.
Sahbudin et al. [38]		A web client that fragments data to be stored on multiple storage servers.
Ahsan et al. [39]		Improving stored data confidentiality and integrity by generating data blocks.
Chinnasamy and Deepalakshmi [40]	ACaaS	Reducing the authorization load on the storage server.
Zhang et al. [41]		Offloading the access control operations on the fog layer.
Meshram et al. [42]		Creating access rules based on the users attributes.
Kumar et al. [43]		Using blockchain to guarantee the immutability of the access request transactions.
Ahmad et al. [44]		A platform for IoT environments that leverages their current management mechanisms.
Taurshia et al. [45]	KMaaS	Providing group key management as a service.
Qiu et al. [46]		Using blockchain to reduce resource consumption of key management processes.
Cao et al. [47]		A key management platform for quantum cryptography.
Cao et al. [48]		A key management platform for quantum cryptography using software-defined networks.
Kalyankar and Kumar [49]	DSaaS	Providing digital signature generation and verification as a service.
Sun et al. [50]		A quantum-based digital signature platform.

safeguarding sensitive data within cloud or fog layers. Users entrust their data to SSaaS, which employs advanced encryption techniques to transform it into ciphertext, ensuring confidentiality and integrity. The encrypted data is securely stored within the SSaaS platform, shielded from unauthorized access. When retrieval is required, stringent authentication processes ensure authorized access, offering a seamless user experience abstracted from the complexities of encryption. SSaaS combines robust data protection with user-friendly interaction, providing a secure haven for data within the cloud or fog, enabling users to harness cloud capabilities while upholding data sanctity in the face of evolving privacy concerns.

In the multi-cloud Secure Storage as a Service (SSaaS) architecture proposed by Bedi et al. [37], the aim is to provide a robust and scalable solution for secure data storage that leverages both cloud and fog computing resources. This platform operates through a collaborative interaction between the cloud and fog layers. In this setup, the storage server, responsible for holding the encrypted data, is located within the cloud layer. On the other hand, the fog layer serves as an intermediary between end-devices and the cloud storage server. When an end-device wishes to store data securely, it sends it to the fog layer, which acts as a processing node. The fog layer performs essential tasks such as data preprocessing, encryption (if not done by the end-device), and data forwarding to the appropriate cloud storage server. To optimize performance and resource utilization, the fog layer employs load-balancing mechanisms. Data is intelligently divided among various cloud storage servers, ensuring no single server becomes a bottleneck and maximizing the overall system efficiency. This distribution strategy helps in managing high loads and mitigating potential latency issues. When data retrieval is requested, the fog layer enforces access control and authentication checks. Prior to granting access to stored data, the fog layer verifies the user's authorization, ensuring that only legitimate users are permitted to access the decrypted content. By coherently integrating cloud and fog layers, this multi-cloud SSaaS platform demonstrates an innovative approach to secure data storage that addresses scalability, efficiency, and security concerns. The architecture harnesses the strengths of both cloud and fog computing paradigms, resulting in an adaptable and resilient solution for modern data storage requirements.

A web client application is proposed by Sahbudin et al. [38]. It allows users to store their data on multiple cloud storage services like DropBox, OpenStack, and Google Drive. When a file is uploaded to this application, a fragmented encrypted file will be generated, as well as a JSON file that helps in retrieving the fragments. Now, each fragment can be stored on different storage service providers, which cannot be decrypted separately.

Indeed, the research presented by Ahsan et al. [39] introduces valuable enhancements to the security aspects of data stored on Secure Storage as a Service (SSaaS) platforms. This work is centered around addressing data confidentiality and integrity concerns, two pivotal aspects of ensuring the safety of outsourced data. The proposed approach employs the Xor-Combination technique to tackle the data confidentiality challenge. This technique involves dividing the data into multiple distinct blocks. A significant feature of Xor-Combination is that any combination of two or three blocks does not lead to the retrieval of an original data block. This characteristic enhances data confidentiality, making it exceedingly difficult for an unauthorized entity to piece together meaningful information from the divided blocks, thereby augmenting the overall security of the outsourced data. On the other hand, the research also addresses the crucial issue of data integrity using the Collision Resisting Hashing technique. This technique focuses on minimizing the occurrence of collisions within the utilized hash function. In this context, collisions refer to instances where two distinct sets of data produce the same hash value. By reducing such occurrences, the technique enhances the system's ability to detect unauthorized modifications to the stored data. Any change to the data will likely result in a different hash value, thus triggering an alert that indicates potential tampering or unauthorized alterations. In summary, Ahsan et al. [39] introduces a comprehensive approach that effectively improves both the confidentiality and integrity of data stored on SSaaS platforms. By combining Xor-Combination and Collision Resisting Hashing techniques, the research contributes valuable insights to secure data storage, ultimately bolstering the protection and trustworthiness of outsourced data in cloud environments.

B. Access Control as a Service (ACaaS)

Access Control as a Service (ACaaS) plays a pivotal role in ensuring the secure sharing of data stored on cloud or fog servers. While securely storing data is essential, controlling and managing who can access that data is equally crucial. ACaaS platforms are designed to facilitate the process of granting or denying access to shared data based on predefined identities and permissions set by the data owner. When a user requests access to specific data, the ACaaS platform initiates a series of steps to determine whether the request should be granted. This process involves querying a relevant database that contains information about the authorized identities and their associated permissions. The platform evaluates the request against this information to ascertain whether the user has the necessary authorization to access the requested data. Upon making a decision, the ACaaS platform generates a response, either allowing or denying access to the data, depending on the outcome of the evaluation. In essence, ACaaS offers a comprehensive solution for managing and enforcing access rights to shared data, ensuring that only authorized individuals or entities can interact with the data. ACaaS platforms contribute significantly to data security, privacy, and proper data management in cloud and fog environments by centralizing access control processes and automating decision-making based on predefined rules and permissions.

In the ACaaS platform proposed by Chinnasamy and Deepalakshmi [40], the key innovation lies in delegating access control responsibilities from storage servers to a dedicated ACaaS server. The data owner initiates the process by authenticating and submitting an access list to the ACaaS server. This server then generates a unique security label and associates it with both the data owner and the authorized access list. Subsequently, when the data owner uploads their data to the storage server, it includes the security label. When a third-party user wishes to access the data, the storage server issues a security label and a corresponding token. These credentials are sent to the ACaaS server, which verifies the access request against the data owner's access list. If the request aligns with the defined permissions, the token is signed by the ACaaS server, confirming the user's authorized access. The storage server then grants access only to users possessing a signed token. This approach offloads much of the access control processing from the storage server, streamlining its operations and enhancing security. On a related note, Zhang et al. [41] introduced a solution that harnesses Fog Nodes (FNs) to manage access control operations. This strategy alleviates the complexity associated with updating attributes used to define authorized users. By shifting access control management to FNs, the platform simplifies the process of maintaining and adjusting access permissions, making it more efficient and responsive to changes. Both of these ACaaS platforms represent significant advancements in access control mechanisms for cloud and fog environments. They offer solutions to streamline access authorization, enhance security, and distribute the computational load, ultimately contributing to improved data management and sharing practices in these contexts.

In the ACaaS platform introduced by Meshram et al. [42], the emphasis is placed on leveraging user attributes to govern access to resources. This approach enables a more dynamic and personalized access control mechanism. Data owners or organizations define access lists by specifying attributes, their corresponding values, and the rules that dictate access based on these attributes. This allows for fine-grained access control, where users with specific attributes can access resources according to predefined rules. For example, an organization might set up rules that grant access to specific files only to users with a certain job role or department affiliation. By incorporating attribute-based access control, this platform offers greater flexibility than traditional access control models relying solely on roles or groups. It enables a more context-aware and adaptable data-sharing approach, accommodating complex access scenarios involving multiple attributes. The platform's architecture typically involves an attribute management component, an access policy engine, and a mechanism for evaluating access requests based on attributes. Blockchain-Enhanced ACaaS Platform by [43]: Building upon the concept of attribute-based access control, Kumar et al. [43] introduces a blockchain-enhanced ACaaS platform. The integration of blockchain technology adds an extra layer of security, transparency, and tamper resistance to the access control process. When data owners make changes to the access lists or policies, the corresponding transactions are recorded on the blockchain. This ledger of access control changes provides an immutable and auditable record of access-related activities. The use of blockchain addresses the challenge of maintaining the integrity and transparency of access control decisions. Changes to access control policies become transparent and traceable, minimizing the risk of unauthorized modifications. This platform's architecture includes components for blockchain integration, attribute management, access policy definition, and transaction recording. Both of these ACaaS platforms introduce innovative approaches to access control by focusing on user attributes and utilizing advanced technologies like blockchain. These advancements contribute to more dynamic, flexible, and secure access control mechanisms that align with the evolving requirements of data sharing and security in modern digital environments.

The solution presented by Ahmad et al. [44] addresses the access control challenges within Internet of Things (IoT) environments. In IoT scenarios, managing access to devices and data becomes complex due to the vast number of interconnected devices with varying capabilities and roles. The proposed solution offers a way to outsource the access control process while integrating seamlessly with the existing IoT environment's policy enforcement and evaluation mechanisms. Rather than replacing the IoT environment's access control mechanisms, the solution acts as an Access Control as a Service (ACaaS) platform that complements the IoT ecosystem. It provides the capability to manage access control policies and specifications externally while allowing the IoT environment to retain control over policy enforcement and evaluation. This approach maintains the coherence of the IoT environment's existing policies while benefiting from the flexibility and centralized management offered by the ACaaS model. By enabling the IoT environment to interact with the ACaaS platform, organizations can streamline access control management across their diverse network of devices. This solution aims to simplify the complexity of managing access rights in IoT environments, ensuring that devices and data are accessed only by authorized parties while preserving the integrity of the IoT ecosystem's existing access control infrastructure.

C. Key Management as a Service (KMaS)

Key Management as a Service (KMaaS) addresses the crucial aspect of cryptography by focusing on the generation, distribution, and management of encryption keys securely and efficiently. In scenarios where an end-user requires cryptographic protection but seeks to offload the complexities of key management, KMaaS becomes invaluable. This service is especially pertinent in multi-provider environments where an end-user employs multiple secure storage service providers, some of which might not be fully trusted. The KMaaS platform is responsible for generating and safeguarding encryption keys, ensuring their proper distribution, and maintaining their security throughout their lifecycle. This allows end-users to securely store their data across various providers without worrying about the intricacies of key management. KMaaS simplifies the user's experience and enhances the overall security posture by centralizing and professionalizing the key management process. KMaaS plays a critical role in facilitating secure and interoperable data sharing within complex cloud environments by decoupling key management from data storage and encryption.

In the context of key management as a service (KMaaS), Taurshia et al. [45] presents a robust platform that focuses on the unique challenges of managing encryption keys within group scenarios. In collaborative environments where multiple entities need access to shared data, ensuring secure key distribution and management becomes paramount. The platform employs advanced techniques such as Logical Key Hierarchy and One-way Function Trees to manage encryption keys for different groups efficiently. Logical Key Hierarchy allows for a structured approach to managing keys based on group hierarchies, while One-way Function Trees offer a scalable method for key derivation and distribution. On a similar note, Qiu et al. [46] introduces a KMaaS platform that leverages blockchain technology to enhance key management processes, particularly in situations involving untrusted cloud providers. Cloud-based environments can involve many users and data-sharing activities, which can strain the key management infrastructure. By integrating blockchain, this platform offers a decentralized and tamper-resistant solution to manage encryption keys effectively. Blockchain's inherent properties of immutability and distributed consensus provide a reliable foundation for secure key management, ultimately leading to resource-efficient and trustworthy data sharing among users. Both of these KMaaS platforms address key management challenges in distinct ways, catering to the needs of secure group communication and efficient key distribution within cloud-based ecosystems.

In the realm of key management as a service (KMaaS), Cao et al. [47] introduces an innovative platform that harnesses the principles of quantum mechanics for enhanced security. The platform operates by virtualizing the secret keys belonging to end-nodes into a centralized pool hosted on the KMaaS server. This virtualization allows for efficient key management and distribution. When two communicating nodes require a secret key, a portion of these keys is allocated to them from the virtualized pool. By utilizing quantum-inspired concepts, this platform enhances the security of key management processes dynamically and efficiently. Similarly, Cao et al. [48] presents a KMaaS platform that draws inspiration from quantum principles, but adds the dimension of software-defined networking (SDN) for managing the intricacies associated with multiple users. This platform leverages the power of SDN to address challenges arising from the complex interactions between users and services. By integrating quantum concepts with SDN capabilities, the platform aims to provide an effective and scalable solution for key management, ensuring secure and streamlined communication within dynamic network environments. Both of these KMaaS platforms showcase innovative approaches to key management by incorporating quantum mechanics and network management techniques to enhance security, efficiency, and adaptability in cloud-based communication scenarios.

