Alloghani, MAMA, Alani, MM, Al-Jumeily, D, Baker, T, Mustafina, J, Hussain, A and Aljaaf, AJ

A Systematic Review on the Status and Progress of Homomorphic Encryption Technologies

A Systematic Review on the Status and Progress of Homomorphic Encryption Technologies

Mohamed Alloghani[a,b,*], Mohammed M. Alani[c], Dhiya Al-Jumeily[a], Thar Baker[a], Jamila Mustafina[d], Abir Hussain[a] and Ahmed J. Aljaaf[a,e]

[a] *School of Computing and Mathematical Sciences, Liverpool John Moores University, Byrom Street, L3 3AF, Liverpool, England, UK*
[b] *Abu Dhabi Health Services Company (SEHA), Abu Dhabi, UAE*
[c] *Khawarizmi International College, Al Bahia, Abu Dhabi, UAE*
[d] *Kazan Federal University, Kazan, Russia*
[e] *Centre of Computer, University of Anbar, Iraq*

ARTICLE INFO

Keywords:
Homomorphic Encryption, Big Data, Cloud Computing, Big Data Security, Cloud Computing Security, Cloud Computing Challenges

ABSTRACT

With the emergence of big data and the continued growth in cloud computing applications, serious security and privacy concerns emerged. Consequently, several researchers and cybersecurity experts have embarked on a quest to extend data encryption to big data systems and cloud computing applications. As most cloud users turn to using public cloud services, confidentiality becomes and even more complicated issue. Cloud clients storing their data on a public cloud always seek solutions to confidentiality problem. Homomorphic encryption emerged as a possible solution where client's data is encrypted on the cloud in a way that allows some search and manipulation operations without proper decryption.

In this paper, we present a systematic review of research paper published in the field of homomorphic encryption. This paper uses PRISMA checklist alongside some items of Cochrane's Quality Assessment to review studies retrieved from various resources. It was highly noticeable in the reviewed papers that security in big data and cloud computing has received most attention. Most papers suggested the use of homomorphic encryption although the thematic analysis has identified other potential concerns. Regarding the quality of the articles, 38% of the articles failed to meet three checklist items, including explicit statement of research objectives, procedure recognition and sources of funding used in the study. The review also presented compendium textual analysis of different homomorphic encryption algorithms, application areas, and areas of future developments. Results of the evaluation through PRISMA and the Cochrane tool showed that a majority of research articles discussed the potential use and application of Homomorphic Encryption as a solution to the growing demands of big data and absence of security and privacy mechanisms therein. This was evident from 26 of the total 59 articles that met the inclusion criteria. The term Homomorphic Encryption appeared 1802 times in the word cloud derived from the selected articles, which speaks of its potential to ensure security and privacy, while also preserving the CIA triad in the context of big data and cloud computing.

1. Introduction

The advent of big data and cloud computing among some of the emerging industry 4.0 concepts have brought with them innumerable security concerns. According to Patil et al. [1], big data refers to the large volume of data collected from the Internet, social network, and smart phones as well as other sources that generate huge volumes of data. Besides the large and complex nature of big data, the other notable characteristics include volume, variety, and velocity [1]. Kumar et al. [2] identified additional dimensions to big data; value and veracity [2]. Volume, in the context of big data, refers the numbers of records, transactions, and tables presented within the data set as measured in terabytes, while velocity refers to real-time processing of the data in batches using streams and associated technical performance [1, 2, 3]. Furthermore, value of big data refers to statistical inferences, events within the data sets, correlations among attributes, and hypotheses used in the analysis, while veracity attributes to the trustworthiness, authenticity, accountability, and availability of the data generated by the systems [2]. Regardless of whether the big data is structured or unstructured, one of the leading issues with big data and its related technology is security. Philip Chen and Zhang [4] asseverate that security issues and challenges experienced in big data supporting systems are largely since the systems use interconnected machines that support different applications. The authors observed that the continued storage and dissemination of sensitive information in big data applications have rendered such systems more vulnerable to intrusions [4, 5] . Consequently, experts and developers are working towards solutions that are compliant with big data analytics requirements.

1.1. Background

Singh et al. [6] identified data security and privacy, compliance issues, legal and contractual matters, migration hurdles, ambiguity in pay per use models, and integration of big data applications and legacy systems as the leading concern for the rapidly growing big data field. Regarding challenges, security of big data applications, incident response arrangements, data leaks and prevention strategies, physical and personal security, identity and access management, segregation and protection of data and management of threats and vul-

