electronics

MDPI

Article

Homomorphic Encryption and Network Coding in IoT Architectures: Advantages and Future Challenges

Goiuri Peralta [1,*], Raul G. Cid-Fuentes [2], Josu Bilbao [1] and Pedro M. Crespo [3]

[1] Information and Communication Technologies Area, Ikerlan Technology Research Centre, 20500 Arrasate-Mondragón, Spain
[2] Telefónica I+D, 28050 Madrid, Spain
[3] Electronics and Communications Department, University of Navarra (Tecnun), 20009 Donostia-San Sebastián, Spain
* Correspondence: gperalta@ikerlan.es

Received: 22 May 2019; Accepted: 24 July 2019; Published: 25 July 2019

Abstract: The introduction of the Internet of Things (IoT) is creating manifold new services and opportunities. This new technological trend enables the connection of a massive number of devices among them and with the Internet. The integration of IoT with cloud platforms also provides large storage and computing capabilities, enabling Big Data analytics and bidirectional communication between devices and users. Novel research directions are showing that Network Coding (NC) can increase the robustness and throughput of wireless networks, as well as that Homomorphic Encryption (HE) can be used to perform computations in the cloud while maintaining data privacy. In this paper, we overview the benefits of NC and HE along the entire vertical of cloud-based IoT architectures. By merging both technologies, the architecture may offer manifold advantages: First, it provides end-to-end data privacy, from end-devices to end-users. Second, sensitive data can be stored in public cloud platforms without concern about their privacy. In addition, clouds can perform advanced operations in a confidential manner, without the need to access actual data. Finally, latency can be reduced and the reliability of the system is increased. We show state-of-the-art works that demonstrate the role of both technologies in this type of architectures on a review basis. Furthermore, we describe the main characteristics of NC and HE and also discuss their benefits and limitations, as well as the emerging open challenges.

Keywords: cybersecurity; data privacy; homomorphic encryption; Industry 4.0; IoT; latency; multi-cloud; network coding; WSN

1. Introduction

The Internet of Things (IoT) is fast becoming a major asset in widespread areas of businesses and everyday life. From smart cities to wearables and to the so-called Industry 4.0, the IoT is transforming each of these sectors by generating new market opportunities and by enabling the creation of more intelligent applications [1–3]. According to a Gartner study, the number of things connected to the Internet is expected to increase to over 20 billion devices in 2020, which will generate a massive amount of data [4]. To create meaningful information for future decision making, all that information needs to be gathered and analyzed; thus, the cloud is becoming an essential part of the IoT ecosystem [5]. Cloud computing offers storage and computation capabilities required by IoT actors and enables real-time data analysis, which helps creating new scopes [6].

With this rapid growth of the IoT, some issues and concerns emerge. According to an International Data Corporation (IDC) survey [7], the top IoT inhibitors are security and privacy concerns. With more connected devices, security risks are incremented and, consequently, more protection is needed [8–10].

Particularly when actuators are remotely monitored, the required security level is even higher. Cybersecurity has become a hot topic, and cyberattacks suffered by large enterprises are well-known. Not only are these corporations target of these attacks, Small- and Medium-sized Enterprises (SMEs) are also potential victims [11]. The increasing number of real-time IoT applications, especially for healthcare and industry, also brings with them latency issues. They require an instantaneous response and, as such, it is crucial to minimize communication delays among smart devices [12].

As a solution to overcome privacy issues, a disruptive encryption scheme, Homomorphic Encryption (HE), is gaining momentum. Unlike conventional encryption algorithms such as Advanced Encryption Standard (AES) or Rivest–Shamir–Adleman (RSA), HE allows performing operations over encrypted data [13]. This attribute provides end-to-end IoT dataflow privacy. HE enables to securely store data in public clouds [14], where computations, such as Machine Learning (ML) predictions [15], can be performed without accessing user's data. However, this technique increases both computational cost and packet size, which implies an increment in network latency. A promising technology to address latency issues is Network Coding (NC) [16]. Its properties enable improving the robustness as well as reduce delays of diverse topologies [17]. In particular, it strengthens Wireless Sensor Networks (WSNs) communications [18] and it improves both data download speed and redundancy efficiency of distributed storage systems [19,20].

In this paper, we review the state-of-the-art regarding the multiple proposals that apply NC and HE over the reference IoT architecture in order to state the potential of the combination of both techniques over the entire vertical of such systems. The considered IoT architecture is presented in Figure 1. As shown, it is comprised of end-point devices responsible for collecting data, and a multi-cloud environment which stores and processes the received data. End-nodes and the multi-cloud environment are connected using an intermediate network. Finally, end-users can access data of end-point devices through the cloud services. On top of that, HE can provide end-to-end privacy, i.e., data are encrypted on the devices and decrypted at destination. These are transmitted along the WSN and the Internet to the multi-cloud environment, where advanced computations can be performed over the encrypted data, protecting user's privacy. The non-negligible increase in packet size and computational cost, and therefore, the increase in latency, is addressed by means of the implementation of NC throughout the architecture. Accordingly, not only can it be applied over the WSN, but it can also be used during the multi-cloud data upload, recovery, and acquisition.

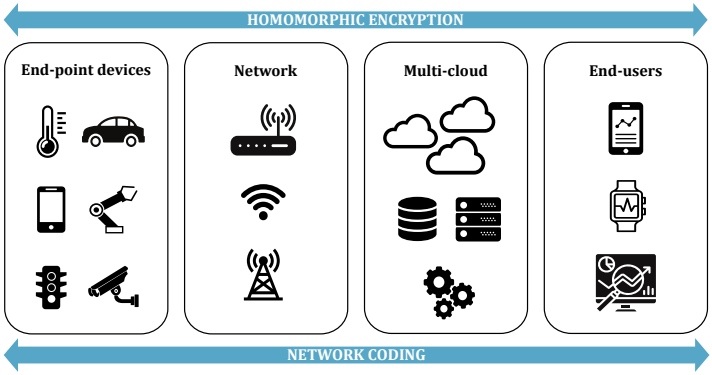

Figure 1. Network coding and homomorphic encryption over IoT architecture.

It can be said that this vision is backed by several research works, presented in Section 3, which are converging towards this overall architecture. The benefits of applying both NC and HE across the entire vertical of the architecture are manifold: it provides end-to-end data privacy to IoT applications, it allows end-users to leverage from public cloud computing services and storage without risking sensitive data, and it reduces latency. We describe the main characteristics and we analyze the state-of-the art related to both technologies. Further, we discuss its benefits and limitations and we provide future research directions.