D. Digital Signature as a Service (DSaaS)

A digital signature is a way of verifying the integrity and authenticity of data. In other words, in the case that the secret keys are not leaked, if a piece of data is received from A, and it has a digital signature, the receiver is sure that (1) the data is definitely sent from A, and (2) the data is not illegally modified by some party other than A. The digital signature can be generated and verified by a cloud provider as a Digital Signature as a Service (DSaaS). When data is signed using a digital signature, it is uniquely associated with the signer's identity and cannot be tampered with without invalidating the signature. This gives recipients confidence that the data originated from the claimed sender and has not been altered by unauthorized parties. In the context of DSaaS, cloud providers offer the computational resources and cryptographic algorithms necessary for generating and verifying digital signatures. This service offloads the complexity of cryptographic operations from the clients, allowing them to focus on their core tasks without needing to implement the intricacies of digital signature generation and verification. Cloud-based DSaaS platforms typically follow standardized cryptographic algorithms and protocols to ensure interoperability and security. DSaaS platforms offer several benefits, including ease of use, scalability, and potential cost savings. Users can leverage the service without needing specialized hardware or deep cryptographic expertise. The cloud infrastructure enables efficient processing of signature operations, making it suitable for applications that require many signatures, such as financial transactions, software updates, and legal contracts. Additionally, the cloud's elastic nature ensures that the service can scale up or down based on demand. Overall, DSaaS simplifies the implementation of secure digital signature mechanisms, making it a valuable tool for organizations and individuals seeking to enhance the security and trustworthiness of their digital communications and transactions.

In the DSaaS platform proposed by Kalyankar and Kumar [49], the focus is on both user authentication and data integrity through digital signatures. Users are provided with a one-time password (OTP) to securely access services. Once authenticated, users can generate digital signatures for their desired messages using their identity. This process ensures the origin and integrity of the data being signed, enhancing overall security. In the case of Sun et al. [50], the DSaaS platform adopts quantum-based signatures for improved security. Quantum signatures leverage the principles of quantum mechanics to provide enhanced protection against various cryptographic attacks. To optimize the signing process, the platform takes advantage of multi-core processors, allowing for parallel signing operations processing. This approach significantly improves the speed of generating digital signatures while maintaining the desired level of security.

VI. EaaS Testbeds

In the realm of EaaS, various testbeds, commercial platforms, and open-source solutions have been developed to showcase the feasibility of EaaS architectures and provide practical platforms for researchers and developers. These platforms help validate the concepts, evaluate performance, and experiment with different cryptographic services and configurations. Let's explore some of these testbeds and platforms:

- Testbeds: EaaS Testbed by Rahmani et al. [28]: This early EaaS testbed was developed to demonstrate the feasibility of providing cryptography services as a cloud service. It allowed researchers to experiment with parallelism and thread scheduling for encryption and decryption processes. Multi-Cloud SSaaS Testbed by Bedi et al. [37]: This testbed focuses on secure storage as a service (SSaaS) in multi-cloud and fog environments. It showcases load balancing and data distribution techniques in a practical setting.
- Commercial Platforms: Amazon Web Services (AWS) offers various cryptographic services, including encryption, key management, and digital signatures. These services can be integrated into applications to provide robust security mechanisms. Microsoft Azure: Azure provides a range of security services, such as encryption and key management, that can be used to implement EaaS solutions. Azure's cloud infrastructure can be leveraged to deploy cryptographic services as needed.
- Open-Source Platforms: OpenStack: OpenStack is an open-source cloud computing platform that can be used to deploy EaaS solutions. Researchers and developers can customize and configure cryptographic services based on their requirements.
- Kubernetes: Kubernetes is an open-source container orchestration platform. Yang et al. [10] proposed an EaaS platform for Kubernetes, demonstrating the integration of encryption processes within pods for secure communication.
- Hyperledger Fabric: Hyperledger Fabric is an open-source blockchain framework that can be adapted to implement secure and auditable key management services in EaaS platforms.
- OpenSSL: OpenSSL is an open-source toolkit for implementing the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols. It can be used to build custom EaaS solutions with encryption and digital signature capabilities. These testbeds, commercial platforms, and open-source solutions collectively contribute to the development and advancement of EaaS technologies. They provide a practical environment for researchers and developers to explore different architectural designs, encryption algorithms, key management techniques, and security mechanisms. As the field of EaaS continues to evolve, these platforms will play a vital role in validating concepts and accelerating innovation in secure data processing and transmission.

Zhang et al. [13] implemented the EaaS platform for smart substations using their local servers (i.e., a common cloud or fog platform is not used). They used Allen-Bradly programmable logic controllers as the intelligent electronic devices in the device layer. The workstations and the remote terminal units, which are assumed to be located on the fog layer, are quad-core Lenovo desktop computers. The edge devices that support the communication between the device and fog layers are Raspberry Pi devices with Ubuntu 16.04 LTS. CNs are also Inspur servers with Ubuntu 16.04 LTS. The communication between the device and fog layers is based on the IEC 61850 standard.

In their implementation, Deb et al. [12] utilized three types of end-devices to showcase the versatility of their EaaS platform. The first type consisted of NodeMCUs, which are compact microcontroller units based on the ESP8266 chipset. These devices are commonly used in Internet of Things (IoT) applications due to their low-cost and limited resource capabilities, making them suitable for scenarios with constrained devices [51]. The second type of end-device used was the Raspberry Pi, a popular single-board computer with Linux-based operating systems. The Raspberry Pi devices were chosen for their versatility and moderate computing power, which allowed them to serve as both end-devices and Fog Nodes (FNs) in the architecture. This flexibility demonstrated how more capable devices can perform both local processing and act as intermediaries for cryptographic operations. Lastly, Dell Inspiron 15 workstations equipped with i5 core processors were employed as more powerful end-devices and FNs. These workstations showcased the ability of the EaaS platform to accommodate devices with higher processing capabilities and resources, highlighting the platform's scalability to different hardware specifications. By incorporating these diverse end-device types, Deb et al. [12] showcased the adaptability of their EaaS platform to various device constraints and resource levels, making it a comprehensive solution for cryptography services across a wide spectrum of devices.

These three studies utilized OpenStack, an open-source cloud computing infrastructure, as the foundation for implementing their proposed platforms. OpenStack is known for its flexibility, scalability, and modular architecture, making it suitable for building cloud-based services. The platforms leveraged specific modules within OpenStack to achieve their cryptographic goals. The Keystone module in OpenStack was used by El Bouchti et al. [17], Zibouh et al. [19], and Sahbudin et al. [38] to provide identity and authentication services. This module enables user authentication and access control, ensuring that only authorized users can access the cryptographic services offered by the platforms. The Swift module, which provides object storage services, was another key component employed by these studies. El Bouchti et al. [17] and Zibouh et al. [19] utilized Swift to store encrypted data securely on the cloud. This module allows the platforms to manage data storage efficiently while maintaining data confidentiality and integrity. Additionally, Sahbudin et al. [38] used Swift to store fragmented encrypted files and associated metadata, showcasing the platform's capability to manage secure data storage across different cloud storage providers. By utilizing OpenStack and its relevant modules, these studies were able to implement cloud-based cryptographic platforms that leverage the infrastructure and services provided by OpenStack, demonstrating the feasibility and practicality of their proposed architectures.

Yang et al. [10] chose Kubernetes, a popular open-source container orchestration platform, as the foundation for their proposed EaaS platform. Kubernetes provides features for automating the deployment, scaling, and management of containerized applications, making it suitable for building scalable and manageable cloud-based services. In their implementation, Yang et al. [10] deployed a microservice-based Elasticsearch service on a Kubernetes cluster. The Elasticsearch service is divided into multiple pods for scalability, with three pods used out of a total of six in the cluster. These pods generate data that needs to be encrypted before transmission. The main proxy used in the platform to provide the encryption service is HAProxy. HAProxy is a widely used load balancer and proxy server that can be employed to handle various aspects of network traffic, including encryption and decryption. In the context of Yang et al. [10]'s platform, HAProxy is responsible for encrypting and decrypting the data transmitted between the pods and other components. The integration of the HAProxy container into the Elasticsearch pods is facilitated by using Kubernetes MutatingAdmissionWebhook. This webhook mechanism allows for the automatic injection of the HAProxy container into the Elasticsearch pods during deployment or scaling operations. This integration ensures that the encryption service is seamlessly applied to the data transmitted within the Kubernetes environment. By utilizing Kubernetes, microservices, and HAProxy, Yang et al. [10] demonstrated the feasibility of their EaaS platform, showcasing how cloud-native technologies can be leveraged to provide encryption services within a containerized environment.

Zheng et al. [23] designed and implemented their anonymous proxy re-encryption (PRE) platform on Amazon Web Services (AWS), utilizing various services provided by the AWS platform to create a functional and secure environment. Amazon Elastic Compute Cloud (Amazon EC2) is a crucial component in their platform, responsible for hosting and executing the re-encryption processes. Amazon EC2 allows users to launch and manage virtual servers in the cloud, providing scalable computing resources. This makes it an ideal choice for executing resource-intensive PRE operations. For storage purposes, Zheng et al. [23] employed Amazon Simple Storage Service (Amazon S3). Amazon S3 is a scalable and highly available object storage service, suitable for securely storing re-encrypted data and other necessary files. This ensures that data can be accessed and retrieved efficiently while maintaining its integrity. To handle email services, Zheng et al. [23] utilized Hastymail, an open-source email platform. Hastymail likely facilitates secure email communication within their platform, enabling users to transfer re-encrypted emails. The AWS IoT (Internet of Things) platform securely connects and manages Internet of Things devices. AWS IoT is likely employed for the secure communication and management of IoT devices within the context of Zheng et al. [23]'s platform. Additionally, authentication and access control services are integral to the platform. The access control approach proposed by Ahmad et al. [44] is based on AWS IoT, demonstrating the seamless integration of access control mechanisms within the AWS environment. By leveraging AWS services, Zheng et al. [23] created a comprehensive platform for anonymous proxy re-encryption that takes advantage of the scalability, security, and versatility of the AWS cloud infrastructure.

Fortanix [52], deployed on Microsoft Azure, is a cloud-based data security platform that provides EaaS with several features, such as centralized management, key generation, and its life-cycle management, encryption and decryption, and access control management. Vault [53], a security platform designed by the Hashicorp company, also provides EaaS supporting different encryption algorithms such as AES, RSA, and ECDSA. The AWS platform [54] also provides data encryption, as one of its cloud services. Different configurations are available to select on this platform. Furthermore, the user can add data encryption to any of its services that are deployed on AWS. Keynexus [55] is a cloud-based platform, founded by Dark Matter Lab. It provides key management services, and its motto is *"separating the lock from the key"*.

There are also several open-source libraries and packages for implementing the individual crypto components in different languages. Bin-Faisal et al. [56] used the *PyCryptodome* [57] library of Python to implement the AES and RSA algorithms. This library supports many cryptographic functionalities, such as authentication modes, elliptic curve concepts, and hashing functions. The *Cryptography* library [58] is another Python alternative for implementing high-level and low-level cryptographic concepts. This library supports several functionalities, such as key and message digest generation. PyKMIP [59] is another Python library that provides key management processes, including the whole key life-cycle. This library was used by Bouamama et al. [60] for implementing key management functions in a cloud environment. Tink [61] is a C++ library developed by Google. It provides a secure API for the developers to perform cryptographic processes. This library was used by Sweet [62] for deploying the RSA and ECDSA algorithms. Java also has an encryption library, Jasypt [63], which provides basic cryptographic functionalities.

- The PyCryptodome library presents Python developers with a comprehensive and versatile toolkit for implementing cryptographic algorithms and functionalities. As demonstrated by Bin-Faisal et al. [56], PyCryptodome is a go-to solution for implementing cryptographic operations like AES and RSA within Python applications. This library boasts extensive features, including authentication modes, elliptic curves, hashing functions, symmetric and asymmetric encryption, digital signatures, and more. This breadth of functionalities makes PyCryptodome a robust and capable toolset for addressing a wide array of cryptographic requirements. One of the key advantages of PyCryptodome is its ease of use and its focus on providing a simplified interface for developers. This library prioritizes clear and intuitive coding practices, making it accessible even to those new to cryptographic programming. Moreover, PyCryptodome's consistent and well-documented API ensures that developers can confidently navigate its functionalities and leverage its capabilities effectively. Its popularity within the Python community further attests to its reliability and utility. For implementing cryptographic algorithms like AES and RSA, PyCryptodome streamlines the process and provides a reliable foundation for building secure and trustworthy applications. By utilizing PyCryptodome, developers can tap into a wealth of cryptographic tools essential for safeguarding sensitive data and ensuring the integrity of communication and transactions within their Python projects.

