A SYSTEMATIC REVIEW OF HOMOMORPHIC ENCRYPTION TECHNOLOGIES IN SUSTAINABLE DEVELOPMENT

Jude Nwoji. O[1], Abdulkadir Maccido Ahmad[2] Abdulhakeem Ishola[3] , Abdullahi Abubakar[4], Abdullaziz Abdullahi Bena.[5]

[1,&2]Department of Computer Engineering, Waziri Umaru Federal polytechnic BK. Kebbi State.
[3,4 &5]Department of Computer Science, Waziri Umaru Federal polytechnic BK. Kebbi State.
judycharles222@gmail.com; amprehmaccido@yahoo.com;abduljedo@yahoo.com; abafo22@gmail.com;

Abstract

With the emergence of encryption technology, the Information and Communication Technology (ICT) was gaze at bringing immense opportunities to leverage digitalization and technological innovation to meet up with so many stainable development challenges including the anti-corruption war, as well as a norm for technological innovations to leverage new dimension of vulnerability in the area of security, as the result of that, so many researchers have shown interest to embark on a quest to extend encryption technology to so many cloud services predominantly use in the area of industrial and private consumption. As most industries and public and private sectors embrace the use of cloud services, this is why the issue of confidentiality becomes an even more complicated issue. Numerous efforts were put in place to seek the solutions to confidentiality problems. However, there are persistence challenges due to the nature of convention security methods in encryption techniques. In this paper, we present a systematic review of research papers in the field of homomorphic encryption related to securing clients' data on clouds. The homomorphic encryption technique emerged as a possible solution to secure data on clouds, it allows some search and manipulation operations without proper decryption. The paper uses the PRISMA checklist to review studies retrieved from various resources. It also pinpointed from the reviewed papers that the security of data in big data and cloud computing has been given more attention as they are the most used technologies in technological Innovation for Sustainable Development in 21 century. Results of the evaluation through PRISMA showed that a majority of research articles discussed the potential use and application of Homomorphic Encryption as a solution to the growing industrial development, particularly on cloud service demands which are rounded with the issue of data security.

Keywords: Homomorphic Encryption, Cloud Computing, SDG

Introduction

In this digital age, lifestyles and the global immediacy, security is the key concern in dealing with information and communication technology (ICT), According to (Gartner, 2022), more than $1.3 trillion in enterprise IT spending is at stake from the shift to cloud, growing to almost $1.8 trillion in 2025. Ongoing disruption to IT markets by cloud will be amplified by the introduction of new technologies, including distributed cloud. Many will further blur the lines between traditional and cloud offerings. Enterprise adoption of distributed cloud has the potential to further accelerate cloud shift because it brings public cloud services into domains that have primarily been non-cloud, expanding the addressable market. as technology deals with vast data which need higher medium to house it, this necessitate the need and support of third-party to render such service in the name of cloud computing services. There as the issue of processing such data house by the third-party becomes an issue due to the nature at which it process. Platonically, the predominant Encryption approaches used do not allow processing on encrypted data in the state of cipher whereas it must be converted to its original form (plaintext). Meanwhile, homomorphic encryption allows computation on encrypted data (on its cipher form) and provides result in encrypted form. Homomorphic encryption not only allows the processing of encrypted data but also preserves privacy in the process.

The relationship between ICT development and human development has received wider attention of so many scholars. So many researches have shown that ICT development can enhance developments in human life when objectives are clearly met this is to say when it is clearly secured. It was reveled that ICT have so many impact on economic growth, it at all it could be properly utilized(Ramasubramanian et al., 2021). According to (Rahu, 2020), it was predicted that with the exponential increase in used of Information and communications Technology (ICT) over the last five years, the computing devices would be among the fifth most used utility on each (after water, electricity, gas, and telephony). Which necessitate the adoption of cloud services for effective utilization of ICT. So many

Enterprises adopt for Big-data processing and storage. Cloud computing is a cutting-edge method of storing large amounts of data also allows users to have unlimited access to it as it involve online file storage, webmail, social networking platforms, and online business applications (Thabit et al., 2022). The security threats are increasing as the demand for cloud services increases as the a third party mostly involved as a result, data protection in the cloud is the primary issue.

Cloud Computing

Cloud computing is a term used to describe the technology of delivering computing services which includes both hardware and software services over the internet (cloud). These services categorized into:

- ✓ Platform as a Service (PaaS)
- ✓ Software as a Service (SaaS)
- ✓ Infrastructure as a Service (IaaS).