The rest of the paper is organized as follows. In Section 2, we overview the main features and applicability of both NC and HE. In Section 3, we outlook the state-of-the-art regarding the works that apply these technologies over the described IoT architecture. In Section 4, we present the different challenges and issues as well as discuss the adoption of the approach. Finally, in Section 5, we report the final conclusions of the paper.

2. Background

This section briefly introduces the main characteristics and advantages of NC and HE, the two proposed technologies.

2.1. Network Coding

NC breaks with the traditional store-and-forward transmission model, enabling any network node not only to store and forward receiving packets but also to recombine them into coded packets, which will be decoded at destination [16]. One of the most widely used scheme is Random Linear Network Coding (RLNC), which linearly combines packets using randomly chosen coefficients from a finite field $\mathbb{F}_q$ of size 2^q [21]. The encoding operation of M packets can be described as follows:

$$p'_i = \sum_{j=1}^{M} c_{i,j} \cdot p_j \tag{1}$$

where $[p_1, p_2, \ldots, p_M]$ are the original packets, each p'_i is the resulting coded packet, and $c_{j,i} \in \mathbb{F}_q$ are the coding coefficients, where, for each p'_i, the corresponding set of coding coefficients $[c_{i,1}, c_{i,2}, \ldots, c_{i,M}]$ forms the coding vector.

RLNC exploits the characteristics of the broadcast nature of wireless medium [22–24], which facilitates node cooperation [25] to provide significant benefits in terms of communication robustness, stability, throughput, and latency [26].

One of the most relevant properties of RLNC is that it is rateless, i.e., the dependency on obtaining a particular packet is removed since the receiver only needs to get enough linearly independent packet combinations in order to recover the original data. Consequently, the coupon collector problem [27] is addressed. This makes RLNC a particularly valuable tool for distributed storage systems [19], such as P2P or multi-cloud environments. Additional data download time in highly loaded conditions can be reduced and it is possible to improve the storage efficiency in terms redundancy [28,29]. Furthermore, clouds are able to exchange data combinations between them [20], which improves the performance of data recovery and acquisition processes (recall Figure 2). Nevertheless, NC poses some security challenges, as it is particularly vulnerable to pollution attacks [30]. This critical problem can be solved by integrating HE techniques [31].

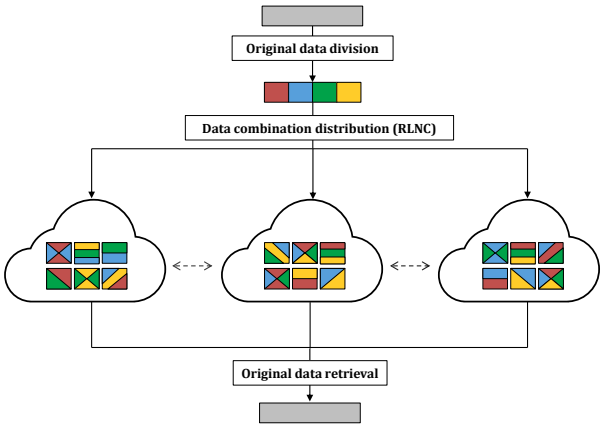

Figure 2. RLNC-based data combination distribution in a multi-cloud deployment.

2.2. Homomorphic Encryption

HE is a breakthrough encryption scheme that enables, due to its homomorphic property, computation over encrypted data and it is based on asymmetric or public key cryptography. It allows to carry out certain operations over the ciphertext that provides an encrypted result, which decrypted, is the same as that obtained if the operation was performed in plaintext [32,33]. The previous differentiates it from conventional encryption algorithms, such as AES, RSA, International Data Encryption Algorithm (IDEA), or Twofish. More precisely, an encryption scheme is called homomorphic for any operation if it supports the following:

$$Dec(k_s, Enc(k_p, m1) \diamond Enc(kp, m2)) = m1 \circ m2 \qquad \forall m1, m2 \in M \tag{2}$$

where *Enc* and *Dec* are the encryption and decryption functions, M is the set of all possible messages, k_p is the public key, k_s is the secret key, and $\diamond$ and $\circ$ are the group operation in the ciphertext and plaintext space, respectively.

There are three different algorithms depending on the operations they allow. Fully Homomorphic Encryption (FHE), created by Gentry [13], allows arbitrary computations on ciphertext. Somewhat Homomorphic Encryption (SHE) is a scheme that can evaluate functions of limited complexity or depth. Partially Homomorphic Encryption (PHE) is an algorithm limited in the type of operations it is able to perform on ciphertext [34,35].

HE can be a powerful tool for helping to preserve data privacy in a wide variety of applications. It is possible to securely store and process data in the cloud [36]. For example, it can be useful for remote electronic or Internet voting [37,38]. HE also opens the door to third parties, which can provide diverse computational services and statistical analysis, such as ML prediction [39,40], of sensitive data [14] in a confidential manner, e.g., in medical applications or fault detection of a sensorized machine. The latter is illustrated as a simple example in Figure 3.

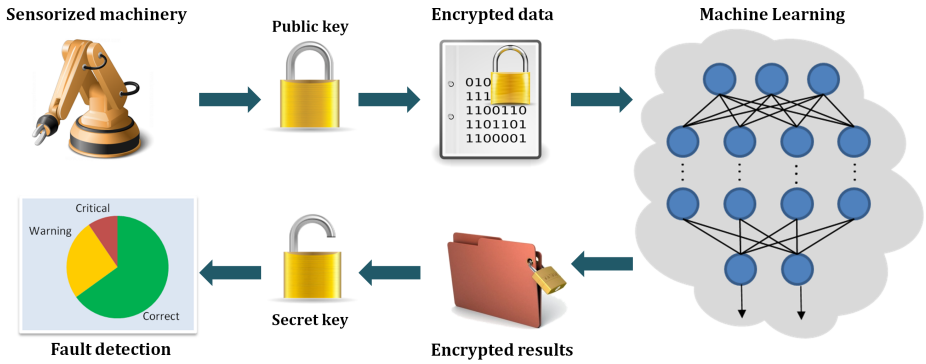

Figure 3. Machine learning over encrypted data for fault detection applications.

3. Related Work

In this section, we show the potential of the two previously introduced technologies over IoT architectures, both individually and combined, based on state-of-the-art work. As shown in Figure 4, the usual IoT scenarios are composed of a large number of devices, e.g., WSN, which send their data to the cloud, where they are processed for real-time or in-rest analysis, to be later visualized or remotely monitored by any client or end-user. Cloud computing provides high scalability and flexibility, Big Data management, and the possibility of performing advanced data analytics that allows obtaining meaningful information and valuable insights. Thus, it is becoming a cornerstone when it comes to Industry 4.0 and IoT applications, as it shown in the literature [41–43].