• Cryptography: Another option for Python developers is the Cryptography library. This library provides both high-level and low-level cryptographic concepts and functionalities. It supports various operations such as key generation, message digest generation, and more. It is a versatile library for implementing cryptography-related tasks in Python.

• In their work, Bouamama et al. [60] employed the PyKMIP library to facilitate the implementation of key management processes. PyKMIP, a Python library, is specifically designed to handle the entire key lifecycle within cryptographic systems. This library offers a comprehensive set of functions for key management tasks, including key generation, secure storage, and efficient distribution. PyKMIP's capabilities make it a valuable tool, particularly in cloud environments where robust and reliable key management is crucial. Its integration into the workflow of Bouamama et al. [60]'s research highlights the practicality and utility of PyKMIP in enabling effective key management solutions.

A. *Analysis of Methodologies*

• (PyKMIP) Bouamama et al. [60]: The methodology presented in this reference is commendable. PyKMIP, a Python-based key management library, was effectively utilized to implement key management processes. The approach is well-documented and provides a comprehensive suite of functionalities for the entire key lifecycle, ensuring secure key generation, storage, and distribution. The methodology is suitable for cloud environments and aligns with the goals of EaaS platforms, providing a reliable foundation for secure encryption services.

• (Cryptography Library) [59]: The Cryptography library for Python offers a sound methodology, encompassing both high-level and low-level cryptographic concepts and functionalities. It enables various operations, including key generation and message digest generation, demonstrating versatility in cryptography-related tasks. This library provides a robust foundation for implementing cryptographic operations in the context of EaaS, enhancing the security and functionality of the platform.

• (PyCryptodome) [57]: The methodology utilizing PyCryptodome, a Python library for cryptographic algorithms like AES and RSA, is well-structured and suitable for implementing a wide range of cryptographic functionalities. The library offers diverse cryptographic operations, including authentication modes, elliptic curves, and hashing functions. The approach provides a robust foundation for implementing encryption processes within EaaS, ensuring a high level of security and performance.

B. *Advantages and Benefits*

• The utilization of PyKMIP [59] contributes to enhanced key management within EaaS. Its comprehensive functionalities and support for the key lifecycle bolster the security and reliability of encryption services, a significant benefit for EaaS platforms.

• The adoption of the Cryptography library [59] offers both high-level and low-level cryptographic functionalities, providing a versatile toolkit for encryption tasks. This versatility enhances the adaptability and efficiency of cryptographic operations in EaaS platforms.

• PyCryptodome Bin-Faisal et al. [56] offers a comprehensive suite of cryptographic functionalities, including widely-used algorithms like AES and RSA. Its versatility in providing various cryptographic operations is a substantial advantage for implementing encryption mechanisms within EaaS, ensuring secure communication and data protection.

C. *Limitations and Potential Shortcomings*

• The PyKMIP library may face challenges with integration or compatibility with specific system architectures. Addressing potential integration issues and ensuring seamless adoption across various environments would be beneficial.

• The Cryptography library might have a learning curve due to its extensive functionalities. Providing ample documentation and support to users for effective utilization is crucial to mitigate the complexity associated with its wide range of cryptographic features.

• PyCryptodome might pose challenges in terms of computational overhead for resource-constrained devices in IoT. Mitigating this limitation through optimizations or alternative lightweight cryptographic libraries would enhance its applicability within the IoT context.

D. *Connections and Relationships Between References*

By presenting these connections and relationships between references, as well as showcasing the evolution of EaaS architectures, we provide a comprehensive understanding of how various works in the field are interlinked and have evolved over time.

• PyKMIP and Cryptography Library : Both references share a foundational connection in enhancing encryption mechanisms within EaaS platforms. While PyKMIP focuses on key management, the Cryptography library offers a broad spectrum of cryptographic functionalities. Integrating these tools could lead to a comprehensive EaaS system, addressing both secure key management and versatile cryptographic operations.

• Cryptography Library and PyCryptodome: These references are interconnected through their emphasis on cryptographic functionalities. While the Cryptography library provides a diverse set of cryptographic concepts, PyCryptodome specializes in cryptographic algorithm implementations. Integrating the high-level concepts from the Cryptography library with the specific algorithms from PyCryptodome can enhance the security and efficiency of cryptographic operations within EaaS.

• Amazon Simple Storage Service (Amazon S3) Zheng et al. [23] and PyKMIP : These references share a practical relationship, highlighting how secure key management (PyKMIP) can be coupled with reliable storage solutions (Amazon S3) in the context of EaaS. The integration of secure key management with robust storage capabilities is critical for ensuring the confidentiality and accessibility of cryptographic keys.

E. Showcasing the Evolution of EaaS Architectures

• The comparison of PyKMIP, Cryptography Library, and PyCryptodome demonstrates the evolution of EaaS architectures. Initially, the emphasis was on comprehensive key management (PyKMIP), followed by the integration of a versatile range of cryptographic functionalities (Cryptography Library). Finally, the focus shifted towards specific algorithm implementations (PyCryptodome), showcasing a progression in the development of encryption capabilities within EaaS architectures.

• The integration of Amazon Simple Storage Service (Amazon S3) highlights the evolving nature of EaaS, incorporating secure storage solutions to complement encryption services. This evolution signifies the recognition of the importance of data storage and access control within EaaS, marking a significant advancement in the architecture and functionality of EaaS platforms.

F. Integration of Ideas from Other References

• Integration of Blockchain Concepts: Incorporating blockchain concepts, such as decentralized key management and immutable audit trails, from the referenced works enhances the proposed EaaS architecture's security and transparency. By leveraging blockchain's tamper-proof nature for key management and audit trails, the architecture gains robustness against unauthorized access and ensures accountability in encryption activities.

• Leveraging Smart Contracts for Access Control: Integrating the concept of smart contracts for access control from the referenced work enhances the efficiency and precision of access management within the EaaS architecture. By automating access policies through smart contracts, access control becomes automated, ensuring that data is accessed only by authorized entities, improving the architecture's security posture.

• Enhancing Key Generation Security through Consensus Mechanisms: Incorporating the concept of consensus mechanisms for key generation from the referenced work strengthens the security of the EaaS architecture. By involving multiple participants in key generation, the architecture ensures a higher level of security in the key generation process, mitigating the risk of a single point of failure and potential security breaches.

• Decentralized Identity Management: Integrating decentralized identity management concepts into the proposed architecture enhances privacy and security. Allowing users to control and verify their identities without a central authority bolsters privacy measures, a vital aspect in the EaaS domain, ensuring user data confidentiality and trust. By integrating these innovative ideas and methodologies from other referenced works, the proposed EaaS architecture gains enhancements in security, efficiency, and robustness. These integrations enrich the architecture by leveraging state-of-the-art concepts to address critical aspects of EaaS, ultimately contributing to the advancement and effectiveness of the proposed architecture.

VII. EaaS Challenges

In this section, we highlight the challenges an EaaS platform may face. Some of these challenges are general, and others are specifically linked to the provisioning of EaaS to large-scale networks, such as IoT.

A. General challenges

One of the major challenges in deploying an EaaS platform is guaranteeing the availability of the crypto components. For example, the whole service will be affected if GC becomes unavailable in the Half-cloud-fog architecture. This is because the other components cannot work without the management commands of GC. On the other hand, since GC is located on FNs, migrating to another alternative FN leads to an extra delay. As a result, the crypto components' availability must be highly important. Launching a Denial of Service (DoS) or a Distributed DoS (DDoS) attack on GC, the adversaries may target the availability of the crypto components. As a result, a detailed security analysis must be conducted to demonstrate the resiliency of an EaaS platform against DoS/DDoS attacks [64].

The availability of the crypto components is not limited to their resistance against DoS/DDoS attacks. The entire design of an EaaS platform must be powerful enough to ensure availability under high-traffic situations. In other words, the platform must avoid having a single-point-of-failure component, either in communication channels, or at the network node level. For example, assume that the communication channel between CNs and FNs has limited bandwidth. In this condition, the waiting queue of the intermediate switches will be overloaded, and some FNs cannot connect to CNs. Consequently, the whole service may become unavailable. As another example, assume a single KC is in the platform. All devices have to use the keys that are generated by this component. But since there is only a single KC, it becomes the single-point-of-failure. This component cannot handle all requests in high-traffic situations, and the service cannot be completed.

The other EaaS challenge is handling the trade-off between an EaaS platform's performance and the number of supported network nodes. CNs and FNs are designed to reduce the load of computations from the end devices, especially the IoT devices that have limited resources. However, communicating with the cloud and fog layers to get the service results in extra delay. An ideal EaaS platform supports as many devices as possible while maintaining network performance. In addition to the end-to-end delay, the encryption power is another performance metric that must be considered. Some strong but complex algorithms can be implemented only on powerful devices. On the other hand, some simple algorithms with a lower level of protection against attacks exist, which can be implemented on the devices with limited resources. Now assume that we have two cases. In the first case, only a few devices can use the encryption service, while their data is strongly encrypted. In the second case, many devices are supported, but the ciphertexts are not resistant to sophisticated attacks. Solving this trade-off is challenging because it is hard to say whether the first case is better than the second one or not.

While EaaS allows outsourcing encryption services, which will elevate the problem of complexity of managing encryption operations by the clients and also the constraints of resources, which are commonly observed in IoT networks, the trust is an issue that needs to be taken into account. Indeed, EaaS relies on trust in the service provider, and proving the trust of a platform is challenging [65].

In heterogeneous networks, especially in IoT environments, some of the end-devices have emergency data to be encrypted, and the others generate only normal packets. For example, in a healthcare system, the sensor nodes collecting the patients' vital signs must have higher priority than the sensors collecting the room temperature. Therefore, DNs have different priorities to be served by the encryption service. This is another challenge for an EaaS platform to first specify the correct priority of DNs, and second to deploy an efficient mechanism for reflecting these priorities in the encryption process.

Considering green computing is another challenge of the EaaS platforms. The consumed energy must be under control in an ideal EaaS platform. All workstations do not have to be active when they have no processes to perform. The sleeping time of the idle components must be controlled to achieve the lowest possible energy-consumption state. Moreover, the lightweight encryption/decryption algorithms can be used to reduce energy consumption. However, designing a powerful but lightweight encryption algorithm is challenging.

EaaS platforms face the critical task of selecting encryption types that align with the unique demands of the domains they serve. This decision greatly influences the platform's ability to effectively cater to specific use cases. For instance, in sensitive environments like healthcare systems, where preserving data privacy and enabling computations on encrypted data are paramount, encryption techniques such as homomorphic encryption and searchable encryption become imperative. These techniques allow for secure analysis and querying of encrypted medical data without compromising privacy. In contrast, proxy re-encryption might be more suitable for scenarios where controlled data sharing and access control are the primary concerns, such as secure email forwarding. This highlights the need for developers to deeply understand the application's intricacies, security requirements, and performance considerations. Developers can make informed choices about the most suitable EaaS approach by accurately assessing these factors. Collaborating with both domain experts and cryptographic specialists is essential to ensure that the chosen encryption type not only aligns with the intended use but also addresses the potential challenges and complexities specific to the domain, resulting in a secure and effective EaaS platform.

B. Challenges of EaaS provisioning to large-scale networks

In the context of large-scale IoT environments, delays can quickly escalate due to the sheer volume of device connections within a short timeframe. This is particularly concerning for processes with significant time requirements, such as key generation in EaaS. In scenarios where each IoT device requires a unique key pair, the EaaS platform may become inundated with an overwhelming number of key generation requests. For instance, generating 1024-bit RSA key pairs for a million devices could take an impractical time, potentially exceeding a day given specific hardware specifications. While storing device identifiers alongside generated key pairs seems like a solution, the substantial space requirements and search times make it inefficient, especially when considering IPv6's 128-bit identifiers. A more efficient strategy could involve utilizing a hash table to group devices by identifier. Instead of generating a new key pair for each device, a single pair could be assigned to all devices within the same hash table row. This approach drastically reduces the key generation workload, as devices in a particular row share the same key pair. To enhance security, geographical information could be incorporated into device identifiers. Considering the device's location, the platform could prevent devices in the same region from sharing key pairs, thus mitigating potential eavesdropping risks from a single geographic area. This optimization ensures timely key generation and maintains security standards, enabling EaaS platforms to efficiently cater to the demands of large-scale IoT environments without compromising on performance or protection.