[*] Corresponding author
m.alloghani1@gmail.com, mloghani@seha.ae (M. Alloghani)

nerabilities are the primary challenges in big data technologies [3, 7, 8, 9, 10] The mitigation techniques to these challenges are dependent on the specifications and functionalities of the platform. For instance, Li et al. [11] suggest that switching bandwidth and the eventual reduction of traffic in cloud environment can help mitigate some of the issues. The authors argue that the type of switches and connection interfaces can affect the velocity and volume of data transmitted between workstations or other network devices [12]. Furthermore, Wang et al. [13] argue that dynamic preclusion of encroachment in Hadoop and other distributed big data file systems can minimize issues related to privacy and security, especially during transmission. Additionally, the authors suggested an encryption system that would mitigate privacy and access issues. A greater understanding of the context may also be gained by reviewing the prevalent threat landscape. Specifically, the use of human factors such as social engineering is gaining more prominence among the attackers. This enables them to execute malicious activity into their target systems, thereby breaching the overall security of the organizationâĂŹs critical infrastructure through people interactions. Basically, social engineering may be defined as the psychological manipulation of targets to generate unwilling responses. In other words, it is a means of coercing the target in a position that puts them at a loss in some form. It is arguable that social engineering poses an equally significant level of threat to the big data and cloud computing domain. Hence, the need for implementing a non-traditional encryption approach is absolutely critical Wang et al. [13], Bos et al. [14, 15], Li et al. [16].

2. Motivation and Scope

Various big data topics and applications have received attention over the past few years and security concerns have been given priority in big data research [1]. Most of the security efforts are geared towards cloud based big data platforms. Evidently, Kumar et al. [2] suggested that the rapid growth in cloud computing services drives the security research in big data and its deployment in cloud platforms. Future applications of big data and related technologies must maintain the three security goals of confidentiality, integrity, and availability (CIA)[2, 3]. Singh and Thokchom [17], as well as Gupta and Shanker [7] have emphasized the importance and role of CIA triad on boosting security of big data and increasing acceptance of big data applications. The researchers discussed some of the commonly used encryption technologies and presented a discourse for a security future. As higher demands for security emerged with big data, developments in encryption algorithms followed. The unique nature of cloud computing and its reliance on rapid deployment of resources have highlighted the need for more sophisticated, advanced, and highly-performing encryption algorithms [18, 19].For instance, Tahir, Stepokus and Ruj developed a novel encryption scheme for big data basing their algorithm on a parallelised disjunctive query [8]. In another article, Stergiou et al. [9] provided proof on encryption techniques that can be used to secure Big Data and Internet of Things (IoT) while maintaining privacy and guaranteeing efficiency and sustainability of the cloud computing system supporting the big data platform [11, 13, 20]. Ding et al. [21] provide a detailed account of a homomorphic re-encryption technique for protecting raw data while encouraging privacy-preserving data processing (PPDP) system. The system is based on a homomorphic re-encryption scheme (HERS) that uses ciphertexts for file decryption [21]. The highlighted studies present specific technologies for security big data, especially in cloud computing environments.

2.1. Contribution

Furthermore, some the review articles on data security encryption are focused on healthcare industry. Another motivation was that most of the review articles do not use any of the conventional tools for systematic reviews because they divulge in theoretical discourse. That is, the reviews are descriptive, and they do not engage in full text screening (detailed study title and abstract screening), data extraction (exploration of study characteristics), quality assessment, especially bias assessment. The reviews focus on title and rapid screening of the texts and in most cases the authors fail to discern the review period. For example, Emmanuel et al. [22] wrote a review article on homomorphic signatures with emphasis on descriptive aspects of linear homomorphic signatures alongside key homomorphism and other lattice based signatures. The thesis of the paper revolved around the timeline of the development of homomorphic encryption with minimal attention of the nature of the papers used in the study. In another review, Dugan and Zou [23] discussed different multi-party security calculations for preserving privacy in genetic testing. Despite using other articles, the researchers did not explore the quantitative techniques that the other researchers used and as such could not ascertain whether the reviewed or cited papers were biased or not. Many other reviews also focused on the descriptive aspects of the different encryptions and data security in cloud computing, especially with respect to big data and data science in general [24, 20, 25]. Sharma [26] and Vivekanand [27] also conducted reviews on security challenges and the homomorphic encryption related solutions and described some of the existing solutions. It is apparent from the existing reviews that homomorphic encryption lacks systematic review studies, and such is the focus of this study.

3. Literature Review

Several studies explored homomorphic encryption for different applications. For instance, Fahsi et al. [28] presented a framework for homomorphic encryption and private information retrieval protocols in the cloud for the purpose of protecting users against unauthorized data access. The researchers acknowledge existence of other homomorphic encryption methods and propose an improvement for protecting users online or in the cloud. It is paramount to understand the basis of homomorphic encryption before focusing on current trends and advancements over traditional methods. Rohilla [29] explain that homomorphic encryption produces cipher texts using specialized calculations that generate encrypted output but with a requirement for reverse computation techniques to produce the plain text version of encrypted message [30]. The homomorphic encryption has different approaches including fully homomorphic encryption (FHE), which is a form of ring homomorphism with structure preserving characteristics [30]. Furthermore, homomorphism can either be additive or multiplicative; in the former randomly chosen prime numbers are added pairwise while in the latter type are multiplied [30].