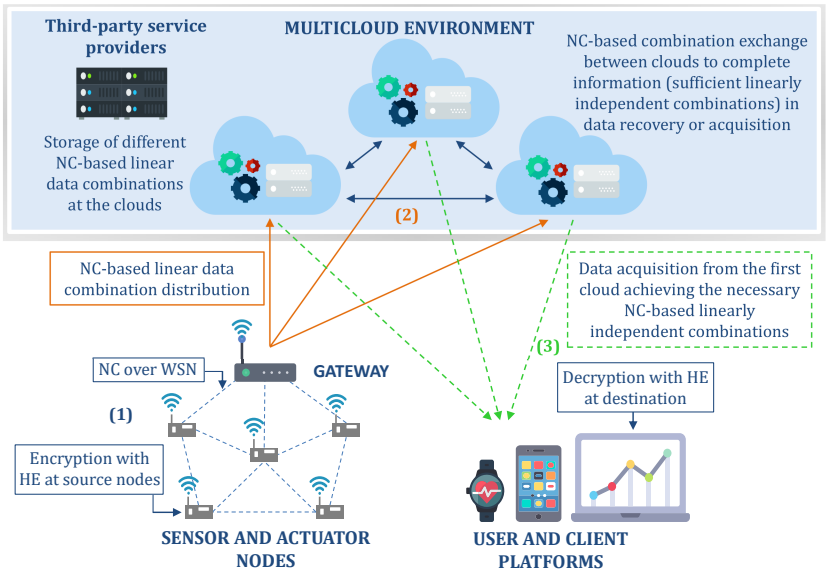

Figure 4. Role of NC and HE over the entire vertical of IoT architectures generally composed of: (1) a WSN; (2) a multi-cloud deployment; and (3) end-users.

The properties of NC are particularly beneficial for enhancing the robustness and reducing delays of WSN communications (Figure 4 (1)). The authors of [44] presented a cooperative NC-based transmission technique for spectrum and energy efficiency in Wireless Body Area Networks (WBANs) and showed the benefits in comparison to direct communication approach. Regarding Vehicular Ad-Hoc Networks (VANETs) and Internet of Vehicles (IoV), NC can improve the reliability of the transmission and can recover the original message in the event of disorder and loss of message, as it is shown in [45,46].

Regarding the cloud deployment (Figure 4 (2)), a multi-cloud strategy provides fault-tolerance and high-availability to the system, as it allows repairing lost data using redundancy, which can be more efficient with the use of NC [47,48]. NC can also be applied for distributing the data into the different clouds benefiting those with better conditions regarding price, download rate, or congestion, among others. In [49], for instance, data are distributed through the clouds, firstly to increase the system reliability and, secondly, to store the data depending on the price of the cloud resources and, thus, be able to reduce the storage cost. Data can also be distributed based on the download rate of each cloud in order to reduce the overall download time (Figure 4 (3)), as shown in [20].

As explained before, HE can ensure end-to-end privacy. Leveraging from its properties, sensors and gateways in WSNs are able to perform operations such as spatiotemporal correlation (Figure 4 (1)), which can be used to significantly reduce data traffic [50]. As shown in [51], HE can as well be an effective method for data aggregation in Vehicle-to-Grid (V2G) networks and since the data aggregation only requires additive operations, PHE is enough to satisfy the privacy preservation requirements. In cloud-based architectures, HE enables performing powerful data analytics in the cloud (Figure 4 (2)) and remote monitoring (Figure 4 (3)) while maintaining data privacy, for example, regarding sensitive medical data [52,53]. It also allows executing ML algorithms in a confidential manner [54]. For example, the authors of [40] presented a multi-key FHE scheme to apply deep learning over data stored in multiple third-party clouds without compromising the confidentiality.

Given the benefits that NC and HE provide to cloud-based IoT architectures individually, the potential advantages of combining such technologies have been analyzed in the literature. The authors of [55] showed the relationship between secure cloud storage and secure NC. For instance, homomorphic Message Authentication Code (MAC) schemes can be applied in order to avoid data and tag pollution attacks in RLNC [56]. The authors of [57] proposed a NC-based secure cloud storage protocol based on a homomorphic signature scheme, which supports public data auditing

and is resilient to data loss, pollution attack and repetitive attack. Conversely, in [58], the authors proposed a different solution for ensuring data and tag privacy. They present a distributed privacy preserving scheme for RLNC in Smart Grids. On the one hand, data of the packet are encrypted with a conventional encryption algorithm and, on the other hand, the tag of the packet, i.e., coefficient, is encrypted by a HE function. Leveraging from the homomorphic feature, forwarder nodes are able to recode the coefficients seamlessly without exposing either data or coefficients.

4. Benefits, Issues, and Open Challenges

While the IoT is transforming our everyday life actions and environments, it also creates some difficulties and threats. This section identifies and describes existing issues which can be addressed with the proposed technologies, as well as limitations and future challenges that will arise with their implementation, which can give directions to new research in this domain.

4.1. Security, Privacy and Trust

Security and privacy concerns are increasing with the exponential growth of IoT devices connected to the Internet, since the opportunities for attacking the network grow with the number of smart devices [10,59]. As such, one of the requirements in IoT environments is guaranteeing the trust of devices, which can become very challenging due to the heterogeneous and large-scale nature of these networks. To provide secure and robust systems, ensuring data privacy is essential. Data privacy can be compromised by illegitimate users or hackers who, through the access to IoT devices, could be able to obtain sensitive data or remotely control such devices. In addition, corporations such as banks or cloud providers, could easily access to the private data of their clients. Data can be threatened at any point, and thus, their authenticity, integrity, and privacy must be ensured, as well as the secure communication between all the involved parties.

Consequently, end-to-end security becomes critical, which can be addressed with the application of HE algorithms. Due to their properties, data only need to be decrypted at the end-user, even if they are required to perform operations over them. Moreover, NC would be protected against pollution attacks. Although the potential of HE is indisputable, it comes with a major disadvantage, its computational cost [32]. It requires significantly complex computations even for basic operations and the encryption process creates ciphertexts of enormous size [60]. This is a critical drawback, especially for IoT applications and protocols that usually employ resource-constrained devices.

In Figure 5, we provide an illustrative example that compares different state-of-the-art encryption mechanisms based on multiple metrics, divided into five levels. On the one hand, the privacy level is depicted in ascending order, i.e., from the lowest offered privacy level (1) to the highest (5). The metric that represents the possibility of performing operations on the encrypted data is also illustrated from 1 to 5, where 1 is the level in which less operations can be performed and 5, in contrast, in which any operation can be performed over the encrypted data. On the other hand, the metrics representing the ciphertext size created by the encryption algorithm, and also its complexity and the execution time, are depicted in descending order, i.e., from their highest level (5) to the lowest (1). Taking the complexity metric as an example, the complexity level decreases as we move towards the edge of the graph.