In the dynamic landscape of IoT networks, especially in mobile scenarios, the challenge of efficiently directing newly joining devices to the appropriate Encryption as a Service (EaaS) components becomes crucial. A parallel can be drawn between this challenge and the Domain Name System (DNS) infrastructure, where a hierarchical approach is employed to manage the resolution of domain names. However, in large-scale IoT deployments, the traditional centralized approach, where a single initiator server handles all device assignments, can be prone to single-points-of-failure and performance bottlenecks. A hierarchical structure of multiple initiators can be adopted to address this, akin to the DNS's hierarchy of servers. Each IoT device connects to a designated regional initiator server, which handles its initial assignments. If the required EaaS component is outside the scope of the regional initiator, the request can be forwarded to a higher-level initiator or root initiator. This distributed and hierarchical setup helps distribute the load and enhance the overall scalability and resilience of the system. The timing and frequency of IoT device connections to initiators should be carefully regulated to optimize this process further. Connecting to an initiator incurs some overhead due to communication and authentication processes, so deciding when and under what circumstances devices should initiate connections must balance performance and resource efficiency. For instance, IoT devices could connect to initiators upon initial registration or only when initiating new requests. Given the dynamic nature of IoT networks and the potential mobility, pre-configuring devices with fixed EaaS components might not be a viable solution. Instead, a mechanism that dynamically assigns EaaS components based on network conditions, device location, and load distribution should be considered. Since IoT devices often have limited storage resources, such mechanisms should be designed to minimize the storage overhead on the devices while ensuring efficient assignment and management of EaaS components.

In large-scale IoT networks, the looming threat of potent botnet armies, exemplified by the Mirai botnet, presents a significant challenge to Encryption as a Service (EaaS) platforms. These networks can serve as breeding grounds for Distributed Denial of Service (DDoS) attacks, which can be highly disruptive and challenging to mitigate effectively. The central challenge lies in safeguarding EaaS platforms against DDoS attacks that can be launched from compromised IoT devices. Balancing security and operational efficiency adds complexity to this challenge. IoT devices often need to send critical data within strict timeframes, leaving little room for delays introduced by mandatory security tests. Requiring every IoT device to undergo security checks before sending data can lead to missed deadlines, undermining the very purpose of time-sensitive IoT applications. Mitigation strategies such as preventing IoT devices from being compromised in the first place are valuable but extend beyond the core scope of EaaS services. One potential avenue is to incorporate load-balancing mechanisms within the EaaS platform. By efficiently distributing incoming requests across different EaaS components, the load balancing component can prevent a flood of traffic from causing service unavailability, thus mitigating the impact of DDoS attacks. Another approach involves implementing auto-scaling mechanisms within the EaaS platform architecture. This entails dynamically provisioning additional resources and capacity in response to traffic spikes or DDoS attacks. This way, the EaaS platform can scale up its capabilities to handle increased demand, ensuring service continuity during surge periods. However, the auto-scaling capability can be leveraged by attackers to reshape a DDoS attack into an Economical Denial of Sustainability (EDoS) attack. This leads to economic losses to service providers due to the increased elastic usage of resources. Thus, appropriate countermeasures to discriminate malicious scaling-up operations from legitimate ones are paramount [66] Overall, safeguarding EaaS platforms in large-scale IoT networks against DDoS threats requires a multi-faceted strategy encompassing efficient load distribution, auto-scaling mechanisms, and collaboration with broader security measures to minimize the risk of compromised IoT devices.

Large-scale networks are known for producing massive amounts of data. Processing these data in a short time requires important computational resources. Some lightweight cryptography algorithms have been recently proposed to cope with this problem. They use parallel and distributed computing with lower overhead. However, their security is not at the same level of the complex algorithms. Solving this trade-off is challenging for EaaS platforms. Moreover, an EaaS platform must pay attention to the huge volume of data that must be stored for end-devices, which request for a "secure storage service". The storage space must be distributed among different servers to support enough spaces. However, managing these servers and also protecting them is challenging. When an end-device tries to recover its stored data, its request must be first forwarded to the appropriate server, and then the specific key must be used to decrypt the stored ciphertext. It is challenging to track which device's data is stored on which server, particularly when the number of devices and their associated data are big.

To provision encryption services to large-scale networks, the EaaS platform has to be deployed in a distributed fashion. However, all distributed components must be synchronized to utilize the last updated data in their processes. For example, assuming the case wherein the key management component updates a device's key, but the encryption component is unaware of this change, and encrypts that device's plaintext with the old key, the ciphertext would become undecryptable. One of the characteristics of IoT networks is the rapid changes in the number of devices joining and leaving the network. In such dynamic situation, synchronization becomes more important. Effectively, under such scenarios, the EaaS platform must update its stored data or parameters when facing the changes, and hence, the components must always access the newest data. Another point to be considered in synchronization is the case wherein a device leaves the platform before being completely served. In this situation, the EaaS component that is performing the canceled process must be notified, so it stops the remaining part of the encryption process and that is in order to avoid wasting resources. In the case that EaaS uses parallel computation, the related components must be also well synchronized.

An EaaS platform that serves a large-scale network must avoid downtime, because the queues of waiting requests will overflow, and many packet losses may occur. This can cause serious damage to the service. In this vein, if a component becomes unavailable, its recovery time must be short. A good solution for this problem is considering some auxiliary/shadow components utilized when another component is down. But the challenging point is how many of these components must be considered. If we consider a big number of auxiliary components, we can avoid downtime, but the unused resources will be wasted, making the overall system not cost-efficient. On the other hand, if we do not consider a sufficient number of auxiliary components, we may face a long downtime. About the recovery process, it must be noted that an intermediary server must store the plaintexts/ciphertexts, so when an encryption/decryption component crashes, after recovering, the previous plaintexts/ciphertexts are again accessible. In other words, the end-devices must not resend their requests when a server crashes. In the case that auxiliary components are used, changing the forwarding rules of the network must be also considered, to handle the redirection between the down component and the auxiliary one. Software Defined Networking technologies may be leveraged in this regard.

C. Security and Privacy Issues in EaaS: An Expansive Exploration

In addition to the comprehensive examination of existing EaaS platforms, this survey paper takes cognizance of the paramount importance of addressing security and privacy concerns within this evolving landscape. Consequently, a thorough exploration was conducted to uncover the security and privacy issues inherent to EaaS platforms, thereby deepening our understanding of potential vulnerabilities and threats that can emerge when encryption services are outsourced. This meticulous exploration delved into the intricate realm of safeguarding sensitive data and ensuring user privacy in the context of EaaS. By offering readers valuable insights into these evolving security challenges, the paper provides a clear perspective on the multifaceted dimensions of security and privacy pertaining to EaaS platforms. This endeavor aims to furnish readers with a comprehensive overview of the intricate security and privacy aspects associated with EaaS platforms. In doing so, the survey not only enhances the comprehension of the advantages and constraints of EaaS but also empowers researchers, practitioners, and decision-makers with the knowledge essential for informed decision-making and the formulation of strategies that enhance the security and privacy of EaaS services. The exploration of security and privacy issues bolsters the relevance and practicality of this survey, as it squarely addresses the burgeoning concerns within the field. This in turn paves the way for more informed dialogues and inspires future research pursuits, thereby contributing to the ongoing discourse and advancement in the realm of EaaS.

D. Considering IoT-Specific Features in the Proposed EaaS Architecture

While the proposed Encryption as a Service (EaaS) architecture demonstrates its applicability to a wide range of scenarios, a pivotal aspect lies in its alignment with the distinct characteristics and demands of the Internet of Things (IoT) landscape. The efficacy of the EaaS solution becomes particularly pronounced when tailored to accommodate the intricate features that define IoT applications. First and foremost, the architecture accounts for the massive influx of IoT devices, each with varying processing capabilities and communication patterns. It leverages distributed components strategically positioned to cater to the dynamic demands of IoT's highly distributed and heterogeneous environment. The EaaS components, deployed across cloud, fog, and edge layers, cater to IoT devices' varying computational capacities while maintaining optimal service availability. Furthermore, the EaaS architecture embraces the dynamic nature of IoT networks, accommodating the rapid changes in device connectivity and mobility. With IoT devices frequently joining and leaving the network, the architecture employs intelligent mechanisms for efficient synchronization and dynamic resource allocation. This ensures that the EaaS services seamlessly adapt to the evolving IoT topology without compromising service quality. Incorporating security at every step, the proposed architecture acknowledges the unique security challenges of IoT ecosystems. It integrates robust authentication, authorization, and encryption mechanisms to safeguard IoT data transmissions, even in the face of potentially compromised devices. Moreover, the architecture aligns with IoT's energy constraints, optimizing cryptographic operations to minimize energy consumption and prolong device lifespans. To address the diverse nature of IoT applications, the architecture also allows for customization based on specific use cases. It supports encryption types suitable for different IoT data, whether it is health data in healthcare applications or industrial data in manufacturing settings. Tailoring the EaaS platform to cater to the unique requirements of various IoT domains ensures that the architecture aligns with the intricacies of IoT-specific applications. In summary, the proposed EaaS architecture offers a versatile solution for encryption services. Its true strength lies in its ability to enhance the specific features of IoT and seamlessly integrate IoT-specific characteristics into its design. This ensures that IoT applications receive robust encryption services tailored to their needs, ultimately contributing to a safer, more efficient, and secure IoT ecosystem.

VIII. Lessons learned

Encryption as a Service (EaaS) is an emerging paradigm that involves providing encryption capabilities as a service to users and applications over a network. This approach offers several advantages, including ease of use, centralized management, scalability, and cost-effectiveness. EaaS platforms typically encompass encryption engines, key management systems, access control mechanisms, and integration interfaces. One of the critical architectural considerations in EaaS is the choice of encryption algorithms and protocols. Different algorithms have varying security, performance, and key management requirements. For instance, symmetric key algorithms like AES (Advanced Encryption Standard) are efficient for bulk data encryption, while asymmetric key algorithms like RSA are essential for secure key exchange and digital signatures. Another architectural aspect involves key management, including key generation, distribution, rotation, and revocation. Effective key management is vital to ensuring the security and confidentiality of data. Secure and efficient key management is a significant challenge in EaaS, and finding appropriate solutions is critical. Performance evaluation is a crucial aspect of EaaS architecture. Encryption and decryption speed, throughput, latency, and resource utilization must be carefully assessed to ensure optimal performance. The choice of encryption algorithms, hardware acceleration, and efficient key management greatly influence the overall performance of the EaaS platform. Security challenges in EaaS encompass data privacy, key protection, and secure data transmission. Addressing these challenges requires robust encryption mechanisms, secure key management, access controls, and adherence to best practices in cryptographic implementations. Optimization strategies involve techniques to enhance the efficiency and effectiveness of EaaS platforms. This includes optimizing encryption and decryption processes, key management algorithms, and network communication protocols to minimize overhead and latency while maximizing security. The ”lessons learned” from a review of existing literature provide invaluable insights. For instance, understanding the trade-offs between security and performance is crucial. Achieving a balance between strong encryption and efficient processing is a persistent challenge in EaaS. Additionally, scalability and interoperability are significant factors to consider as EaaS solutions need to accommodate a growing number of users and diverse applications. Furthermore, the integration of EaaS with existing systems and cloud infrastructures is a topic of critical importance. Seamless integration while maintaining security and performance is a complex task requiring careful consideration of architectural design and implementation choices. In conclusion, Encryption as a Service (EaaS) represents a dynamic and evolving field at the intersection of security, networking, and cloud computing. Navigating this landscape requires a deep understanding of the architectural intricacies, security challenges, and optimization strategies associated with EaaS platforms. The ”lessons learned” serve as valuable guidelines for future research and development efforts, aiding in creating more secure, efficient, and scalable EaaS solutions.

A. *Full-Cloud Architecture*

A rigorous and critical analysis was conducted in the comprehensive review of each reference about the Full-Cloud Architecture. This analysis thoroughly examined the methodologies, experiments, and theoretical frameworks presented in these works. The primary objective was to assess the robustness and credibility of the findings and insights derived from each reference.