3.1. Homomorphic Encryption Methods

Suppose $(M, \circ)$ is a message space and is a finite semigroup or group with σ as a security parameter, then a homomorphic cryptosystem on the message space is a quadruple (K, E, D, A) of probabilistically expected time based algorithms conforming to the following conditions.

- **Key Generation (K):** On providing initiation parameter 1^{σ} the key generation scheme produces an encryption and a decryption key pair $\left(k_e, k_d\right) = k \in \kappa$ where κ represents the key space.

- **Encryption (E):** On providing 1^{σ}, k_e, and an element in the message space $m \in M$, the encryption scheme produces a cipher-text (c) in the cipher-space (C): $c \in C$.

- **Decryption (D):** The decryption scheme is deterministic and it requires 1^{σ}, k, $c \in C$ to produce $m \in M$ so that $\forall\ m \in M$ if $c = E\left(1^{\sigma}, k_e, m\right)$ then $Prob\left[D\left(1^{\sigma}, k, c\right)\right] \neq m$ is negligible and the probability $\leq 2^{-\sigma}$.

- **Homomorphic Property (A):** A is a scheme that requires 1^{σ}, k, and $c_1, c_2 \in C$ to produce a third ciphetext element $c_3 \in C$ such that $\forall\ m_1, m_2 \in M$ holds only when $m_3 = m_1 \circ m_2$, $c_1 = E\left(1^{\sigma}, k_e, m_1\right)$, and $c_2 = E\left(1^{\sigma}, k_e, m_2\right)$ such that $Prob\left[D\left(A\left(1^{\sigma}, k_e, c_1, c_2\right)\right)\right] \neq m_3$ is negligible.

Some of the articles discussed multiplicative, additive and XOR techniques while other explore hybrid encryption systems including the use of bio-metrics as well as quantum computing in implementing the keys.

3.1.1. Multiplicative Homomorphic Encryption

Barkataki and Zeineddine [31] and Jingli et al. [32] explored the concept of multiplicative homomorphic encryption in their articles. It is important to note that different researchers discuss different cryptographic technique when discussing the different types of homomorphic encryptions. However, one of the commonly discussed cryptography is the Rivest-Shamir-Adleman (RSA) public-key encryption algorithm [33, 34, 35, 36]. The RSA cryptosystem consists of four steps. At the first step, a pair of keys is generated by a random number generator. These keys must be large prime numbers for the algorithm to be secure, such as u and v [36]. The generated numbers are used to calculate a modulus n, which is a product of u and v. The modulus constitutes both the private and public key. It was later proven that key length that exceeds 1024 bits cannot be solved using any of the available computing methods [37]. Secondly, the public part of the generated key pair is distributed between the communicating parties. Each party shares its public for encryption of the sent message but withholding the private key for decrypting [38]. In the third step, the communicating parties agree on a padding scheme for encrypting the message. The sender then encrypts the text using the public key then transmit to the target. Finally, the recipient recovers or decrypts the message from the cipher text using the private key and eventual retrieve the message based on the agreed padding scheme. Furthermore, Hazay et al. [39] explained later that RSA encryption can also be used in signing data packets or messages digitally, and as such the technique has been adopted to thwart the actions of man-in-the middle attacks. In homomorphic encryption, suppose that the modulus and the exponent of the RSA public key are N and L, the encryption computation equation for a message sent is expressed as follows [40, 41].

$$E(S) = S^{L} mod\, N \tag{1}$$

In which E(S) denotes the encrypted message, S is the transmitted message while mod N is the modulus of the key, and the homomorphic characteristic of the unpadded RSA key must comply with the following.

$$E\left(S\right) \cdot \left(S_1\right) = {S_1}^{L} {S_2}^{L} mod\, N = \left(S_1 S_2\right)^{L} mod\, N \tag{2}$$

The equation represents the message sent and received between the two actors, and the plain messages, S_1 and S_2, are multiplied and the resultant message encrypted using the RSA algorithm producing the Ciphertext. As per multiplicative property, each of the messages can also be encrypted independently and the resultant cipher texts multiplied to produce a final RSA encrypted text [40, 36, 37]. Nonetheless, it is a requirement that a padding layer be included before encrypting the message although the implementation of the layer violates the homomorphic property of the technique [41]. Besides the RSA cryptography, multiplicative homomorphism can also be based on ElGamal cryptographic system, which is based on asymmetric public key encryption algorithm [40, 31]. The algorithm generates the key over a cyclic group with an order and a defined generator index. The exponent of the ElGamal encryption is a function of the order (d) and the public key is a function of the cyclic group (G), generator (T), and an exponent product (L). That is, both the private and public keys are presented as follows.

$$PublicKey : (G, T, d, L); PrivateKey : p$$

In which L is the exponent product of the generator and the private key and it is calculated as follows.

$$L = T^{p}$$

Additionally, note that private key selection is an integer that meets the condition $p \in \{1, 2, 3, ..., d-1\}$. That is, the integer lies within the domain of the order of the cyclic group. The encryption process involves computation of a random number (p), a shared secret number based on the value of p, and conversion of the message into the cyclic group, and eventually sending as a cipher text [36]. Decrypting the message requires the public key as well as the shared secret number, and it has been shown than ElGamal is a homomorphic scheme.