We show conventional algorithms, such as RSA or AES, as well as three HE techniques, namely, FHE, Fan and Vercauteren (FV), which is an SHE algorithm, and Paillier, which is equivalent to PHE. It can be observed that the size of the encrypted data, and both the complexity and execution time of the algorithm, increase with the use of more powerful techniques. Regarding the allowed operations, any operation can be performed if data are in plaintext. On the contrary, RSA/AES algorithms do not allow computing encrypted data. The use of HE techniques enables different operations depending on the algorithm. FHE allows any operation but is limited due to its complexity, FV can perform operations of limited depth, and Paillier only allows summing encrypted data. Regarding privacy, in the case we do not apply any data encryption, we offer no data protection. In contrast, the use of HE algorithms

provides end-to-end data privacy. Conventional algorithms, in turn, offer an intermediate protection since they require decrypting data for performing any operation over them.

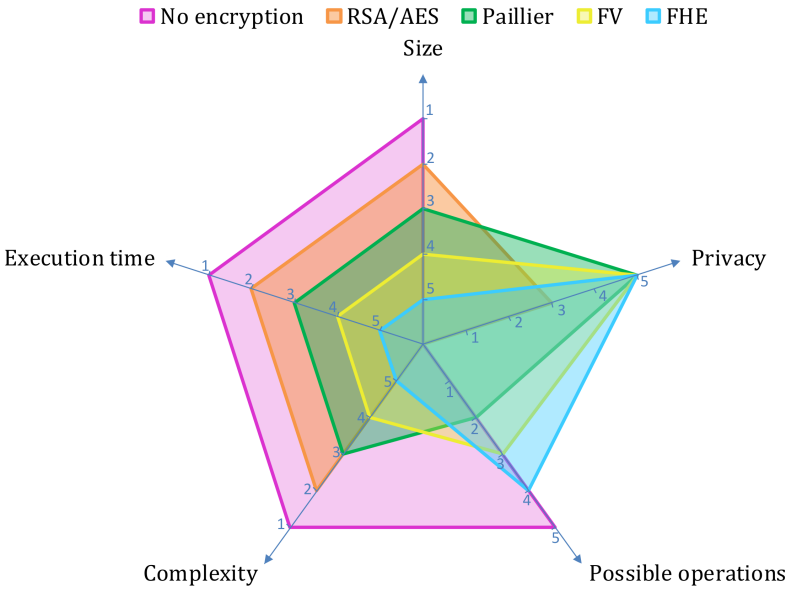

Figure 5. Comparison of different encryption techniques.

Thus, to make HE suitable to the constraints of IoT devices and applications, it will be needed to achieve more lightweight HE algorithms which require lower computational and communication costs, as well as complexity, for the performance of encrypted data operations.

4.2. Latency

In applications such as factory automation, where machines and systems of manufacturing lines are controlled in real time, or autonomous driving, where immediate vehicle-to-vehicle communications and detection of the surrounding environment are required, instant problem detection is critical to prevent major disasters. Even applications that do not rely on instantaneous feedback must react almost in real time [61]. These systems make decisions based on collected data, which means that these data must be collected, transmitted, and processed with very low latency.

NC helps reducing delays in congested networks as well as in highly loaded cloud deployments. However, the introduction of NC imposes some future challenges related to latency requirements of real-time applications. With NC, intermediate nodes must have the capability to perform operations fast enough to be able to recode and forward receiving data in real time to the next node. If this process is too complex, the use of IoT devices can generate extra delays since they have limited computational power. As such, it will require the development of simpler algorithms and coding schemes. Moreover, to optimize transmissions between intermediate nodes and reduce latencies of distributed systems while meeting the stringent demands of real-time scenarios, existing packet scheduling and routing algorithms may need to be reconsidered. If data are encrypted, intermediate nodes will need to decrypt receiving packets in order to be able to recombine them, which will introduce additional delays. The use of HE will play an enabling role in this regard, since data are only decrypted at destination and it releases the intermediate nodes from this task.

4.3. Reliability and Availability

IoT architectures require to remain available even when the whole system or part of it breaks down. Especially in industrial and health applications, robustness is an essential attribute [62]. The system should provide self-configurable services with the capacity of handling external perturbations

without affecting the application. Reliable communication among smart connected devices, gateways and cloud services or applications are also crucial for distributed environments where data are traveling between numerous different devices across the network. Continuous data availability also plays an essential role when it comes to meet the requirements of real-time applications. To satisfy application demands, cloud providers offer redundancy and backup options. Nonetheless, the entire infrastructure may fail.

As explained above, the reliability and availability of the architecture can be improved by uploading NC-based data combinations into a multi-cloud environment. Even if an entire cloud infrastructure fails, it will be possible to repair lost data thanks to additional data combinations placed in the remaining clouds. Therefore, dependencies on a single cloud vendor are reduced and the system autonomy increases. However, in an attempt to ensure reliability, data download speed can be compromised. Thus, it can be necessary to design new codes and distribution mechanisms capable of maintaining a trade-off between reliability and performance. Moreover, migrating data among different cloud platforms becomes a significant challenge too. First, it requires additional effort on data migration and distribution planning. Second, due to cloud vendor lock-in, there might emerge difficulties to move data from one cloud provider to another one.

4.4. Service Outage

Service continuity is as critical as system reliability or data availability for IoT applications, particularly for those whose data rely on third-party cloud providers. Interruptions suffered by services offered by important cloud vendors are not unusual. Only in 2017, well-known brands such as Amazon Web Services (AWS) or IBM suffered service disruptions which caused a big impact on a huge number of websites and applications. A service outage can lead to extremely serious consequences for businesses and final users. Besides the loss of critical data, a downtime of the application service may also occur. The negative effect of a cloud outage is also visible in businesses expenses [63].

Multi-cloud environments can help to provide service continuity. Applications can be transferred from one cloud vendor to any other in case of a service outage. However, this type of infrastructures poses additional challenges due to lack of standardization in cloud Service Level Agreements (SLAs) and interoperability. Each provider offers different platforms, tools, and analytics, which can hamper the execution of applications. The lack of integration between vendors may require the use of multiple management tools and interfaces. The development of open platforms and frameworks that integrate and migrate data and applications seamlessly across cloud vendors has become an essential demand.