• Methodologies: The methodologies outlined in the references were scrutinized to evaluate their appropriateness and effectiveness in addressing the research objectives. This involved assessing the research design, data collection methods, and analytical techniques. Additionally, consideration was given to the sample sizes, selection criteria, and potential biases that could impact the research outcomes.

• Experiments: A meticulous evaluation of the experiments conducted in the references was carried out. This included an assessment of the experimental setup, parameters, and variables involved. The experiments' accuracy, repeatability, and control were considered, ensuring they were conducted under controlled conditions to yield reliable results. Any limitations or assumptions made during the experiments were identified and considered.

• Theoretical Frameworks: The theoretical frameworks proposed in the references were critically reviewed to gauge their relevance, applicability, and coherence. This involved assessing how well the frameworks aligned with established theories and concepts in the field. Any novel contributions or extensions to existing frameworks were evaluated for their potential to advance the understanding of Full-Cloud Architecture. By critically analyzing these aspects, the reliability and validity of the findings and insights from each reference were assessed. The objective was to ensure that the conclusions drawn and insights provided were well-founded, supported by sound methodologies and experiments, and aligned with the field's theoretical foundations. Additionally, comparisons were drawn across references to identify commonalities, differences, and emerging patterns. This comparative analysis further enriched the evaluation, offering a holistic view of the research landscape related to Full-Cloud Architecture. The insights gleaned from this critical analysis provided a robust foundation for synthesizing the collective knowledge and formulating the ”lessons learned” section, which serves as a valuable guide for researchers, practitioners, and developers in the domain of Full-Cloud Architecture. The Full-Cloud Architecture is designed to provide centralized management and streamline deployment processes, offering advantages in terms of ease of administration and efficient resource allocation. However, like any architectural approach, it has its challenges, particularly regarding scalability and availability, especially in the context of expansive and complex networks.

• Scalability Challenges: Implementing the Full-Cloud Architecture in large-scale networks can present scalability challenges. As the network grows in size and complexity, the centralized resources and management may struggle to handle the increased load and demand efficiently. Scaling up the central cloud infrastructure to meet these growing needs can be technically and economically challenging.

• Availability Concerns: Ensuring high availability in a Full-Cloud Architecture can be a significant concern. Relying on a centralized cloud infrastructure means that if the central cloud experiences downtime or disruptions, it can impact the entire network. This vulnerability to central points of failure risks the availability of services and data accessibility.

• Performance Limitations: While the centralized management simplifies administration, it can introduce performance limitations. The distance between end-users and the centralized cloud can increase latency, affecting real-time applications and services. Achieving low-latency communication across a wide network might be a challenge in this architecture.

• Bottlenecks and Single Points of Failure: The centralized nature of Full-Cloud Architecture can lead to bottlenecks at the central cloud point. If a critical service or infrastructure component at the central cloud experiences a failure, it can disrupt the entire network, leading to a single point of failure scenario. Redundancy and failover mechanisms need to be carefully implemented to mitigate this risk.

• Suitability for Performance-Critical Environments: Full-cloud architecture may not be the best fit for environments that require extremely high performance and low latency, such as finance or real-time analytics. These environments often demand distributed architectures that can process data locally or in a more distributed fashion to meet stringent performance requirements. In conclusion, while the Full-Cloud Architecture offers benefits in centralized management and ease of deployment, it's crucial to carefully consider its suitability for specific use cases. Understanding its limitations, particularly in terms of scalability, availability, and performance, is vital for making informed architectural decisions. Hybrid or distributed architectures might be more suitable for scenarios where stringent performance and availability requirements are paramount.

B. Half-Cloud Architecture

Similarly to examining the Full-Cloud Architecture, an in-depth analysis was conducted for each reference related to the Half-Cloud Architecture. This analysis encompassed a rigorous evaluation of methodologies, experimental setups, and theoretical frameworks presented in these references. The insights distilled from this extensive analysis have revealed important lessons about the Half-Cloud Architecture: Balance Between Centralization and Distribution: The Half-Cloud Architecture strikes a balance between centralization and distribution of components. By leveraging both cloud and edge computing capabilities, it optimally distributes tasks and processes between centralized cloud servers and local edge devices.

• Mitigation of Scalability and Latency Issues: This architecture effectively addresses some scalability and latency challenges observed in the Full-Cloud Architecture. By utilizing edge computing for processing closer to the data source alleviates the burden on the centralized cloud and significantly reduces latency for critical applications.

• Consideration of Synchronization and Load Balancing Challenges: Despite its advantages, the Half-Cloud Architecture introduces synchronization and load-balancing challenges. Coordinating tasks and data between the cloud and edge components requires careful design to ensure smooth operations and efficient load distribution, especially when dealing with fluctuating workloads.

• Suitability for Data Proximity Requirements: The Half-Cloud Architecture is particularly suitable for scenarios where data processing needs to occur near the data source. Applications that require real-time or near-real-time processing, or those that involve sensitive data, can greatly benefit from this architecture by ensuring data remains localized or processed closer to its origin. Understanding these lessons is vital for informed decision-making when considering the implementation of the Half-Cloud Architecture. It provides valuable insights into the architecture's strengths, potential challenges, and ideal use cases. By leveraging the benefits of centralized cloud and edge components and being mindful of synchronization and load balancing, this architecture can offer an efficient and effective solution for various applications, particularly those with specific data processing and latency requirements.

C. Half-Fog Architecture

In the analysis of references concerning the Half-Fog Architecture, an extensive and meticulous assessment of methodologies, experiments, and theoretical frameworks was conducted to ensure the credibility and validity of the findings and insights presented in these references.

• Efficient Data Processing and Latency Reduction: The Half-Fog Architecture offers a significant advantage by distributing components across edge devices. This distribution enhances data processing efficiency and reduces latency, making it particularly suitable for applications where real-time processing and low latency are critical, such as those in the domain of IoT.

• Applicability in Real-Time and Low-Latency Scenarios: This architecture is highly applicable in scenarios where real-time processing and minimal latency are paramount requirements. By leveraging fog computing capabilities at the edge, data can be processed swiftly, meeting the demands of applications that rely on rapid decision-making and responses.

• Management and Security Challenges: Despite its advantages, the Half-Fog Architecture introduces challenges related to managing and securing a distributed network of fog devices. Ensuring proper orchestration, synchronization, and load balancing while maintaining a robust security posture is imperative in this architecture. Addressing these challenges is crucial to realizing the benefits of the distributed approach.

• Synchronization and Load Balancing as Key Considerations: Proper synchronization of tasks and data and effective load balancing across the fog devices are pivotal considerations in the Half-Fog Architecture. Efficient task distribution and balanced workloads are essential to achieving optimal performance and responsiveness across the fog network. Understanding these lessons is essential for making informed decisions and implementing the Half-Fog Architecture effectively. By capitalizing on the benefits of edge device distribution for enhanced data processing efficiency and reduced latency and addressing the challenges related to network management, security, synchronization, and load balancing, this architecture can deliver efficient and responsive solutions, especially in IoT and other real-time applications.

D. Half-Cloud-Fog Architecture

In the comprehensive literature review of each reference related to the Half-Cloud-Fog Architecture, a meticulous analysis of methodologies, experiments, and theoretical frameworks was conducted to assess the quality and validity of the presented work thoroughly. The insights gleaned from this extensive analysis have provided critical lessons about the Half-Cloud-Fog Architecture:

• Synergy of Cloud and Fog Strengths: The Half-Cloud-Fog Architecture represents a promising approach that harnesses the strengths of both cloud and fog components. By effectively integrating cloud capabilities with edge-fog resources, this architecture offers a powerful solution with high potential for various applications.

• Suitability for Large-Scale IoT Networks: This architecture proves particularly well-suited for large-scale IoT networks, providing scalability, low latency, and efficient resource utilization. By extending computing capabilities to the edge (fog) while leveraging the scale and capabilities of the cloud, it addresses the unique requirements of IoT applications.

• Synchronization and Load Balancing Challenges: Despite its promise, effective synchronization and load balancing across the distributed cloud and fog components present significant challenges. Ensuring that tasks are optimally distributed and balanced across these diverse components is crucial for achieving optimal performance and responsiveness.

• Robust Orchestration Mechanisms are Vital: The complexity inherent in managing both cloud and fog resources necessitates robust orchestration mechanisms. Efficient orchestration

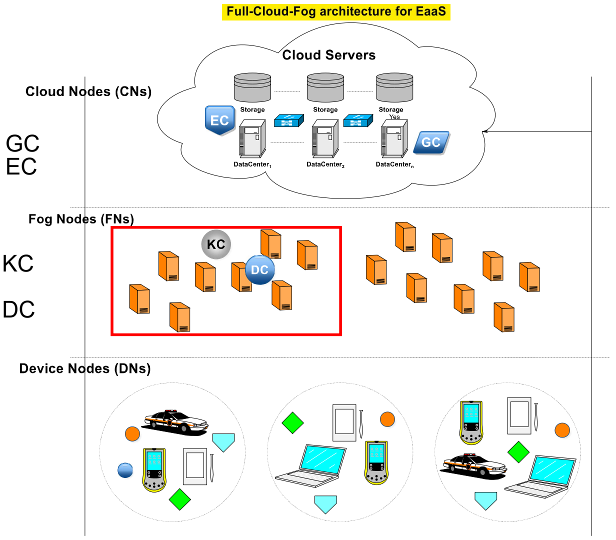

Fig. 6. The Full-Cloud-Fog architecture is suggested for EaaS.

is essential to manage, monitor, and optimize the utilization of resources across the cloud and fog layers, ensuring seamless operations and performance. Understanding these lessons is paramount for making informed decisions when adopting the Half-Cloud-Fog Architecture. By capitalizing on the combined strengths of cloud and fog components and effectively addressing synchronization, load balancing, and orchestration challenges, this architecture can unlock significant potential, especially in large-scale IoT networks.

IX. EaaS Open Issues

The EaaS architectures are discussed in section III. They are categorized into Full-Cloud, Half-Cloud, and Half-Fog. We believe that designing a Full-Cloud-Fog architecture may bring additional advantages compared to existing architectures. In the Full-Cloud-Fog architecture, the most frequent processes are performed by FNs, and CNs handle the others. The frequency of reading operations is greater than writing operations. Similarly, the frequency of encryption operations is greater than that of decryption operations. Hence, CNs can handle the general tasks (i.e., GC) and the encryption (EC) tasks, while FNs support the key management (KC) and decryption (DC) steps. DNs are not involved in the main cryptography activities. Therefore, with any limited resources, all the different types of devices can use the services. The overview of the suggested architecture is illustrated in Figure 6.

Our proposed architecture presents an effective solution to address the limitations of IoT networks, particularly the challenge of accommodating a significant influx of devices requesting encryption services. In such networks, the availability of cryptographic components may be at risk due to the sheer volume of requests. However, our architecture strategically tackles this issue by distributing the most common operations across multiple Fog Nodes (FNs). This decentralized approach efficiently handles high request loads, ensuring the system remains responsive and available. Furthermore, our architecture leverages the capabilities of Cloud Nodes (CNs) to support complex encryption algorithms. This ensures that the security level of the encryption services remains uncompromised despite the distributed nature of the operations. By combining the strengths of FNs and CNs, our architecture addresses the availability concerns and maintains the necessary security standards for encryption services in IoT networks. Through this approach, we mitigate the impact of limitations inherent to IoT networks, enhancing the overall performance and reliability of the Encryption as a Service (EaaS) platform.

Machine learning approaches indeed hold great potential for addressing challenges in Encryption as a Service (EaaS) platforms, as highlighted in section VII. The intricate trade-off between encryption service quality and the capacity to support a growing number of devices can be effectively tackled using machine learning techniques. With their ability to analyze multiple influencing factors and patterns, machine learning models can make more informed decisions that optimize this trade-off. Considering various features and characteristics, these models can dynamically adapt the encryption service to ensure security and scalability. Additionally, the concept of shadow nodes presents an innovative way to enhance the availability of cryptographic nodes. For instance, by employing a strategy where a group of shadow nodes, essentially replicas of primary nodes, are strategically placed to improve response time, the overall availability of the service can be increased. Machine learning, particularly reinforcement learning models, can play a vital role in the intelligent deployment of these shadow nodes. These models can learn from historical data and optimize the placement of shadow nodes to minimize delay and ensure cost-effectiveness, thus enhancing the reliability and responsiveness of the EaaS platform. Incorporating machine learning into EaaS not only improves decision-making and resource allocation but also contributes to the adaptability and efficiency of the platform, making it better equipped to handle the dynamic challenges posed by large-scale networks like IoT.