3.1.2. XOR Homomorphic Encryption

The technique is based on Goldwasser-Micali method; an encryption scheme that is based on computational probability [42]. The scheme is based on assumption that finding solution to quadratic residues is a computational demanding task and the subsequent cipher text is of larger size compared to the plain text [41]. The difference in the size has been attributed to the computation requirement during encryption, which involves random selection of two random prime numbers although of the same length (bit-length) and then finding non-residue associated with each of the numbers. Suppose the two prime numbers are a and b, and the product is V=a.b, then the non-residue and the subsequent private and public keys are generated as follows.

$$t_a^{(1-a)/\frac{1}{2}} = -1 mod a; t_b^{(1-b)/\frac{1}{2}} = -1 mod b \tag{3}$$

In which t is the non-residual and the public and private keys used for encryption and decryption are $PulicKey : (t, V)$ and $Privatekey : (a, b)$ respectively [40, 38]. It should be noted the homomorphism of Goldwasser—Micali encryption is dependent on the quadratic residual characteristics of encryption algorithm. However, it is also one of the probabilistic, additionally homomorphic cryptosystem on $M = (\mathbb{Z}/2\mathbb{Z}, +)$ with a cipher space defined as $C = Z = (\mathbb{Z}/N\mathbb{Z})$ and N is the product of the two large numbers used to generate the key.

3.1.3. Additive Homomorphic Encryption

The additive homomorphism is based on Parlier encryption scheme; an asymmetric probabilistic encryption scheme with properties similar to ElGamal scheme [31, 32]. However, the scheme uses different private and public keys to encrypt and decrypt messages. Additionally, the encryption scheme is based on the computation of the greatest common divisor the two randomly chosen prime numbers. The steps of implementing the scheme include choosing the two random numbers (a, b) and calculating the GCD as follows.

$$GCD(ab, (a-1)(b-1)) = 1 \tag{4}$$

Computing L and a parameter based on least common multiple as follows.

$$L = ab, H = lcm(a-1, b-1) \tag{5}$$

Then subsequently selecting a generator T such that the following equation holds.

$$\left(T^H mod L^2 - 1\right) 1/L, L = 1 \tag{6}$$

Finally, calculate a parameter that is a function of model and it serves as the boundary condition that requires satisfaction in defining both the public and private keys.

$$q = \left(y\left(T^H mod L^2\right) - 1 mod L, where y(q) = q - 1/L\right) \tag{7}$$

The equation provides the domain of input values that satisfy the condition that $q = 1 mod L$. The public and private keys used for encryption and decryption are $PulicKey : (L, T)$ and $Privatekey : (H, q)$ respectively.

3.1.4. Fully Homomorphic Encryption

The homomorphic techniques that have described operate as component and the processes must be completed independently. However, an encryption scheme is considered full when it consists of a plain text, a cipher text, a key space, an encryption algorithm, and a decryption algorithm [33, 28, 29]. According to Chen et al. [43], "a fully homomorphic encryption (FHE) scheme allows arbitrary functions on certain data (referred to as plaintexts) to be performed via their ciphertexts (the encrypted version of the plaintexts) without decrypting the ciphertexts first; therefore, performing these functions does not require one to hold the secret decryption key corresponding to the encryption algorithm." Based on the discourse and argument, FHE are more secure since they are self-contained and does not require or obligate actors to use secret keys, and it is this feature that render FHE suitable for advanced applications such as biometric verification [40, 44, 30]. Furthermore, systems based on FHE are not susceptible to both false match and false non-match that affects most cryptosystems [42]. The FHE consists of four algorithms: KeyGen, Enc, Dec and Evaluate. The FHE scheme is defined as follows.

As previously stated, the FHE can be based in several assumptions including LWE and RLWE. The FHE based on LWE focuses on noise management and key-size reduction that renders it effective compared to other classical algorithms.

3.1.5. Security on Critical Infrastructure Encryption

In recent years, security is gaining focus in critical infrastructure encryption and lately researchers began exploring new methods for Intrusion Detection Systems (IDS). For instance, in Aloqaily et al. [45] the authors proposed an automated secure incessant cloud-based service availability framework for smart connected vehicles that enables an intrusion detection mechanism against security attacks. The proposed solution achieved an overall accuracy of 99.43% with 99.92% detection rate and 0.96% false positive and a false negative rate of 1.53% A very recent research study has described the components of the monitoring systems for critical infrastructures include Otoum et al. [46] where they proposed Adaptively Supervised and Clustered Hybrid IDS (ASCH-IDS) for wirelessly connected sensor clusters that monitor critical infrastructures with monitoring behavior of the receiver operating characteristics, and adaptively directing the incoming packets at a sensor cluster towards either misuse detection or anomaly detection module.