Part of it contribution to economical development, cloud computing provinces necessary services to an industries in lieu of such organization or company to own their computing infrastructure or data centres, companies can rent access to the computing ferocities of the services providers. The company also could benefit from saving the cost of maintenance of such facilities as it repose to the services provider(Ranger, 2022).

Accoding to Tech analyst Gartner predicts that business process services and system infrastructure markets will have shifted to the cloud by 2025, up from 41% in 2022. As in Figure 2.1 below.

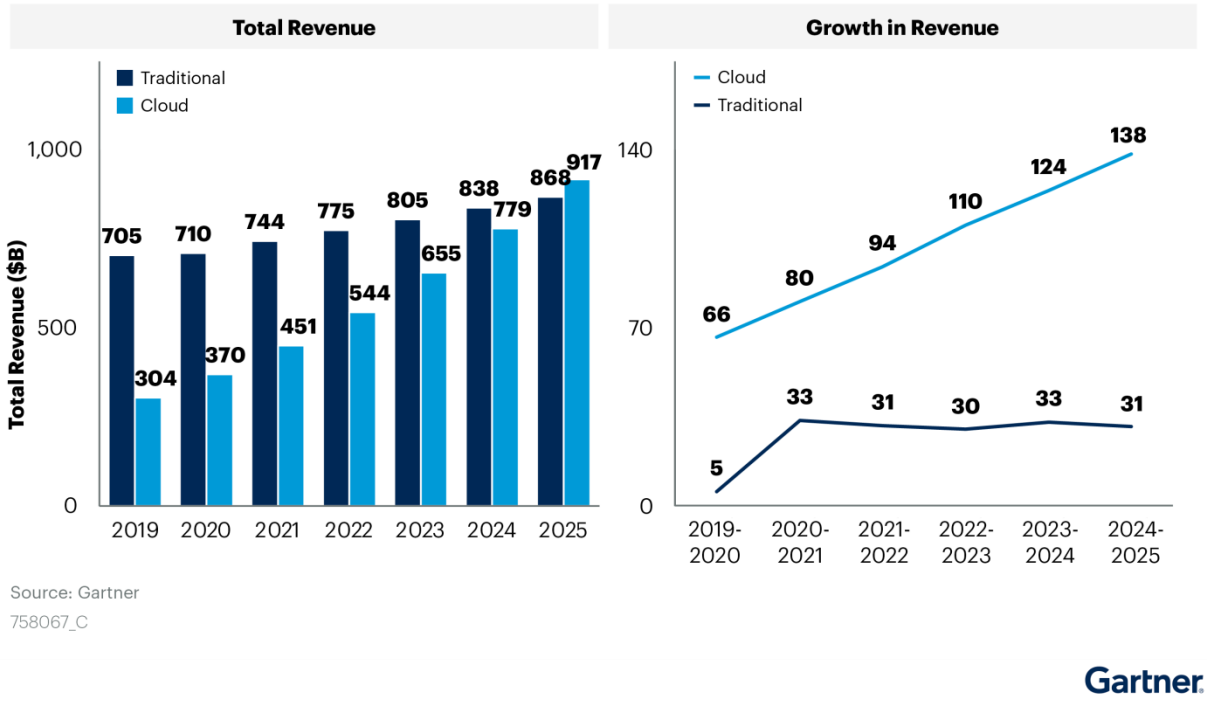


Figure 2.1 Sizing Cloud shift, worldwide, 2019-2025: Source: https://www.gartner.com

It estimates that almost two-thirds of spending on application software will be via cloud computing, up from 57.7% in 2022. "In 2022, more than $1.3 trillion in enterprise IT spending is at stake from the shift to cloud, growing to almost $1.8 trillion in 2025, according to Gartner. Ongoing disruption to IT markets by cloud will be amplified by the introduction of new technologies, including distributed cloud. Many will further blur the lines between traditional and cloud offerings".

2.1 CLOUD COMPUTING SECURITY

Security of data in clouds faces number of challenges as it is characterized by flexibility and elasticity. From the research conducted by Enterprise panel of International Data Corporation (IDC) shows that so many companies been faced by different security challenges in dealing with cloud computing technology, the chart in figure2.2 shows the

parameters along with the percentage of issues that has been faced by different companies and organizations in adopting cloud computing technology.