Addressing security concerns, including DoS/DDoS attacks and their countermeasures, is indeed a critical aspect of Encryption as a Service (EaaS) platforms. While Zhang et al. [13] acknowledges the importance of considering DoS/DDoS attacks and proposes countermeasures, there remains a need for further research in this field, particularly in conducting more comprehensive and detailed security analyses. As the landscape of cybersecurity evolves, it becomes imperative to continually enhance the resilience of EaaS platforms against emerging threats. Furthermore, in the context of EaaS platforms, ensuring security against various attack vectors is paramount. Zheng et al. [23] discussed the security of their platform against chosen ciphertext attacks, highlighting their efforts to protect the platform's cryptographic operations from vulnerabilities in this regard. Similarly, Tahir et al. [22] delved into distinguishability attacks, emphasizing the importance of robust encryption mechanisms to prevent unauthorized access to sensitive data. In conclusion, while various studies touch upon security concerns in EaaS platforms, ongoing research efforts are essential to strengthen these platforms' security posture. A comprehensive understanding of potential attack vectors, advanced cryptographic techniques, and proactive countermeasures is vital for ensuring the integrity, confidentiality, and availability of EaaS services.

A. Potential solutions based on Blockchain

More open issues deserve to be discussed, such as the solutions based on blockchain. Blockchain technology has gained significant attention recently due to its potential to enhance security, transparency, and decentralization. Exploring how blockchain can be integrated into EaaS platforms to address security, trust, and data integrity concerns is a promising area for future research. The scalability and performance implications of using blockchain in EaaS architectures should be thoroughly examined. Other open issues include the impact of quantum computing on encryption algorithms used in EaaS, the development of standardized protocols and interfaces for interoperability between different EaaS components, and the integration of machine learning techniques for adaptive and efficient resource allocation within EaaS platforms [67]. These emerging topics present exciting opportunities for further investigation and innovation, ensuring the continuous advancement of EaaS in the evolving landscape of information security and encryption services. Blockchain can play a pivotal role in bolstering EaaS platforms through many solutions. Decentralized Key Management, utilizing blockchain's inherent tamper-proof nature, allows the creation of a distributed key management system. Participants can possess unique key pairs, with blockchain recording key-related transactions, enhancing security and minimizing dependence on a single authority. Immutable Audit Trails harness blockchain's transparency and immutability to establish verifiable audit trails for encryption activities encompassing encryption, decryption, key generation, and access control, fostering accountability crucial for security and compliance. Smart Contracts for Access Control introduce automated access control policies via smart contracts, enacting predefined access rules and ensuring data is exclusively accessed by authorized entities, with access changes transparently recorded on the blockchain. Secure Data Sharing and Collaboration leverage blockchain to facilitate encrypted data sharing and collaboration among diverse parties, storing encrypted data on the blockchain and managing access permissions through smart contracts, thus enhancing data integrity and restricting access to authorized participants. Blockchain's Distributed Trust Establishment enables verifying the legitimacy of encryption services, certificates, and keys, leveraging blockchain's immutable and distributed nature to mitigate the risk of compromised services. Decentralized Identity Management transforms identity management, endowing users with control over their identity information, while identity verification occurs sans reliance on a central authority, bolstering privacy and thwarting identity-related threats. Data Provenance and Auditing achieve tamper-proof data provenance and auditing, with each data interaction, including encryption, decryption, and sharing, recorded unalterably on the blockchain, ensuring data integrity and facilitating detailed audits for regulatory adherence. Consensus Mechanisms for Key Generation enhance key generation security, employing blockchain's consensus mechanisms for collaborative key generation, bolstering the security of generated keys through multiparty involvement. While blockchain offers these solutions, challenges like scalability, performance, and integration must be navigated. Researchers can conduct in-depth investigations into these solutions, carefully analyzing their advantages, potential challenges, and real-world implementations. By conducting such thorough examinations, researchers can comprehensively uncover the intricate ways blockchain can contribute to the advancement of EaaS platforms. This exploration addresses the landscape's dynamic security and privacy concerns and establishes a foundation for well-informed dialogues and future research initiatives. Moreover, future researchers should consider delving further into these areas to refine and expand upon the proposed solutions, pushing the boundaries of knowledge in the field and fostering continued innovation. Potential solutions based on Blockchain for Encryption as a Service (EaaS) platforms encompass a range of innovative applications. Firstly, Blockchain offers secure cross-platform data sharing and collaboration by encrypting and storing data on the chain, with smart contracts defining access rules to ensure only authorized parties can access and collaborate on specific data. Immutable digital signatures for encrypted data can also be stored on the Blockchain, leveraging its immutability to detect any unauthorized modification or tampering, thus ensuring data integrity. Additionally, Blockchain enables decentralized and encrypted messaging, enhancing communication security. Furthermore, it can secure the supply chain by encrypting critical data such as transaction records, shipment details, and quality certifications, thus enhancing supply chain security and traceability. Blockchain can also revolutionize identity verification by storing encrypted identity information and enabling cryptographic proofs without exposing sensitive data, thus enhancing privacy and security in identity management. Moreover, Blockchain can define decentralized access control and permissions through smart contracts, enhancing overall data security. Integration with Hardware Security Modules (HSMs) further enhances key management security by securely storing encryption keys and recording access transactions on the Blockchain. Additionally, encrypted data can be securely stored and backed up on the Blockchain, and secure IoT communication can be facilitated by recording encryption-related transactions on the chain. Lastly, Blockchain's immutability is utilized for creating tamper-proof logs of encryption-related activities and security events, enhancing security auditing and forensic analysis. Implementing and refining these solutions can substantially elevate security, transparency, and efficiency for EaaS platforms, ultimately providing a more robust and secure environment for encrypted data management and services.

B. Potential solutions based on Homomorphic Encryption

Homomorphic encryption is a cryptographic method that enables computations to be conducted on encrypted data, maintaining data privacy and security. The term ”homomorphic” is derived from ”homo-” meaning the same and ”-morphic” implying form, indicating that the structure of the data remains consistent even when encrypted. This unique property allows mathematical operations to be applied to encrypted data so that the results, when decrypted, correspond to the outcomes of operations performed on unencrypted data. There exist several types of homomorphic encryption schemes, each with varying levels of computational capabilities:

- Partial Homomorphic Encryption (PHE): PHE permits evaluating specific mathematical operations like addition or multiplication on encrypted data. For instance, encrypted numbers can be added or multiplied, and upon decryption, the results precisely match those obtained by performing the operations on the plaintext numbers.
- Somewhat Homomorphic Encryption (SHE): SHE schemes extend PHE by allowing multiple mathematical operations, typically addition and a constrained form of multiplication. While they do not support an unlimited range of operations, they provide more flexibility than PHE, allowing for moderately complex computations on encrypted data.
- Fully Homomorphic Encryption (FHE): FHE represents the most potent form of homomorphic encryption, enabling an arbitrary number of additions and multiplications on encrypted data. This advanced capability means highly intricate computations can be carried out on the encrypted data. The decrypted results match those computed on the plaintext data. Homomorphic encryption finds critical applications across various domains, including secure cloud computing, privacy-preserving data analysis, and secure machine learning. For instance, a healthcare service provider could utilize homomorphic encryption to perform calculations on encrypted patient data stored in the cloud without compromising patient privacy. However, it's essential to note that homomorphic encryption is computationally demanding, resulting in slower processing than traditional encryption and decryption methods. Ongoing advancements in this field aim to improve the efficiency and practicality of homomorphic encryption to broaden its usage in real-world applications.

C. Potential solutions based on Federated Learning emerges Encryption

In Encryption as a Service (EaaS), Federated Learning emerges as a powerful tool for collaborative enhancement without compromising data privacy. EaaS providers can harness Federated Learning to refine encryption models collectively, elevating the overall service quality while preserving the sanctity of sensitive encryption algorithms and user data. By involving participating entities like organizations or devices, Federated Learning enables the customization of encryption algorithms tailored to specific security requirements and usage patterns, ensuring a seamless alignment with evolving security standards. Moreover, Federated Learning extends its capabilities to fortify critical management systems, allowing for the collaborative improvement of crucial aspects such as key generation, distribution, and rotation, all while upholding confidentiality. This collaborative approach extends to security domains, enabling decentralized attack detection and prevention through collective analysis of attack patterns and anomalies in encrypted communication. Additionally, Federated Learning empowers EaaS platforms to efficiently allocate resources and balance loads based on local usage patterns, ensuring optimized performance and resource provisioning without compromising data privacy. The potential also lies in collective security parameter tuning, allowing entities to collaboratively adjust parameters such as critical lengths and cryptographic hash functions to balance security and performance. Furthermore, the application of Federated Learning extends to the realm of IoT, facilitating the creation of adaptive encryption algorithms designed to evolve according to IoT device characteristics and usage patterns, bolstering IoT data transmission security without centralizing sensitive information. Lastly, Federated Learning aids in the optimization of Secure Multi-Party Computation (SMPC) techniques, enhancing efficiency and scalability while maintaining data privacy. These potential solutions collectively underscore how Federated Learning can revolutionize EaaS, enabling heightened security, efficiency, and customization while diligently preserving data privacy and confidentiality.

D. Potential solutions based on Trusted Execution Environments (TEEs)

In Encryption as a Service (EaaS), leveraging Trusted Execution Environments (TEEs) presents an unparalleled opportunity to fortify the security landscape. TEEs like Intel SGX or ARM TrustZone offer secure enclaves, creating isolated and impenetrable environments where critical encryption processes and key management operations can be executed. These secure enclaves are bastions of data confidentiality and integrity, ensuring that encryption tasks remain shielded from threats. EaaS providers can capitalize on TEEs to establish enhanced encryption protocols and secure communication channels. Secure key exchanges and encryption handshakes can seamlessly occur within these enclaves, guaranteeing end-to-end data confidentiality and bolstering the security of encryption processes. Additionally, TEEs can be instrumental in securing data at rest, allowing EaaS to encrypt and store sensitive data within these secure enclaves and providing additional protection against unauthorized access or data breaches. Looking forward, in the face of emerging threats from quantum computing, the integration of post-quantum cryptography within EaaS stands paramount. Quantum-resistant cryptographic algorithms, such as lattice-based cryptography or hash-based signatures, promise to ensure the longevity and resilience of encryption mechanisms against potential quantum attacks. Furthermore, adopting quantum-secure key exchange protocols, such as those proposed by NIST PQC competition finalists, reinforces secure communication, ensuring that encryption key distribution and management remain impervious to quantum threats. These combined potential solutions underscore how integrating TEEs and embracing post-quantum cryptography can substantially elevate the security posture of EaaS platforms, guaranteeing data confidentiality, integrity, and future-proofing against the evolving threat landscape, notably quantum computing.

E. Potential solutions based on Post-Quantum Cryptography

In the dynamic and ever-evolving landscape of data security, encryption ensures the confidentiality and integrity of sensitive information. However, with the imminent threat of quantum computing, traditional encryption algorithms face potential vulnerabilities. Quantum computers, leveraging the principles of quantum mechanics, possess unparalleled processing power that could undermine widely used encryption methods like RSA and ECC. To fortify the encryption ecosystem and prepare for the post-quantum era, a paradigm shift towards Post-Quantum Cryptography (PQC) is imperative. Encryption as a Service (EaaS) is pivotal in this security revolution. EaaS providers increasingly recognize the importance of integrating post-quantum cryptographic techniques into their platforms. By seamlessly incorporating post-quantum encryption algorithms such as lattice-based cryptography and hash-based signatures, EaaS platforms future-proof their security infrastructure. Lattice-based cryptography, for instance, relies on the mathematical properties of lattices, providing a foundation for quantum-secure cryptographic schemes. Similarly, hash-based signatures utilize the computational hardness of hash functions to achieve post-quantum security. These cryptographic approaches ensure that data remains confidential and secure, even in the face of rapidly advancing quantum computing capabilities. Hybrid encryption schemes present another layer of security by combining classical encryption algorithms with post-quantum cryptography. This fusion offers a resilient approach, leveraging the strengths of both classical and post-quantum cryptographic techniques. The classical algorithms provide robust and efficient encryption, while the post-quantum elements safeguard against potential quantum threats. This integration aims to achieve a security architecture that remains potent against emerging cryptographic challenges. Quantum-secure fundamental exchange mechanisms are pivotal in this ecosystem. Algorithms proposed by the NIST PQC competition finalists, such as those based on isogenies, hash functions, or code-based cryptography, provide the foundation for secure key management and distribution. These mechanisms ensure that encryption keys are securely exchanged, preventing potential compromise due to future quantum advancements. Moreover, incorporating quantum-resistant digital signatures and secure multi-party computation (SMPC) protocols further enhances the security of EaaS platforms. Quantum-resistant digital signatures, such as hash-based signatures, guarantee the authenticity and integrity of digital messages, crucial for secure communication and data verification. On the other hand, SMPC protocols enable secure computations on encrypted data, ensuring confidentiality and integrity in collaborative encryption processes even in a quantum-threatened environment. Strengthening critical management systems using post-quantum cryptographic techniques ensures that encryption keys maintain their integrity and security throughout their lifecycle. This includes secure key generation, distribution, and rotation, providing a robust foundation for the overall security of the encryption processes within EaaS. Equally important is disseminating knowledge and awareness about the implications of post-quantum security within the EaaS ecosystem. Educating users and organizations about the significance and integration of post-quantum cryptography empowers them to secure their data in this rapidly advancing digital age. It involves training on the usage and benefits of post-quantum algorithms, potential vulnerabilities in the era of quantum computing, and best practices to navigate this evolving security landscape. In conclusion, these combined potential solutions underscore how EaaS, fortified by Post-Quantum Cryptography, stands resilient in the face of quantum computing. They ensure data confidentiality, integrity, and adaptability in a dynamic security landscape. By integrating these advanced cryptographic techniques and promoting awareness, EaaS platforms prepare for a secure and quantum-safe future, assuring users of their data's protection even in the era of quantum advancements.