4.5. Flexibility and Scalability

The exponential growth in the number of connected objects, with networks constantly increasing their size, makes scalability a key factor for IoT applications development [64]. Moreover, devices within this kind of distributed systems do not necessarily have to be permanently connected, indeed, they may be constantly linking and leaving the network. Thus, the implemented architecture should be flexible in order to adapt to changing environments from different use cases. Moreover, it has to fit application and user requirements. The introduction of a multi-cloud environment provides to the architecture the capability of handling big amounts of data as well as to manage network topology changes. In addition to a flexible distributed infrastructure, the applied coding mechanisms must also be scalable in order to adapt to the continuous environment variations.

4.6. Cost

The IoT generates massive amounts of data gathered and transmitted continuously by billions of interconnected things. To get valuable information for decision making, big data management and analysis are necessary, which require infrastructures with powerful storage and computing capabilities. These requirements, present in almost every IoT application, entail big investments in hardware and software resources to collect, manage, and process all these additional data.

The use of a multi-cloud deployment allows users to design strategies depending on offered services and prices, such as AWS Spot Instances [65]. Users can place their workloads in the cloud that better fits their demands, which can result in a cost reduction. This solution also allows leveraging from public clouds, which are more cost-effective than private ones since the infrastructure and maintenance costs are the responsibility of the provider. Nonetheless, cloud data storage, migration, and computation involve inherent costs. Thus, new solutions are needed to minimize those expenses. A possible answer to this issue can be to optimize NC schemes that use minimum amount of redundancy and recovery data to reduce associated costs.

Furthermore, the need for lightweight HE algorithms is not limited to latency. As it implies the transmission of larger packets, the communication cost is increased, in particular, if licensed frequency bands are used, which charge per transmitted byte.

4.7. Integration

The evolution of the IoT comes together with the need for interoperability. The large number of heterogeneous devices makes their communication and integration more challenging, which turns the interoperability into a critical issue [66]. Different services, frameworks and protocols applied in the IoT are represented in Figure 6. One of the problems created by this fragmentation is the inability to use common APIs or interfaces. It also poses big challenges when integrating devices from different manufacturers since they use communication protocols and standards which are not interoperable.

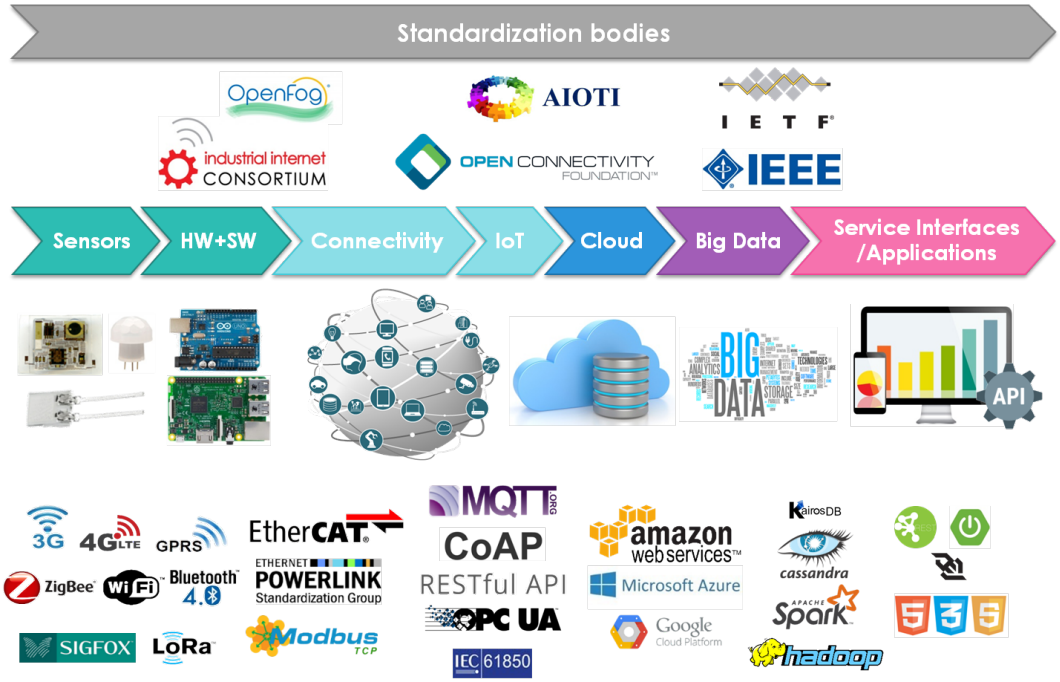

Figure 6. IoT landscape.

Integration is a substantial issue for the proposed architecture. The lack of interoperability among cloud vendors has been evidenced in previous sections. One of the demands in these scenarios is a platform that supports data, application and service migration between different cloud providers. The heterogeneous capabilities of IoT devices, regarding computational power and storage capacity, bring challenges to coding techniques which should be suitable for the diversity of objects within the network. The lack of interoperability remains a major barrier and can limit the optimal development of IoT applications.

4.8. IoT Communication Protocols

IoT devices are usually limited in battery, storage, and computing resources. Their constrained nature creates the need for communication protocols capable of handling these conditions. Thus, with the growth of IoT applications, novel protocols have emerged. Low Power WiFi [67] and Bluetooth Low Energy (BLE) [68] have been developed in order to meet these requirements. Furthermore, Low Power Wide Area Network (LPWAN) protocols [69] such as Sigfox, Lora, or Narrowband IoT enable long-range communications in power constrained devices. The use of new lightweight application layer protocols, such as MQTT [70] and CoAP [71], is rapidly growing, which, due to their characteristics, e.g., a minimum packet size, makes them ideal for IoT environments.

However, these IoT protocols pose some challenges regarding NC and HE. NC introduces a header overhead due to the coefficients used in the encoding process. Nevertheless, it is important to note that there is no need for a complete redesign, since the fields or headers reserved for future use of existing protocols can be adapted in order to integrate these coefficients. Regarding HE, it generates large encrypted data, which also complicates the introduction to the mentioned protocols. Thus, it becomes crucial to develop HE algorithms which produce smaller ciphertexts, in order to be applied in IoT lightweight protocols.

4.9. Discussion

One of the main advantages of the combination of both technologies is the end-to-end data privacy provided by the use of HE, as it removes the need for decrypting data until they reach the end user. This way, it enables private information sharing in multi-party scenarios among several data owners. It is worth stressing that third-party cloud computations are allowed while ensuring data privacy. However, HE implies greater computational costs due to its inherent complexity. As it generates large ciphertext, data traffic increases, which implies bigger transmission costs regarding both energy consumptions and charges per transmitted byte. Taking into account that IoT devices are mainly resource-constrained, and that IoT protocols are commonly lightweight protocols, it can be challenging to implement this encryption scheme. Nevertheless, HE is a field that generates big interests due to its tremendous privacy advantages and, therefore, it is rapidly advancing. Indeed, lighter algorithms are already emerging [72]. Moreover, SHE or PHE can be used in applications which require simpler operations, such as vote counting.