Figure 2.2 Cloud Computing Security Issues

The above-mentioned security issues is like a hand shake between the cloud user and cloud provider for maintaining trust between them and ensuring the security in all interconnecting scenarios(Thabit et al., 2022). Cloud security is one of the most difficult and promising computer technologies which provide various communications to the user. In other words, cloud data security is another advancing pattern in data innovation where more security for data is essential. Traditionally, the data centers maintain and control the data but are insecure. They are prone to various types of attacks. Hence, there must be an effective mechanism for providing secure transformation and privacy-preserving of data in the servers. An immense amount of information is shared over the system by utilizing the various services and lots of information is stored in the cloud server. Various schemes of encryption were adopted for protecting and securing the information in the cloud(Thabit et al., 2022).

Cryptography in Cloud security

Cryptography is considered to be one of the safety measures for secure communications. To bridge the security gap, the most widely used technique is the encryption of remotely stored data. The cloud environment keeps on changing rapidly, and this poses a fundamental challenge for outsourcing computation(Baharuddin et al., 2021). Hence, it has created an impetus for many computing researchers to improve available symmetry/asymmetry algorithms.

The encryption and decryption technologies are available in three types: symmetric, asymmetric, hybrid algorithms which may be utilized in cloud storage to encrypt and decode data(Satamraju & Malarkodi, 2021). Symmetric encryption is a cryptographic technique in which the sender and recipient share a single public key to encrypt and decrypt the data. The standard symmetric algorithm used for data cryptography is the Data Encryption Standard (D.E.S.), the Advanced Encryption Stan-dard (A.E.S.)(Gahi et al., 2015).

Asymmetric encryption consists of two distinct keys: the encryption used the public key and decryption used the private key only the authorized receiver able to decode the message using the private key. An asymmetrical algorithm example used for data cryptography is the R.S.A. algorithm.

Hybrid encryption is a kind of encryption that integrates multiple or more encryption algorithms, using a combination of symmetric and asymmetric encryption to take use of each type's capabilities. This hybrid cryptography method was created in order to provide an efficient and secure encryption algorithm capable of encrypting and decrypting data fast and safely(Orobosade et al., 2020) . Since the advent of the Data Encryption Standard (DES), lightweight block ciphers have played an increasing role in cryptology.

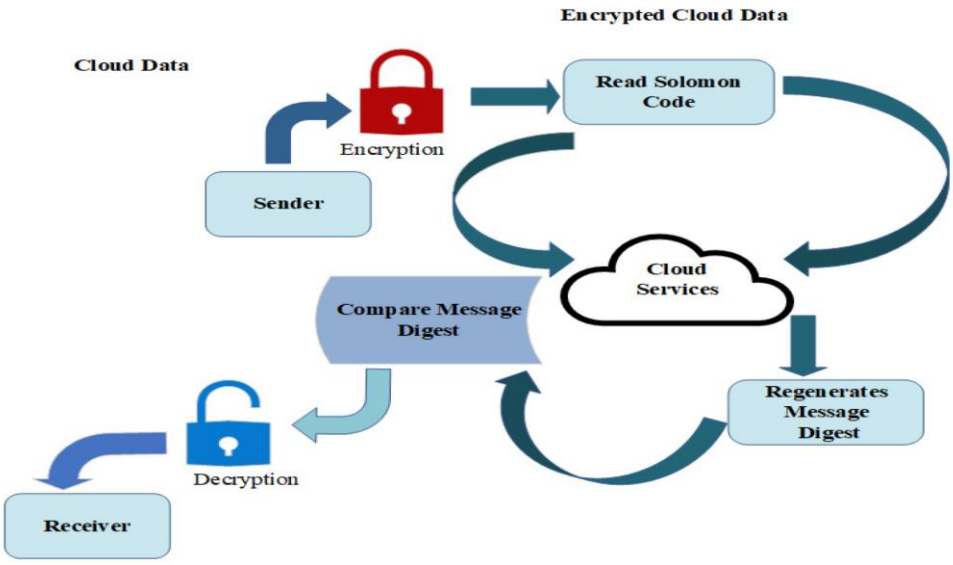


Figure 2.3 Hybrid AES-ECC Model for the Security of Data over Cloud Storage framework