X. Conclusion

A. Conclusion and Finding

The Internet of Things (IoT) paradigm has brought forth the need to safeguard the security and privacy of the vast data generated by IoT devices. Encryption as a Service (EaaS) emerges as a potential solution to address these concerns by providing cryptographic capabilities to protect IoT data. This paper provides a comprehensive overview of the diverse EaaS platforms proposed in the literature, organizing them into distinct categories such as Full-Cloud, Half-Fog, Half-Cloud-Fog architectures. By categorizing these platforms, the paper helps researchers and practitioners navigate the landscape of EaaS solutions. Furthermore, the paper delves into these platforms' encryption types, ranging from attribute-based and homomorphic encryption to searchable encryption and even quantum encryption. This exploration sheds light on the versatility of EaaS in accommodating various encryption needs across different domains. The paper also provides valuable insights into real-world implementations by highlighting testbeds that have realized EaaS solutions. It identifies the open-source tools and commercial platforms that have brought these solutions to life, offering researchers and developers practical resources for further exploration and experimentation. In essence, this paper contributes to the understanding of how EaaS can contribute to securing IoT data while presenting a comprehensive overview of the existing landscape of EaaS platforms, their architectural approaches, encryption capabilities, and real-world implementations. By categorizing and summarizing this information, the paper serves as a valuable resource for those seeking to leverage EaaS to address the security challenges posed by the ever-growing realm of IoT. In addition to its comprehensive exploration of existing EaaS platforms, this paper also critically examines the challenges they face in delivering their services effectively. These challenges encompass multiple aspects, including the availability of platform components, the delicate balance between service performance and the number of supported devices, and the consideration of green computing practices to optimize resource utilization. Recognizing the significance of addressing these challenges, the paper goes beyond a mere overview and proposes potential solutions to enhance the overall effectiveness of EaaS platforms, particularly in the context of IoT applications. The paper outlines strategies to tackle these challenges and underscores the importance of innovation and problem-solving in EaaS. One notable proposed solution is the reimagining of platform architecture to accommodate the demands of IoT networks better. Additionally, the integration of machine learning techniques is highlighted to optimize the trade-off between service quality and scalability [68]. These solutions provide a roadmap for addressing the challenges and underscore the paper's commitment to contributing actionable insights to the field. In summary, this paper not only identifies the hurdles that EaaS platforms face but also demonstrates a forward-looking perspective by offering innovative solutions to enhance their efficiency and efficacy, particularly in the intricate landscape of IoT. By doing so, the paper encapsulates the essence of research and development in the evolving realm of encryption services, paving the way for future advancements in securing IoT data through EaaS solutions.

B. Summing up

The widespread adoption of Internet of Things (IoT) technology, characterized by a vast network of interconnected devices, has significantly transformed the way we interact with the digital world. However, this proliferation has also introduced a host of cybersecurity challenges, emphasizing the need for robust security measures to protect sensitive data and ensure the smooth functioning of IoT ecosystems. One of the critical aspects of IoT security is encryption, a fundamental tool in safeguarding data integrity and confidentiality. As IoT devices often operate with limited resources, traditional encryption methods may be too computationally intensive. To address this issue, encryption services are being offloaded to cloud and fog platforms, optimizing resource usage and mitigating cybersecurity risks associated with IoT. Encryption as a Service (EaaS) has emerged as a promising remedy, offering tailored cryptographic solutions that align with the resource constraints of IoT devices. EaaS optimizes encryption processes, allowing IoT devices to operate efficiently while maintaining high security. This study delves into the realm of EaaS, thoroughly examining existing EaaS platforms and categorizing them based on encryption algorithms and service offerings. In addition to categorization, this study outlines various EaaS architecture types based on the placement of key components, providing insights into the optimal design and configuration of EaaS solutions for diverse IoT environments. Practical implementations of these platforms are explored through different testbeds, providing real-world demonstrations of EaaS capabilities and advantages in IoT security. A key focus of this comprehensive exploration lies in dissecting EaaS's challenges, particularly in IoT. These challenges encompass scalability, latency, interoperability, and key management issues. Addressing these challenges is crucial for adopting and implementing EaaS in IoT environments. The study suggests potential remedies and innovative approaches to mitigate these challenges, enhancing the efficacy and adoption of EaaS in IoT security. Overall, this work stands out as an all-encompassing exploration, bridging the gap left by previous surveys and providing a deep understanding of EaaS in the context of IoT security. By addressing the nuanced intricacies of EaaS and its alignment with IoT requirements, this study contributes to the advancement of secure IoT ecosystems. It sets a foundation for future research and innovation in this critical domain.

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), and the Research Council of Finland (former Academy of Finland) 6G Flagship program (Grant No. 346208). The paper reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains.

The work of Prof. Y. Bin was supported in part by the National Natural Science Foundation of China under Grant No. 62372076. The work of Dr. Y. Zhao was supported by the National Science Foundation of China under Grant No. U20B2049, U20B2048 and U20B2046.

References

[1] A. Javadpour, F. Ja'fari, T. Taleb, and C. Benzaïd, "Reinforcement learning-based slice isolation against ddos attacks in beyond 5g networks," *IEEE Transactions on Network and Service Management*, 2023.

[2] Y. Wang, Z. Su, N. Zhang, J. Chen, X. Sun, Z. Ye, and Z. Zhou, "Spds: A secure and auditable private data sharing scheme for smart grid based on blockchain," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7688–7699, 2020.

[3] S. Kaur, T. Kaur, and A. Sharma, "Cloud-enabled education-as-a-service (eaas)—a review," *ICT Systems and Sustainability: Proceedings of ICT4SD 2021, Volume 1*, pp. 397–404, 2022.

[4] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, "Advanced lightweight encryption algorithms for iot devices: survey, challenges and solutions," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–18, 2017.

[5] S. Kang, B. Veeravalli, and K. M. M. Aung, "Espresso: An encryption as a service for cloud storage systems," in *Monitoring and Securing Virtualized Networks and Services: 8th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2014, Brno, Czech Republic, June 30–July 3, 2014. Proceedings 8*. Springer, 2014, pp. 15–28.

[6] R. F. Olanrewaju, T. Islam, O. O. Khalifa, F. Anwar, and B. R. Pampori, "Cryptography as a service (caas): quantum cryptography for secure cloud computing," *Indian Journal of Science and Technology*, vol. 10, no. 7, pp. 1–6, 2017.

[7] N. Rahimi, J. J. Reed, and B. Gupta, "On the significance of cryptography as a service," *Journal of Information Security*, vol. 9, no. 4, pp. 242–256, 2018.

[8] M. Al-Shabi, "A survey on symmetric and asymmetric cryptography algorithms in information security," *International Journal of Scientific and Research Publications (IJSRP)*, vol. 9, no. 3, pp. 576–589, 2019.

[9] Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, T. H. Luan, and X. Shen, "A survey on metaverse: Fundamentals,

security, and privacy," *IEEE Communications Surveys Tutorials*, vol. 25, no. 1, pp. 319–352, 2023.

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

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

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

[13] H. Zhang, B. Qin, T. Tu, Z. Guo, F. Gao, and Q. Wen, "An adaptive encryption-as-a-service architecture based on fog computing for real-time substation communications," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 658–668, 2019.

[14] A. Javadpour, G. Wang, and S. Rezaei, "Resource management in a peer to peer cloud network for iot," *Wireless Personal Communications*, vol. 115, pp. 2471–2488, 2020.

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

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

[17] A. El Bouchti, S. Bahsani, and T. Nahhal, "Encryption as a service for data healthcare cloud security," in *2016 fifth international conference on future generation communication technologies (FGCT)*. IEEE, 2016, pp. 48–54.

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

[19] O. Zibouh, A. Dalli, and H. Drissi, "Encryption as a service based on parallelizing fully homomorphic encryption implementation on openstack cloud computing," *International Journal of Applied Engineering Research*, vol. 12, no. 22, pp. 12 982–12 988, 2017.

[20] K. Zkik, M. Tebaa, T. Tachihante, and G. Orhanou, "A new authentication and homomorphic encryption as a service model for preserving privacy in clouds." *J. Comput. Sci.*, vol. 13, no. 12, pp. 702–717, 2017.

[21] S. Tahir, S. Ruj, A. Sajjad, and M. Rajarajan, "Fuzzy keywords enabled ranked searchable encryption scheme for a public cloud environment," *Computer Communications*, vol. 133, pp. 102–114, 2019.

[22] S. Tahir, L. Steponkus, S. Ruj, M. Rajarajan, and A. Sajjad, "A parallelized disjunctive query based searchable encryption scheme for big data," *Future Generation Computer Systems*, vol. 109, pp. 583–592, 2020.

[23] Q. Zheng, W. Zhu, J. Zhu, and X. Zhang, "Improved anonymous proxy re-encryption with cca security," in *Proceedings of the 9th ACM symposium on Information, computer and communications security*, 2014, pp. 249–258.

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

[25] ——, "Cloud file sharing using preaas," *EHEI-Journal of Science & Technology*, vol. 1, no. 2, pp. 52–63, 2021.

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

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

[28] H. Rahmani, E. Sundararajan, Z. M. Ali, and A. M. Zin, "Encryption as a service (eaas) as a solution for cryptography in cloud," *Procedia Technology*, vol. 11, pp. 1202–1210, 2013.

[29] S. Kang, B. Veeravalli, and K. M. M. Aung, "Espresso: An encryption as a service for cloud storage systems," in *IFIP International Conference on Autonomous Infrastructure, Management and Security*. Springer, 2014, pp. 15–28.

[30] Q. H. Vu, M. Colombo, R. Asal, A. Sajjad, F. A. El-Moussa, and T. Dimitrakos, "Secure cloud storage: a framework for data protection as a service in the multi-cloud environment," in *2015 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2015, pp. 638–642.

[31] K. Ateeq, M. R. Pradhan, B. Mago, and T. Ghazal, "Encryption as a service for multi-cloud environment," *International Journal of Advanced Research in Engineering and Technology (IJARET)*, vol. 11, no. 7, pp. 622–628, 2020.

[32] C. Benzaid, K. Lounis, A. Al-Nemrat, N. Badache, and M. Alazab, "Fast authentication in wireless sensor networks," *Future Generation Computer Systems*, vol. 55, pp. 362 – 375, 2016.

[33] A. Sbai, C. Drocourt, and G. Dequen, "A new delegated authentication protocol based on pre," in *18th International Conference on Security and Cryptography*. SCITEPRESS-Science and Technology Publications, 2021, pp. 468–478.

[34] R. F. Olanrewaju, T. Islam, O. O. Khalifa, F. Anwar, and B. R. Pampori, "Cryptography as a service (caas): quantum cryptography for secure cloud computing," *Indian Journal of Science and Technology*, vol. 10, no. 7, pp. 1–6, 2017.

[35] A. Boudi, M. Bagaa, P. Poyhonen, T. Taleb, and H. Flinck, "Ai-based resource management in beyond 5g cloud native environment," *IEEE Network Magazine*, vol. 35, no. 2, pp. 128 – 135, Mar. 2021.