The implementation of NC throughout the architecture can reduce the entire system's latency. It optimizes the following processes: communications over the WSN, multi-cloud data upload and download, as well as data recovery and decoding. Thus, it improves the performance of congested wireless networks and multi-cloud deployments of high workloads. With NC, data reliability and availability are improved while less redundancy and fewer recovery data are required. Nonetheless, due to the reduced computational capabilities of the things, the introduction of complex NC schemes can lead to additional delays, which can be a drawback for real-time applications. Despite this, as mentioned above, these schemes can be adapted to existing IoT protocols.

Another advantage is that the architecture's security level is increased since data are distributed across multiple clouds and they are stored differently from the original form, which reduces the possibilities of suffering a malicious attack. The multi-cloud environment enhances the robustness regarding service outages and it provides the possibility of taking advantage of new computing services. Besides, it is capable of adapting to cloud and connectivity conditions. However, the migration of both data and application among different cloud providers brings interoperability problems due to lack of standardization. In addition, the heterogeneity of IoT remains a visible problem for the integration of different technologies across the architecture. Therefore, the research in this field becomes imperative in order to find new solutions that make possible to handle different technologies and platforms.

Although the presented techniques have certain limitations for a current implementation, we believe that it can provide great benefits for future IoT scenarios and applications, and we hope that it can be a source of inspiration for researchers as well as encourage them towards future research

directions. To summarize what we have previously discussed throughout this section regarding NC and HE, we outline in Table 1 the advantages and disadvantages of the proposed technologies.

Table 1. Overview of the benefits and drawbacks of NC and HE technologies.

	Advantages	**Disadvantages**
Homomorphic Encryption	• Provides end-to-end data privacy, allowing secure third-party cloud computations.	• Implies greater computational costs due to its inherent complexity.
	• Enables private information sharing in multi-party scenarios among several data owners.	• Generates large ciphertext, which poses challenges to introduce HE to IoT lightweight communication protocols.
	• SHE or PHE can be used in applications which require simpler operations.	• The size of the encrypted data also implies higher transmission costs.
Network Coding	• Improves the performance, e.g., latency and cost, of congested wireless networks and highly loaded multi-cloud deployments.	• Can lead to additional delays due to the introduction of a header overhead or complex recoding processes.
	• Enhances system reliability and availability requiring less redundancy and recovery data.	• Data download speed can be compromised in an attempt to ensure reliability.
	• Distributes and stores data differently from the original form, increasing the architecture security level.	• Makes necessary to design new codes and distribution mechanisms to maintain a trade-off between reliability and performance.

5. Conclusions

In this paper, we present a review of two technologies, NC and HE, aimed at enhancing the privacy as well as improving the communications and data distribution among the layers of IoT architectures. We overview the potential of the implementation of NC and HE across the entire architecture, where end-users will be able to manage and monitor the data sensed by a WSN making use of the multi-cloud deployment, responsible for storing and processing these data. Furthermore, we show the suitability of the combination of NC and HE by outlining the advantageous characteristics of both techniques and overviewing state-of-the-art works that show their applicability over the IoT architecture. We present different issues of the IoT that can be addressed with these techniques, such as privacy, reliability, and latency. Remaining challenges are also explained, which will require future research. Computational cost and lack of interoperability are some of the issues to highlight. Finally, we discuss the strengths and limitations of the application of both technologies over this type of architectures.

Author Contributions: Conceptualization, G.P. and R.G.C.-F.; Investigation, G.P.; Supervision, R.G.C.-F., J.B. and P.M.C.; Writing—original draft, G.P.; and Writing—review and editing, R.G.C.-F., J.B. and P.M.C.

Funding: This work was partially supported by the Basque Government through the Elkartek program (Grant agreement no. KK-2018/00115), the DIGITAL Elkartek program (Grant agreement no. KK-2019/00095), the H2020 research framework of the European Commission under the ELASTIC project (Grant agreement no. 825473), and the Spanish Ministry of Economy and Competitiveness through the CARMEN project (TEC2016-75067-C4-3-R) and the COMONSENS network (TEC2015-69648-REDC).

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Lee, J.; Bagheri, B.; Kao, H.A. A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. *Manuf. Lett.* **2015**, *3*, 18–23.
2. Lu, Y. Industry 4.0: A survey on technologies, applications and open research issues. *J. Ind. Inf. Integr.* **2017**, *6*, 1–10.
3. Wollschlaeger, M.; Sauter, T.; Jasperneite, J. The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0. *IEEE Ind. Electron. Mag.* **2017**, *11*, 17–27.