Materials and methods

The Methodology adopted in this paper was "systematic review methodology". The systematic review methodology is a protocol driven comprehensive review method where relevant data for a given topic would be gathered and synthesis, it is typically performed by experienced methodologists with the input of domain experts. The first step to conduct a systematic review is to formulate specific key questions can be defined as a method in which a predefined research question is answered on the basis of empirical evidence that is gathered and summarized according to the specified eligibility criteria. The adopted methodology it apt to this research as the paper try to investigate the pertinence of Homomorphic Encryption techniques in tacking issue of could data vulnerability. The chosen methodology was found apt to this paper as it allowed in systematic collection, evaluation and summarization of current knowledge regarding Homomorphic Encryption. This study follows the systematic review was accomplished by following the following steps:

Step 1: Formulation of problem statement: The problem at hand was that there was no systematic review that clearly addresses the sustainable development in respect to Homomorphic Encryption scheme.

Step 2: Performing search: The relevant articles were searched from different databases by the use of keywords Homomorphic Encryption in combination with Technologies, as well as cloud computing.

Step 3: Data extraction: From the research articles collected, relevant data were extracted and documented.

Step 4: Data synthesis: This step involved the presentation of data to evaluate the overall outcomes by the use of statistical methods (meta-analysis).

Step 6: Results: Finally, All the findings that satisfy the research objective was presented in the results section.

Description of PRISMA Framework

PRISMA is an as an evidence based framework used for systematic reviews and meta-analyses. PRISMA framework provides researchers with an ability to conduct a critical search and selection of relevant data form published articles. PRISMA is an effective framework in conducting critical assessment of published articles.

The steps involved in the PRISMA framework were applied as follows:

- **Preparation:** The PRISMA checklist explaining the entire framework was downloaded and filled up based on topic at hand, see Figure. 3.1
- **Performing the search:** The search strategies was performed by searching for Homomorphic Encryption articles and other relevant articles from the subsequent database while making use with Boolean operators (AND) and (OR) as and when necessary.

- **Eliminating duplication:** After retrieving 350 articles, it was evaluated and filtered out in terms of duplication of concepts, principles, technologies and applications.
- **Article screening:** The titles and abstracts of the remaining articles after elimination were filtered using inclusion and exclusion criteria to identify the most for our systematic review.