4. Advances and Applications of Homomorphic Encryption

Most of the reviewed studies discussed homomorphic encryption in the context of big data and cloud computing, and as such most of the trends and advances are leaning towards these areas. However, Cheon and Kim [47] present one of the most unique application of homomorphic encryption; the research explored the application of a novel approach to drone security. In specific, the authors described a linearly homomorphic authenticated encryption framework that supports and protect ground controlled multi-rotor drones with the objective of preventing eavesdropping and forgery attacks [29, 5]. Cheon and Kim [47] also introduced a hybrid public-key encryption system that reduces the storage requirement associated with somewhat homomorphic encryption (SHE) [48]. The proposed scheme combines the computational abilities and procedures used in FHE as well as the multiplicative functionalities with a focus on composite mathematical rings [31]. Further review of retrospect suggests that one major application of Homomorphic Encryption is in the realm of outsourcing computation and storage. HE can be applied across organizations that process big data and outsource its storage and computation. In this sense, HE can be of use by allowing the companies to securely outsource these attributes without revealing any sensitive information that may be entailed therein [23]. This makes the technology ideal for implementation across companies of all sizes. For example, a small-scale company may implement HE to safeguard its sensitive data during the process of migrating to the cloud. Such a scenario would put the company at a loss in the absence of HE, as it may have to reveal the sensitive information while not being able to encrypt it at all. Thus, HE can serve as a viable solution.

Another critical application of Homomorphic Encryption is in the PIR and private queries processing. Specifically, users can leverage on the capabilities of HE to enable private queries to a certain search engine or database; Private Information Retrieval is a good example of such application. For PIR queries, the end-users usually look for retrieving a single record from a server that holds a huge database of records. While retrieving this record from bulk records may be vulnerable to threats, the user can implement HE to the index of the required record to retrieve it in an encrypted format. This makes PIR fast, secure and private, while upholding the CIA triad. A similar application may also extend to the larger and more complex SQL query to databases.

Homomorphic Encryption can also be readily implemented to general two-party computations, where there are cases involving two parties that are mutually suspicious; both the parties intend to compute the common function. For example, Jim and Joe with inputs A and B are involved in a sample use case, while there is a need to make Jim aware of the function F(A,B). There is also a need to ensure that Joe learns nothing. To do so, HE may prove to be the ideal technology.

The unique traits and attributes of Homomorphic Encryption also make it viable to be implemented across zero-knowledge proof protocols. Considering the same example of Jim and Joe with inputs A and B respectively, HE can be applied to achieve zero encryption to fulfill the zero-knowledge protocol; here, there is an involvement of a fresh zero and an evaluated encryption of zero. Thus, the same zero represents the encrypted text in the event that Jim is unable to distinguish between the evaluated encryption of zero and the fresh zero.

4.1. Big Data and Cloud Computing

The other emerging application of homomorphic encryption is in the field of big data and cloud computing.Chakraborty and K Patra [49] investigated the use of functional encryption in big data analytics and concluded that functional encryption algorithms that create public keys and secret masters keys have an added advantage because all the generated keys are based the master key and the computation involved in decrypting the message is dependent on the value of the generated key [32]. Liu et al. [50] and other authors Dijk and Gentry [40], Jie and Jing [51], Wang et al. [52], Tsoutsos and Maniatakos [53], Geetanjali and Sambhaji [54], Chou et al. [55] also discussed the application of homomorphic encryption in online systems and proposed different points of integrating the encryptions within the big data systems. Besides, the Paillier and ElGamal cryptosystems [56], Menandas and Joshi [57] postulated that Okamoto Uchiyama Cryptosystem, despite its complexity, is more suited for big data systems with sensitive information. However, this cryptosystem is also based on the same steps as its counterparts. Kocabas et al. [58], Papadimitriou et al. [59], Yakoubov et al. [38], and Thayananthan and Albeshri [60] have explored security issues in big data and concluded that either homomorphic encryption based on ElGamal and Paillier algorithms suit most big data applications [61, 62, 35, 10, 63]. The other area that has received more attention regarding security and the prospect of using homomorphism is cloud computing, especially in respect to different healthcare application and data storage systems [51]. Patil et al. [1] proposed an arithmetic based homomorphism that can to protect cyber space and promote secure sharing of information in different communication settings. However, the proposed system relies on FHE and ElGamal cryptosystems to encrypt the data although on a system [50]. The drive behind the proposed system is the need to protect users from intrusion other users or people with access and privileges on some parts of the systems [64, 9]. Daniel [65] explored a specific application of such a system although based on a different algorithm. The specific application addressed focuses on filtering information based on homomorphic techniques and the objective is to retrieve medical information without mismatch or other accidental acquisition of sensitive information [51, 19, 34, 66]. The studies that focused on the application of homomorphic encryption in health care systems include Tang et al. [67], Çetin et al. [68], Emmanuel et al. [22], [23], Bocu and Costache [69], and Wang and Zhang [70]. Some other applications include encryption of biomarkers and other genetic data, especially given that the medical fraternity is moving towards personalized health [71, 72, 18, 73, 74]. The studies explored the application of encryption in ensuring privacy and protection of patient data amid concerns regarding the probably misuse of information electronic medical records and other healthcare database systems. Given the growing concern for data and knowledge protection, the trends in the implementation of different homomorphic techniques and the implementation on big data system will continue to drive research and development in the field.