4. Gartner Inc. *Analysts to Explore the Value and Impact of IoT on Business*; Gartner Symposium/ITxpo: Barcelona, Spain, 2015.
5. Zhong, R.; Xu, X.; Klotz, E.; Newman, S. Intelligent Manufacturing in the Context of Industry 4.0: A Review. *Engineering* **2017**, *3*, 616–630.
6. Zhan, Z.H.; Liu, X.F.; Gong, Y.J.; Zhang, J.; Chung, H.H.; Li, Y. Cloud computing resource scheduling and a survey of its evolutionary approaches. *ACM Comput. Surv.* **2015**, *47*, 63.
7. IDC. *Worldwide and Regional Internet of Things 2014–2020 Forecast: A Virtuous Circle of Proven Value and Demand*; IDC: Framingham, MA, USA, 2014.
8. Sicari, S.; Rizzardi, A.; Grieco, L.; Coen-Porisini, A. Security, privacy and trust in Internet of things: The road ahead. *Comput. Netw.* **2015**, *76*, 146–164.
9. Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J. DDoS in the IoT: Mirai and other botnets. *Computer* **2017**, *50*, 80–84.
10. Yang, Y.; Wu, L.; Yin, G.; Li, L.; Zhao, H. A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet Things J.* **2017**, *4*, 1250–1258.
11. Alert Logic. *5 Cybersecurity Statistics Every Small Business Should Know in 2018*; Alert Logic: Houston, TX, USA, 2018.
12. Al-Falahy, N.; Alani, O. Technologies for 5G Networks: Challenges and Opportunities. *IT Prof.* **2017**, *19*, 12–20.
13. Gentry, C. A Fully Homomophic Encryption Scheme. Ph.D. Thesis, Standford University, Stanford, CA, USA, 2009.
14. Kumarage, H.; Khalil, I.; Alabdulatif, A.; Tari, Z.; Yi, X. Secure Data Analytics for Cloud-Integrated Internet of Things Applications. *IEEE Cloud Comput.* **2016**, *3*, 46–56.
15. Kim, M.; Song, Y.; Wang, S.; Xia, Y.; Jiang, X. Secure logistic regression based on homomorphic encryption: Design and evaluation. *JMIR Med. Inform.* **2018**, *6*, e19.
16. Ahlswede, R.; Cai, N.; Li, S.Y.; Yeung, R.W. Network information flow. *IEEE Trans. Inf. Theory* **2000**, *46*, 1204–1216.
17. Hansen, J.; Lucani, D.; Krigslund, J.; Médard, M.; Fitzek, F. Network coded software defined networking: Enabling 5G transmission and storage networks. *IEEE Commun. Mag.* **2015**, *53*, 100–107.
18. Fragouli, C.; Le Boudec, J.Y.; Widmer, J. Network coding: an instant primer. *ACM SIGCOMM Comput. Commun. Rev.* **2006**, *36*, 63–68.
19. Dimakis, A.G.; Godfrey, P.B.; Wu, Y.; Wainwright, M.J.; Ramchandran, K. Network coding for distributed storage systems. *IEEE Trans. Inf. Theory* **2010**, *56*, 4539–4551.
20. Sipos, M.; Fitzek, F.H.P.; Lucani, D.E.; Pedersen, M.V. Dynamic allocation and efficient distribution of data among multiple clouds using network coding. In Proceedings of the 2014 IEEE 3rd International Conference on Cloud Networking (CloudNet), Luxembourg, 8–10 October 2014; pp. 90–95.
21. Ho, T.; Medard, M.; Koetter, R.; Karger, D.R.; Effros, M.; Shi, J.; Leong, B. A Random Linear Network Coding Approach to Multicast. *IEEE Trans. Inf. Theory* **2006**, *52*, 4413–4430.
22. Katti, S.; Rahul, H.; Hu, W.; Katabi, D.; Medard, M.; Crowcroft, J. XORs in the air: Practical wireless network coding. *IEEE/ACM Trans. Netw.* **2008**, *16*, 497–510.
23. Xie, L.; Chong, P.; Ho, I.; Guan, Y. A survey of inter-flow network coding in wireless mesh networks with unicast traffic. *Comput. Netw.* **2015**, *91*, 738–751.
24. Liu, A.; Zhang, Q.; Li, Z.; Choi, Y.J.; Li, J.; Komuro, N. A green and reliable communication modeling for industrial internet of things. *Comput. Electr. Eng.* **2017**, *58*, 364–381.
25. Hernández Marcano, N.; Heide, J.; Lucani, D.; Fitzek, F. Throughput, energy and overhead of multicast device-to-device communications with network-coded cooperation. *Trans. Emerg. Telecommun. Technol.* **2017**, *28*, e3011.
26. Szabo, D.; Gulyas, A.; Fitzek, F.H.P.; Lucani, D.E. Towards the Tactile Internet: Decreasing Communication Latency with Network Coding and Software Defined Networking. In Proceedings of the European Wireless 2015: 21th European Wireless Conference, Budapest, Hungary, 20–22 May 2015; pp. 1–6.
27. Fragouli, C.; Soljanin, E. Network coding applications. *Found. Trends® Netw.* **2008**, *2*, 135–269.
28. Chen, H.C.H.; Hu, Y.; Lee, P.P.C.; Tang, Y. NCCloud: A Network-Coding-Based Storage System in a Cloud-of-Clouds. *IEEE Trans. Comput.* **2014**, *63*, 31–44.

29. Saleh, B.; Qiu, D. Performance Analysis of Network-Coding-Based P2P Live Streaming Systems. *IEEE/ACM Trans. Netw.* **2016**, *24*, 2140–2153.
30. Talooki, V.N.; Bassoli, R.; Lucani, D.E.; Rodriguez, J.; Fitzek, F.H.; Marques, H.; Tafazolli, R. Security concerns and countermeasures in network coding based communication systems: A survey. *Comput. Netw.* **2015**, *83*, 422–445.
31. Yao, S.; Chen, J.; Du, R.; Deng, L.; Wang, C. A survey of security network coding toward various attacks. In Proceedings of the 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Beijing, China, 24–26 September 2014; pp. 252–259.
32. Acar, A.; Aksu, H.; Uluagac, A.; Conti, M. A survey on homomorphic encryption schemes: Theory and implementation. *ACM Comput. Surv.* **2018**, *51*, 79.
33. Mohan, M.; Devi, M.K.K.; Prakash, V.J. Homomorphic encryption-state of the art. In Proceedings of the 2017 International Conference on Intelligent Computing and Control (I2C2), Coimbatore, Tamil Nadu, India, 23–24 June 2017; pp. 1–6.
34. Naehrig, M.; Lauter, K.; Vaikuntanathan, V. Can homomorphic encryption be practical? In Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop, Chicago, IL, USA, 21 October 2011; pp. 113–124.
35. Wang, L.; Li, J.; Ahmad, H. Challenges of fully homomorphic encryptions for the internet of things. *IEICE Trans. Inf. Syst.* **2016**, *E99D*, 1982–1990.
36. Shafagh, H.; Hithnawi, A.; Burkhalter, L.; Fischli, P.; Duquennoy, S. Secure Sharing of Partially Homomorphic Encrypted IoT Data. In Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems, Delft, The Netherlands, 6–8 November 2017.
37. Yi, X.; Okamoto, E. Practical Internet voting system. *J. Netw. Comput. Appl.* **2013**, *36*, 378–387.
38. Will, M.A.; Nicholson, B.; Tiehuis, M.; Ko, R.K.L. Secure Voting in the Cloud Using Homomorphic Encryption and Mobile Agents. In Proceedings of the 2015 International Conference on Cloud Computing Research and Innovation (ICCCRI), Singapore, 26–27 October 2015; pp. 173–184.
39. Graepel, T.; Lauter, K.; Naehrig, M. ML Confidential: Machine Learning on Encrypted Data. In *Information Security and Cryptology—ICISC 2012*; Kwon, T., Lee, M.K., Kwon, D., Eds.; Springer: Berlin/Heidelberg, Germany, 2013; pp. 1–21.
40. Li, P.; Li, J.; Huang, Z.; Li, T.; Gao, C.Z.; Yiu, S.M.; Chen, K. Multi-key privacy-preserving deep learning in cloud computing. *Future Gener. Comput. Syst.* **2017**, *74*, 76–85.
41. Georgakopoulos, D.; Jayaraman, P.; Fazia, M.; Villari, M.; Ranjan, R. Internet of Things and Edge Cloud Computing Roadmap for Manufacturing. *IEEE Cloud Comput.* **2016**, *3*, 66–73.
42. Fisher, O.; Watson, N.; Porcu, L.; Bacon, D.; Rigley, M.; Gomes, R. Cloud manufacturing as a sustainable process manufacturing route. *J. Manuf. Syst.* **2018**, *47*, 53–68.
43. Qu, T.; Lei, S.; Wang, Z.; Nie, D.; Chen, X.; Huang, G. IoT-based real-time production logistics synchronization system under smart cloud manufacturing. *Int. J. Adv. Manuf. Technol.* **2016**, *84*, 147–164.
44. Talha, S.; Ahmad, R.; Kiani, A.K.; Alam, M.M. Network Coding for Energy Efficient Transmission in Wireless Body Area Networks. *Procedia Comput. Sci.* **2017**, *113*, 435–440.
45. Muhammad, S.J.; Zhang, S.; Dyo, V. Network coding for reliable safety message communication in vehicular Ad-Hoc networks: A review. In Proceedings of the 2015 Fourth International Conference on Future Generation Communication Technology (FGCT), Luton, UK, 29–31 July 2015; pp. 1–6.
46. Wang, Z.; Li, J.; Fang, M.; Li, Y.; Feng, B. A Reliable Routing Algorithm with Network Coding in Internet of Vehicles. *China Commun.* **2017**, *14*, 174–184.
47. Arya, N.; Rout, R.R.; Lingam, G. Network Coding Based Multiple Fault Tolerance Scheme in P2P Cloud Storage System. In Proceedings of the 2018 IEEE 13th International Conference on Industrial and Information Systems (ICIIS), Rupnagar, India, 1–2 December 2018; pp. 223–228.
48. Mao, B.; Wu, S.; Jiang, H. Improving Storage Availability in Cloud-of-Clouds with Hybrid Redundant Data Distribution. In Proceedings of the 2015 IEEE International Parallel and Distributed Processing Symposium, Hyderabad, India, 25–29 May 2015; pp. 633–642.
49. Peralta, G.; Garrido, P.; Bilbao, J.; Agüero, R.; Crespo, P. On the combination of multi-cloud and network coding for cost-efficient storage in industrial applications. *Sensors* **2019**, *19*, 1673.
50. Vuran, M.C.; Akan, Ö.B.; Akyildiz, I.F. Spatio-temporal correlation: theory and applications for wireless sensor networks. *Comput. Netw.* **2004**, *45*, 245–259.