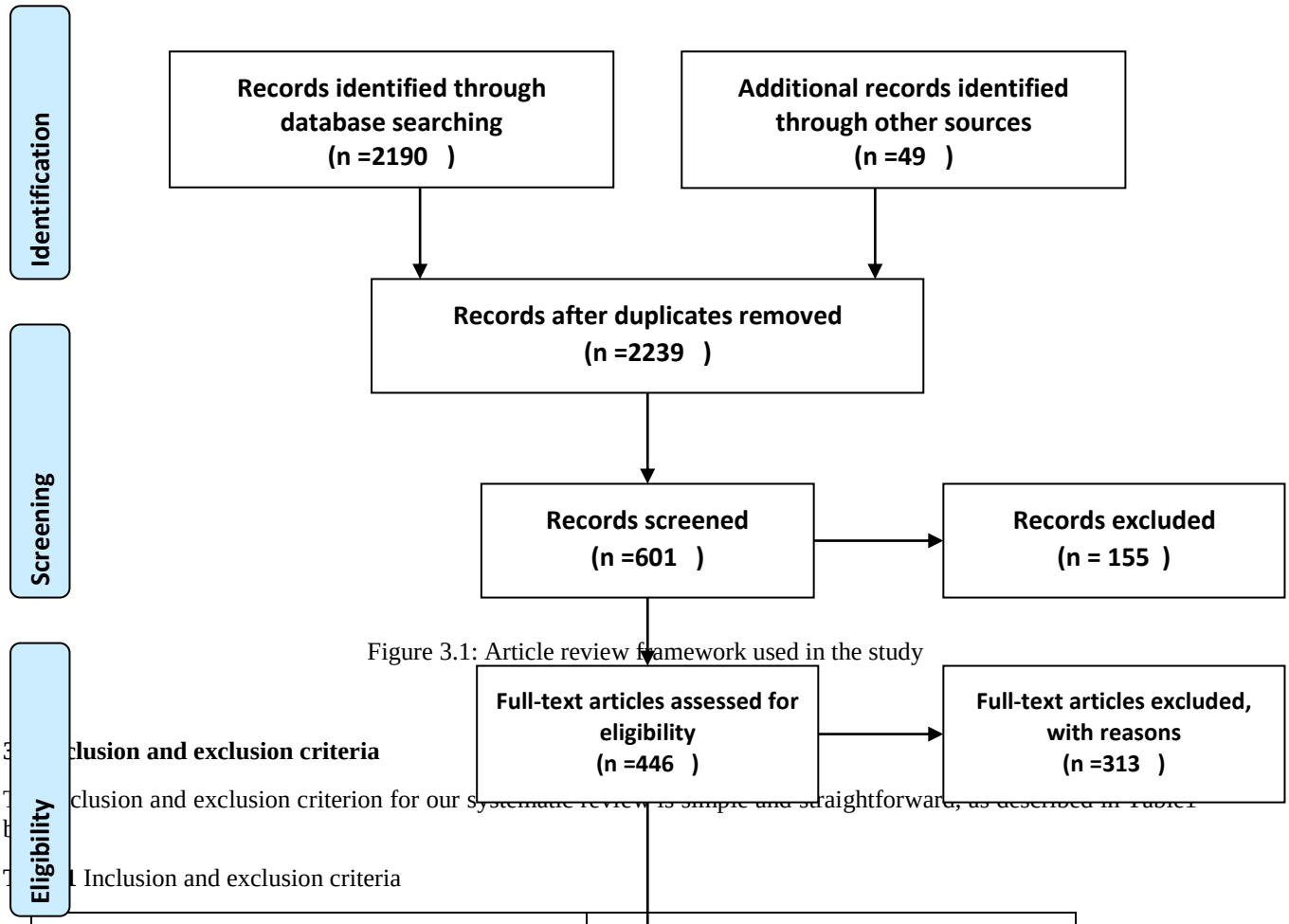


Figure 3.1: Article review framework used in the study

3. clusion and exclusion criteria

T clusion and exclusion criterion for our systematic review is simple and straightforward, as described in Table1 b

T 1 Inclusion and exclusion criteria

Inclusion criteria	Exclusion criteria
ticles published in renown journals as well as ademic databases such as IEEE, ScienceDirect, ringer, and Google Scholar	Non-English Articles
ticles publishedon or after 2018	d on Homomorphic Encryption in non cloud computing aspect
Articles should be written in English	The articles keywords include Fully Homomorphic Encryption without considering it in their research paper

Articles containing a discussion or evaluation of the keywords, including Homomorphic Encryption AND (Big Data) OR (Big Data Security) OR (Cloud Computing) OR (Cloud Computing technology).	

Results and discussion

There are only 50 articles that metup with the inclusion criteria, the criteria gives emphases on a search word "Homomorphic" in both Abstract and title of the collected articles. 44 documents consisted of 5 feature articles, 2 general information articles, 33 journal articles, and 1 journal article that doubled as a feature article. Most of the articles were published in india followed by Hong Kong, London and New York as well Heidel-berg. Regarding the distribution of the articles based on the year of publication, the year 2021 recorded the highest number of published papers (16) while only 5 papers have been published in 2018. As Fig. 3 shows, in 2019 and 2020, only 17 articles were published about homomorphic encryption techniques. The distribution of reviewed articles by pace of publication. Figure 3.2 The distribution of the number of articles published on holistic encryption techniques and or any related cloud data security technology. The development of Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing is attempt conducted by Thabit and Alhomdy in 2022. Other major developments noted from the article include development of FHE scheme based on Ap-proximate Greatest Common Divisor (AGCD) algorithm, reduction of the size of public-key, introduction of module switching to further reduce the size of public key, inclusion of batching and introduction of permutation, and reduction of Learning with Errors (LWE) to AGCD.