[36] C. Benzaid, T. Taleb, and J. Song, "AI-based Autonomic & Scalable Security Management Architecture for Secure Network Slicing in B5G," *IEEE Network Magazine*, vol. 36, no. 6, pp. 165 – 174, July 2022.

[37] R. K. Bedi, J. Singh, and S. K. Gupta, "Mwc: an efficient and secure multi-cloud storage approach to leverage augmentation of multi-cloud storage services on mobile devices using fog computing," *The Journal of Supercomputing*, vol. 75, no. 6, pp. 3264–3287, 2019.

[38] M. A. B. Sahbudin, R. Di Pietro, and M. Scarpa, "A web client secure storage approach in multi-cloud environment," in *2019 4th International Conference on Computing, Communications and Security (ICCCS)*. IEEE, 2019, pp. 1–7.

[39] M. M. Ahsan, I. Ali, M. Imran, M. Y. I. Idris, S. Khan, and A. Khan, "A fog-centric secure cloud storage scheme," *IEEE Transactions on Sustainable Computing*, 2019.

[40] P. Chinnasamy and P. Deepalakshmi, "A scalable multilabel-based access control as a service for the cloud (smbacaas)," *Transactions on Emerging Telecommunications Technologies*, vol. 29, no. 8, p. e3458, 2018.

[41] P. Zhang, Z. Chen, J. K. Liu, K. Liang, and H. Liu, "An efficient access control scheme with outsourcing capability and attribute update for fog computing," *Future Generation Computer Systems*, vol. 78, pp. 753–762, 2018.

[42] A. Meshram, S. Das, S. Sural, J. Vaidya, and V. Atluri, "Abacaas: attribute-based access control as a service," in *Proceedings of the Ninth ACM Conference on data and application security and privacy*, 2019, pp. 153–155.

[43] R. Kumar, B. Palanisamy, and S. Sural, "Beaas: Blockchain enabled attribute-based access control as a service," in *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2021, pp. 1–3.

[44] T. Ahmad, U. Morelli, S. Ranise, and N. Zannone, "A lazy approach to access control as a service (acaas) for iot: an aws case study," in *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies*, 2018, pp. 235–246.

[45] A. Taurshia, G. J. W. Kathrine, S. David, and S. S. Ilango, "A hybrid groupkey management service for static iot applications," *Annals of the Romanian Society for Cell Biology*, pp. 4449–4455, 2021.

[46] M. Qiu, H. Qiu, H. Zhao, M. Liu, and B. Thuraisingham, "Secure data sharing through untrusted clouds with blockchain-enhanced key management," in *2020 3rd International Conference on Smart BlockChain (SmartBlock)*. IEEE, 2020, pp. 11–16.

[47] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, "Kaas: Key as a service over quantum key distribution integrated optical networks," *IEEE Communications Magazine*, vol. 57, no. 5, pp. 152–159, 2019.

[48] ——, "Sdqaas: Software defined networking for quantum key distribution as a service," *Optics Express*, vol. 27, no. 5, pp. 6892–6909, 2019.

[49] M. A. Kalyankar and C. Kumar, "Aadhaar enabled secure private cloud with digital signature as a service," in *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)*. IEEE, 2018, pp. 533–538.

[50] S. Sun, R. Zhang, and H. Ma, "Efficient parallelism of post-quantum signature scheme sphincs," *IEEE Transactions on Parallel and Distributed Systems*, vol. 31, no. 11, pp. 2542–2555, 2020.

[51] A. Javadpour, A. Nafei, F. Ja'fari, P. Pinto, W. Zhang, and A. K. Sangaiah, "An intelligent energy-efficient approach for managing ioe tasks in cloud platforms," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 4, pp. 3963–3979, 2023.

[52] Fortanix, "Encryption as a service," https://www.fortanix.com/solutions/use-case/encryption-as-a-service, 2022, [Accessed: June 2022].

[53] Vault, "Encryption as a service: Transit secrets engine," https://learn.hashicorp.com/tutorials/vault/eaas-transit, 2022, [Accessed: June 2022].

[54] A. W. S. (AWS), "Introduction to aws security: Aws whitepaper," https://docs.aws.amazon.com/whitepapers/latest/introduction-aws-security/data-encryption.html, 2021, [Accessed: June 2022].

[55] Crunchbase, "Keynexus - crunchbase company profile & funding," https://www.crunchbase.com/organization/keynexus, 2022, [Accessed: Aug 2022].

[56] S. Bin-Faisal, D. Nandi, and M. Rahman, "Dual layer encryption for iot based vehicle systems over 5g communication," *International Journal of Information Technology and Computer Science(IJITCS)*, 2022.

[57] pycryptodome, "Cryptographic library for python," https://pypi.org/project/pycryptodome/, 2022, [Accessed: June 2022].

[58] cryptography, "A package which provides cryptographic recipes and primitives to python developers," https://pypi.org/project/cryptography/, 2022, [Accessed: June 2022].

[59] pykmip, "Kmip library," https://pypi.org/project/PyKMIP/, 2021, [Accessed: June 2022].

[60] J. Bouamama, M. Hedabou, and M. Erradi, "Cloud key management using trusted execution environment," 2021.

[61] tink, "Tink cryptographic library," https://developers.google.com/tink, 2022, [Accessed: June 2022].

[62] L. Sweet, "A decentralized computation platform," 2019.

[63] jasypt, "Java simplified encryption," http://www.jasypt.org/, 2019, [Accessed: June 2022].

[64] A. Javadpour, F. Ja'fari, T. Taleb, and M. Shojafar, "A cost-effective mtd approach for ddos attacks in software-defined networks," in *GLOBECOM 2022-2022 IEEE Global Communications Conference*. IEEE, 2022, pp. 4173–4178.

[65] C. Benzaïd, T. Taleb, and M. Z. Farooqi, "Trust in 5G and Beyond Networks," *IEEE Network*, vol. 35, no. 3, pp. 212–222, 2021.

[66] C. Benzaid, T. Taleb, A. Sami, and O. Hireche, *A Deep Transfer Learning-powered EDoS Detection Mechanism for 5G and Beyond Network Slicing*. GLOBECOM 2023 IEEE Global Communications Conference, p. 3963–3979.

[67] Y. Wang, Z. Su, J. Ni, N. Zhang, and X. Shen, "Blockchain-empowered space-air-ground integrated networks: Opportunities, challenges, and solutions," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 160–209, 2021.

[68] A. Javadpour, S. K. Abharian, and G. Wang, "Feature selection and intrusion detection in cloud environment based on machine learning algorithms," in *2017 IEEE international symposium on parallel and distributed processing with applications and 2017 IEEE international conference on ubiquitous computing and communications (ISPA/IUCC)*. IEEE, 2017, pp. 1417–1421.

Amir Javadpour obtained his MSc degree in Medical Information Technology Engineering from University of Tehran, Iran, in 2014. He received a PhD in Computer Science/Mathematics/Cybersecurity from Guangzhou University, China. In addition, he has published papers with his colleagues in highly ranked journals and several ranked conferences on several topics, including Cloud Computing, Software-Defined Networking (SDN), Big Data, Intrusion Detection Systems (IDS), and the Internet of Things (IoT), Moving Target Defence (MTD), Machine Learning (ML) and optimization algorithms. Additionally, he reviewed papers for several reputable venues such as IEEE Transactions on Cloud Computing, IEEE Transactions on Network Science and Engineering, ACM Transactions on Internet Technology, the Journal of Supercomputing, several journals of Springer and Elsevier, etc. He is a Technical Program Committee (TCP) Member of various conferences.

Forough Ja'fari is a Senior Researcher in cybersecurity and computer science. She received her Bachelor's degree from Sharif University of Technology and her Master's degree in Computer Network Engineering from Yazd University, Iran. She is a visiting scholar researcher at Guangzhou University, China. Cloud computing, software-defined Networking (SDN), cyber deception, Intrusion Detection Systems (IDS), Internet of Things (IoT), Moving Target Defence (MTD), and Machine Learning are some of her research interests. She is currently a Guest Editor (GE) of Cluster Computing (CLUS) Journal and a reviewer for several journals and conferences.

Bin Yang received his PhD in systems information science from Future University Hakodate, Japan, in 2015. He is a Professor at the School of Computer and Information Engineering, Chuzhou University, China, and a Senior Researcher with MOSA!C Lab, Finland. His research interests include unmanned aerial vehicle networks, cyber security and the Internet of Things. (Email: yangbinchi@gmail.com

Tarik Taleb Prof. Tarik Taleb is currently a full Professor at the Faculty of Electrical Engineering and Information Technology, Ruhr University Bochum, Germany, and a professor at the Center of Wireless Communications, The University of Oulu, Finland. He is the founder and director of the MOSA!C Lab (www.mosaic-lab.org). Between Oct. 2014 and Dec. 2021, he was an Associate Professor at the School of Electrical Engineering, Aalto University, Finland. Prior to that, he was working as a Senior Researcher and 3GPP Standards Expert at NEC Europe Ltd, Heidelberg, Germany. Before joining NEC and till Mar. 2009, he worked as an assistant professor at the Graduate School of Information Sciences, Tohoku University, Japan, in a lab fully funded by KDDI, the second-largest mobile operator in Japan. From Oct. 2005 till Mar. 2006, he worked as a research fellow at the Intelligent Cosmos Research Institute, Sendai, Japan. He received his B. E degree in Information Engineering with distinction, M.Sc. and Ph.D. degrees in Information Sciences from Tohoku Univ., in 2001, 2003, and 2005, respectively. Prof. Taleb's research interests lie in the field of telco cloud, network softwarization and network slicing, AI-based software-defined security, immersive communications, mobile multimedia streaming, and next-generation mobile networking. Prof. Taleb has also been directly engaged in developing and standardizing the Evolved Packet System as a member of 3GPP's System Architecture working group 2. Prof. Taleb served on the IEEE Communications Society Standardization Program Development Board. Prof. Taleb served as the general chair of the 2019 edition of the IEEE Wireless Communications and Networking Conference (WCNC'19) held in Marrakech, Morocco. He was the guest editor-in-chief of the IEEE JSAC Series on Network Softwarization and Enablers. He was on the editorial board of different IEEE journals and magazines. Till Dec. 2016, he served as chair of the Wireless Communications Technical Committee, the largest in IEEE ComSoC. Prof. Taleb is the recipient of the 2021 IEEE ComSoc Wireless Communications Technical Committee Recognition Award (Dec. 2021), the 2017 IEEE ComSoc Communications Software Technical Achievement Award (Dec. 2017) for his outstanding contributions to network softwarization. He is also the (co-) recipient of the 2017 IEEE Communications Society Fred W. Ellersick Prize (May 2017), the 2009 IEEE ComSoc Asia-Pacific Best Young Researcher award (Jun. 2009), the 2008 TELECOM System Technology Award from the Telecommunications Advancement Foundation (Mar. 2008), the 2007 Funai Foundation Science Promotion Award (Apr. 2007), the 2006 IEEE Computer Society Japan Chapter Young Author Award (Dec. 2006), the Niwa Yasujirou Memorial Award (Feb. 2005), and the Young Researcher's Encouragement Award from the Japan chapter of the IEEE Vehicular Technology Society (VTS) (Oct. 2003). Some of Prof. Taleb's research work has been awarded best paper awards at prestigious IEEE-flagged conferences.

Zhao Yue born in 1983, received the B.S. degree from the North China Institute of Science and Technology, Langfang, China, in 2006, and the Ph.D. degree from Southwest Jiaotong University, Chengdu, China, in 2012. He is currently a professorate senior engineer with the Science and Technology on Communication Security Laboratory, Chengdu. He is also the master student supervisor of School of Computing and Artificial Intelligence of Southwest Jiaotong University, School of Computer and Software Engineering of Xihua University, and School of Computer and Information Engineering of Chuzhou University. His research interests include wireless networks and information security. (Email: yuezhao@foxmail.com)

Chafika Benzaïd is currently a senior research fellow at University of Oulu, Finland. Between Nov. 2018 and Dec. 2021, she was senior researcher at Aalto University. Before that, she worked as an associate professor at University of Sciences and Technology Houari Boumediene (USTHB). She holds Engineer, Magister and "Doctorat ès Sciences" degrees from USTHB. Her research interests lie in the field of 5G/6G, SDN, Network Security, AI Security, and AI/ML for zero-touch security management. She is an ACM professional member.