51. Han, W.; Xiao, Y. Privacy preservation for V2G networks in smart grid: A survey. *Comput. Commun.* **2016**, *91–92*, 17–28.
52. Kocabas, O.; Soyata, T. Utilizing Homomorphic Encryption to Implement Secure and Private Medical Cloud Computing. In Proceedings of the 2015 IEEE 8th International Conference on Cloud Computing, New York, NY, USA, 27 June–2 July 2015; pp. 540–547.
53. Hussein, A.F.; Kumar N, A.; Burbano-Fernandez, M.; Ramírez-González, G.; Abdulhay, E.; De Albuquerque, V.H.C. An Automated Remote Cloud-Based Heart Rate Variability Monitoring System. *IEEE Access* **2018**, *6*, 77055–77064.
54. Sun, X.; Zhang, P.; Liu, J.K.; Yu, J.; Xie, W. Private machine learning classification based on fully homomorphic encryption. *IEEE Trans. Emerg. Top. Comput.* **2019**, doi:10.1109/TETC.2018.2794611.
55. Chen, F.; Xiang, T.; Yang, Y.; Chow, S.S.M. Secure Cloud Storage Meets with Secure Network Coding. *IEEE Trans. Comput.* **2016**, *65*, 1936–1948.
56. Esfahani, A.; Mantas, G.; Rodriguez, J.; Neves, J. An efficient homomorphic MAC-based scheme against data and tag pollution attacks in network coding-enabled wireless networks. *Int. J. Inf. Secur.* **2017**, *16*, 627–639.
57. Liu, X.; Huang, J.; Zong, G. Public Auditing for Network Coding Based Secure Cloud Storage. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security And Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 713–720.
58. He, S.; Zeng, W.; Xie, K.; Yang, H.; Lai, M.; Su, X. PPNC: Privacy preserving scheme for random linear network coding in smart grid. *KSII Trans. Internet Inf. Syst.* **2017**, *11*, 1510–1532.
59. Sonami M. *Connect the Dots: IoT Security Risks in an Increasingly Connected World*; IBM: Hong Kong, China, 2018.
60. Zhou, J.; Cao, Z.; Dong, X.; Vasilakos, A.V. Security and Privacy for Cloud-Based IoT: Challenges. *IEEE Commun. Mag.* **2017**, *55*, 26–33.
61. Nokia. *5G Connected Industry*; Technical Report; Nokia: Espoo, Finland, 2018.
62. Yan, J.; Meng, Y.; Lu, L.; Li, L. Industrial Big Data in an Industry 4.0 Environment: Challenges, Schemes, and Applications for Predictive Maintenance. *IEEE Access* **2017**, *5*, 23484–23491.
63. Ponemon Institute. *Cost of Data Center Outages*; Technical Report; Ponemon Institute: MI, USA, 2016.
64. Naito, K. A survey on the internet-of-things: Standards, challenges and future prospects. *J. Inf. Process.* **2017**, *25*, 23–31.
65. Amazon Web Services, Inc. Amazon Elastic Compute Cloud: User Guide for Linux Instances. 2019. Available online: https://docs.amazonaws.cn/en_us/AWSEC2/latest/UserGuide/ec2-ug.pdf (accessed on 22 May 2019).
66. Noura, M.; Atiquzzaman, M.; Gaedke, M. Interoperability in Internet of Things: Taxonomies and Open Challenges. *Mobile Netw. Appl.* **2019**, *24*, 796–809.
67. IEEE. *IEEE 802.11ah-2016*; Technical Report; IEEE: Piscataway, NJ, USA, 2017.
68. Bluetooth. *Bluetooth Low Energy (BLE)*. Available online: https://www.bluetooth.com/bluetooth-technology/radio-versions/ (accessed on 22 May 2019)
69. IETF Tools. RFC 8376—Low-Power Wide Area Network (LPWAN) Overview. 2018. Available online: https://tools.ietf.org/html/rfc8376 (accessed on 22 May 2019).
70. OASIS. MQTT Version 3.1.1. 2014. Available online: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.pdf (accessed on 22 May 2019).
71. IETF Tools. RFC 7252—The Constrained Application Protocol (CoAP). 2014. Available online: https://tools.ietf.org/html/rfc7252 (accessed on 22 May 2019).
72. Lepoint, T.; Naehrig, M. A comparison of the homomorphic encryption schemes FV and YASHE. In *International Conference on Cryptology in Africa*; Springer: Cham, Switzerland, 2014; pp. 318–335.