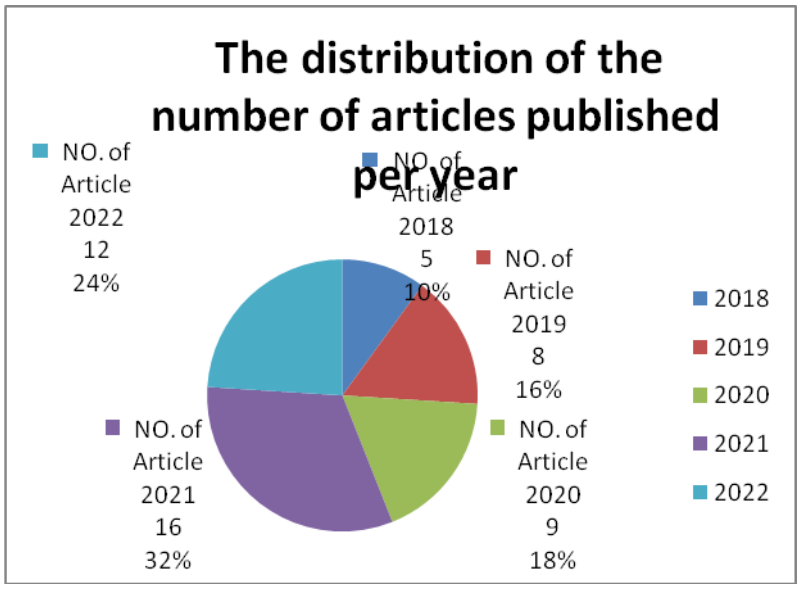


Figure 3.2 . The distribution of the number of articles published per year

Most of the recent researches address sub exponential time attacks and the modification of Fully homomorphic encryption (FHE) to reduce the breaches. These developments and evolutions have been driven by bottlenecks in their previous schemes. For instance, the implementation of the original Gentry scheme required handling of integers with millions of bits to improve its security, which reduced the efficiency of the algorithm in two ways [30,33,38]. First, the sizes of the public-keys were too large ranging between 69 megabytes and 2.25 gigabytes for lattice dimensions of 2048 and 32,768 respectively.

Conclusion

The goal of this paper is to investigate how homomorphic encryption technologies can address sustainability; specifically, data security and productivity without compromising the well-being of society. The role of cloud

computing in different industries is unmatched, and security issues and challenges continuous to deter the growth rate. The need to protect the privacy of users, especially on online platforms continues to be a major challenge given that the rate of assimilation of applications. Of the many remedies to the current security issues, homomorphic encryption, whether based on RSA algorithm, ElGamal algorithm or Paillier algorithm among others, continue to become a significant part of security development. As the review has established, several research articles address the basics of homomorphic, while some present different novel approaches and frameworks for future consideration.

References

Baharuddin, Ampera, D., Fibriasari, H., Sembiring, M. A. R., & Hamid, A. (2021). Implementation of cloud computing system in learning system development in engineering education study program. *International Journal of Education in Mathematics, Science and Technology*, *9*(4), 697–740. https://doi.org/10.46328/ijemst.2114

Gahi, Y., Guennoun, M., Guennoun, Z., & El-khatib, K. (2015). *On the use of homomorphic encryption to secure cloud computing, services, and routing protocols*. *88*(3), 416–438. http://arxiv.org/abs/1508.05411

Orobosade, A., Aderonke, T., Boniface, A., & J., A. (2020). Cloud Application Security using Hybrid Encryption. *Communications on Applied Electronics*, *7*(33), 25–31. https://doi.org/10.5120/cae2020652866

Rahu, M. (2020). *Impact of Cloud Computing on IT Industry: A Review & Analysis*. https://www.researchgate.net/publication/273126120_Impact_of_Cloud_Computing_on_IT_Industry_A_Review_Analysis

Ramasubramanian, G., Shaikh, A. A., & Sharma, R. (2021). Examining the impact of ICT on sustainable development: A data-driven narrative. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2020-Janua*, 4394–4403. https://doi.org/10.24251/hicss.2021.534

Ranger, S. (2022). *What is cloud computing? Everything you need to know about the cloud explained | ZDNet*. https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-about-the-cloud/

Rocha, V. F., López, J., & Falcão Da Rocha, V. (2019). An Overview on Homomorphic Encryption Algorithms. *Institute of Computing, UNICAMP*.

Satamraju, K. P., & Malarkodi, B. (2021). A decentralized framework for device authentication and data security in the next generation internet of medical things. *Computer Communications*, *180*(August), 146–160. https://doi.org/10.1016/j.comcom.2021.09.012

Tebaa, M., & Hajji, S. El. (2014). *Secure Cloud Computing through Homomorphic Encryption*. *5*(December), 29–38. http://arxiv.org/abs/1409.0829

Thabit, F., Can, O., Alhomdy, S., Al-Gaphari, G. H., & Jagtap, S. (2022). A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing. *International Journal of Intelligent Networks*, *3*, 16–30. https://doi.org/10.1016/J.IJIN.2022.04.001