4.2. Electronic Voting Applications

Besides the growing security concerns about big data, cloud computing, and healthcare systems, most political factions, economic development considered, are constantly pursuing robust voting systems to further democratic practices. However, such systems have proven vulnerable and of high cost. For instance, Gibson et al. [73] identified verifiability, anonymity, dependability, security and trust as the major challenges associated with such voting systems. Cortier [75] also emphasised that the increase demand for electronic voting system has mandated the need for more security and assurances that the system work without human interference. One of the key elements of electronic voting is the streaming of data and as RAJALAKSHMI et al. [76]posit unsecure streaming channels can lead to lost trust in the system and gravely reduce its dependability. After conducting a search in Papadimitriou et al. [59] segmented data stream, the authors concluded that electronic voting systems require homomorphic-based filters to ensure integrity of the system. Lancichinetti et al. [77] also conducted a comprehensive study on different electronic voting systems, especially those based on cloud platforms and identified that attribute based encryption (ABE), identity based encryption (IBE), Hierarchical Identity Based Encryption (HIBE) and Hierarchical Attribute Set Based Encryption (HASBE) are some of the commonly used encryption techniques in electronic voting systems [60, 78]. However, the researcher identified that homomorphic encryptions are rarely used in e-voting systems. Tsoutsos and Maniatakos [53], in their investigation of random errors associated with additive homomorphic encryptions, recognized that the integrity of electronic voting systems could benefit from homomorphic encryption techniques [54, 79]. The homomorphic properties of encryption scheme deployed in e-voting system ensures that decryption of received votes would yield the correct result, as if encryption was never a part of the computation [80, 81, 16]. The trust in such systems is dependent on the computation process and the final tally. Abu Aziz et al. [82]emphasized that the inclusion of homomorphic model in e-voting systems guarantees quality and trustworthiness of the outcome. The authors reiterated that schemes based on homomorphic encryptions possess the property of verifiability while preserving privacy. It is critical to note that most of the current voting systems are based on multiplicative homomorphic models [60]. Suwandi et al. [83] explored the integration of encryption algorithms based on homomorphic properties to secure e-voting system and establish that Paillier and Okamoto Uchiyama algorithms can easily be integrated into e-voting systems to improve security. Moreover, Homomorphic Encryption is also potentially applicable to the domain of control and optimization, as evident from the two studies by Yang and Zhu [84]. In one of their studies, the researchers utilized HE in combination with reinforcement learning to devise a distributed algorithm that facilitated in preserving both, security and privacy of the operators and agents within discrete constrained games [84]. The same distributed algorithm also enabled them to ensure Nash equilibria in a formal manner [85]. Hence, it is clear that the applicability of Homomorphic Encryption is rather broad in scope than originally anticipated.

5. Research Methodology

The principle research methodology utilized for this paper was the systematic review methodology. The systematic review methodology 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 rationale behind selecting the systematic review research methodology was that there are currently no systematic reviews that focus on Homomorphic Encryption system, technologies and applications. Thus, the systematic review is intended to fill in this prevalent research gap. This methodology was found to be ideal for this paper as it allowed in systematic collection, evaluation and summarization of current knowledge regarding Homomorphic Encryption. Although systematic review methodology was originally developed and utilized in medical sciences, yet it was also readily adopted by other fields and disciplines. The motive of systematic review in medical sciences was to examine the impact and influence of various interventions. In a same manner, systematic review of Homomorphic Encryption is set to analyze it as an intervention for big data security and privacy, particularly over the cloud. A general understanding of the systematic review methodology can be gained by reviewing the steps listed below:

Step 1: Formulation of Problem Statement: The problem at hand was that despite considerable research and development involving Homomorphic Encryptions, no systematic reviews could be identified that consider the quality of research and development.

Step 2: Performing Search: The most relevant research articles were searched from key databases by making use of keywords containing the term Homomorphic Encryption in combination with Technologies, Methods and Applications.

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

Step 4: Critical Appraisal: The extracted data was subjected to critical appraisal and quality assessment while abiding by the PRISMA methodology.

Step 5: Data Synthesis: This step involved the presentation of data in both, narrative and graphical form to facilitate the overall evaluation of outcomes.

Step 6: Results: Finally, data synthesized, evaluated and summarized was presented in the results section to satisfy the research objective; the lack of a systematic review on Homomorphic Encryption.

5.1. Explaining the PRISMA Framework

Each of the selected articles was reviewed based on Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework. In [86] identify that the PRISMA checklist consist of the title, abstract, introduction, methods, results, discussion, and funding disclosure. However, the focus of the review was on the structure of the summary, objectives, rationale, information sources, data items where applicable, inferences and interpretation of results, summary of the evidence, and limitations of each of the studies. Basically, the PRISMA framework is ideal for systematic reviews and meta analyses, and can be defined as an evidence-based set of items that is utilized for reporting in both types of studies [86]. The rationale behind selecting the PRISMA framework was that it has been developed to help researchers enhance the reporting of their systematic reviews, and the fact that PRISMA is an effective framework in conducting critical appraisal of published articles. The steps involved in the PRISMA framework were applied in conjunction with the principles elicited in the PRISMA Explanation and Elaboration document.

Specifically, the PRISMA framework was applied as follows:

- Preparation: The PRISMA checklist explaining the entire framework was downloaded and populated with respect to the research at hand (see figure 1).
- Performing the Search: The search was performed by entering each key search term or keyword while making use of Boolean operators (And) and (Or) as and when necessary. The total number of articles identified were added up.
- Additional Sources: Apart from the key databases of ProQuest and Web of Science, certain additional sources were also identified and included from the Google Scholar database while utilizing the same strategy. The articles were added up to the total number of articles.
- Eliminating Duplication: Once the total 418 articles were collected, they were evaluated in terms of duplication of concepts, principles, technologies and applications.
- Article Screening: The titles and abstracts of the selected articles were screened in accordance with the inclusion and exclusion criteria to further identify the most relevant research studies for the systematic review.

To sum up, the improvised version of the PRISMA framework implemented in this study consisted of preparation, article identification, article selection, article screening (rapid or title screening), eligibility best on full text detailed abstract and title screening, and article selection or inclusion based on Cochrane quality assessment tool.

5.2. Inclusion Criteria

The inclusion criteria for the current systematic review was straightforward and simple. As such, the articles fulfilling the following criteria were included, while the rest were excluded from the study:

1. Articles published in peer-reviewed journals and periodicals available on the prominent databases, including the ProQuest Database, the Web of Science Database, IEEE Database and the Google Scholar Database.
2. Articles published on or after 2014.
3. 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). Articles that did not fall into this inclusion criteria were excluded from the systematic review. Moreover, since 418 articles in total were selected, the criteria were further restricted by exclusively considering the articles that considered the term Homomorphic Encryption in their titles.

5.3. Secondary Data Search

As identified earlier, secondary data was searched and identified from a variety of databases through keywords and Boolean operators And and OR. The search was conducted on ProQuest Database as well as Web of Science. Based on the preliminary reviews, Homomorphic Encryption emerged to be a data security technique associated with big data and clouding computing technologies and as such the search key words were construed around (Homomorphic Encryption) AND (Big Data) OR (Big Data Security) OR (Cloud Computing) OR (Cloud Computing technology). The search results were narrowed so that the selected articles were full-text, peer reviewed, and scholarly articles published between 2014 and 2018.The other search limitations that were deployed to synthesise the results further included considering only articles with the search phrase (Homomorphic Encryption) in the publication (PUB) and in the title (TI). The overall review process is as summarized by the following flow chart. Besides ProQuest and Web of Science, other studies were retrieved from Institute of Electrical and Electronics Engineers (IEEE) journals, in addition to conference papers and publications on the status of Homomorphic Encryption. Figure 1 shows the article review framework used in the study. It is important to note that characteristics of the 59 articles were evaluated and in cases where numerical data could not be extracted, qualitative information was provided for each case. The objective of the quantitative assessment was to explore the possibility of biasness-based allocation concealment with regards to excluded papers. Some other elements of selective reporting of the outcome of the studies were also considered although the literature pointed to qualitative aspects of homomorphic encryption. Figure 1 illustrates the steps used in conducting and filtering the search results. Firstly, search strings were implemented on

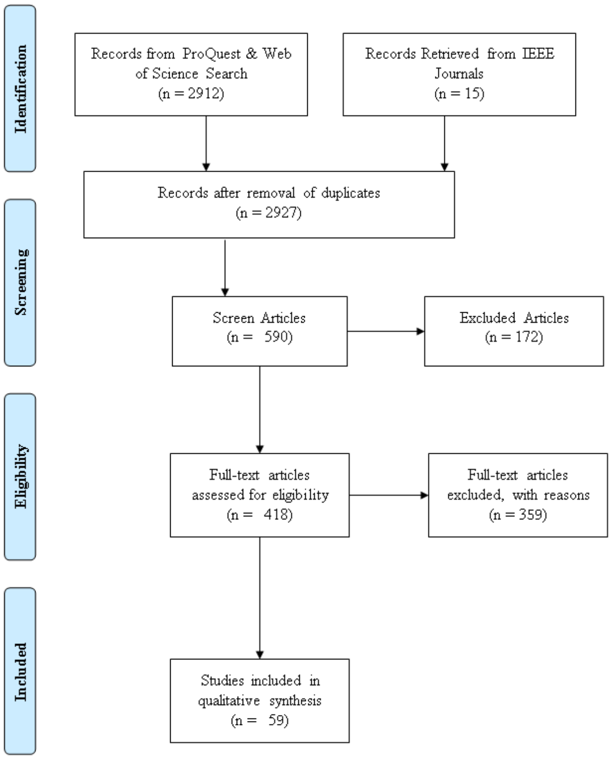
Identification
Records from ProQuest & Web of Science Search (n = 2912)
Records Retrieved from IEEE Journals (n = 15)
Screening
Records after removal of duplicates (n = 2927)
Screen Articles (n = 590)
Excluded Articles (n = 172)
Eligibility
Full-text articles assessed for eligibility (n = 418)
Full-text articles excluded, with reasons (n = 359)
Included
Studies included in qualitative synthesis (n = 59)

Figure 1: The Article Review Framework Used in the Study (Based on PRISMA Framework that Moher et al. [87] proposed)

ProQuest and IEEE Access databases and the number of articles recorded. Secondly, the records were filled to remove duplicates. Thirdly, the articles were screened based on the major PRISMA checklist and the ones lacking any of the components excluded from the review. Finally, full-text articles were evaluated based on the specific items under each main PRISMA checklist items and qualified studies included in this review.

6. Discussion of Results

Of the 418 eligible articles, only 59 met the inclusion criteria, which prioritized articles that had the search string Homomorphic both in the Abstract, Document Text, Document Title and Publication title. Of the 59 articles, 45 were retrieved from ProQuest Central while the rest were obtained from IEEE journals. However, one of the papers retrieved from ProQuest was in Chinese and was excluded from the review at the very last stages. The paper had a title and an abstract written in English and the meta-data also indicated that the manuscript was written in English. The remaining 44 documents (excluding the 15 IEEE articles) consisted of 8 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 Udaipur (7) followed by Heidel-berg, Hong Kong, London and New York (5). The summary of the distribution of the articles based on geographical location is as shown in Figure 2. The distribution illustrates the trends in authorship and subsequent implementation of the advances in FHE. Given the ongoing debate on security on the cyberspace, it is not surprising that countries like India, the US, the UK, and China are leading in publications of cryptography related studies. Regarding the distribution of the articles based on the year of publication, the year 2014 recorded the highest number of published papers (15) while only 7 papers have been published in 2018. As Figure 3 shows, in 2015 and 2016, only 12 articles were published about homomorphic encryption or about any related data security technology. The development of FHE traces back to 2009 when Gentry developed the first FHE scheme although the first attempt at implementation was conducted by Smart and Vercauteren. The first functional FHE was implemented in 2011 and the principal idea of polynomial-time quantum attack introduced in 2016. Other major devel-opments 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. It was also observed that the development of Ring Learning with Errors (RLWE) FHE scheme was also associated with key and modulus switching

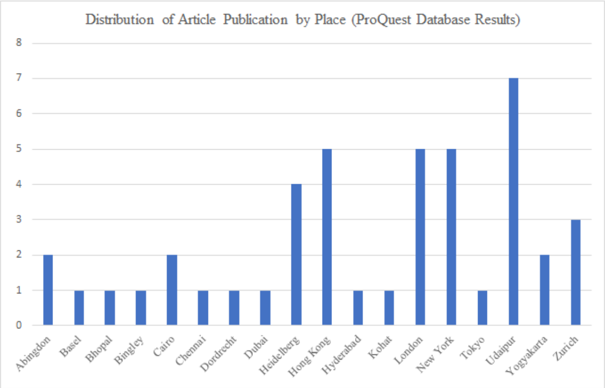

Figure 2: The distribution of Reviewed Articles by Place of Publication

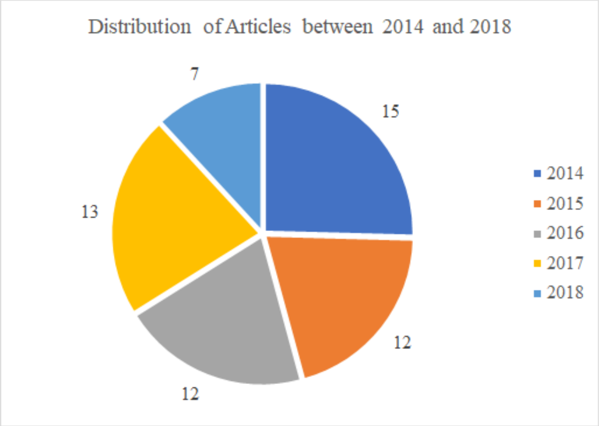

Figure 3: The Distribution of the number of Articles Published per Year

as well as introduction of scale-invariant scheme to reduce noise growth. Also, the changes in the FHE scheme necessitated other considerations including bootstrapping with 1s and 0.1s. However, the major developments involved reduction of RLWE scheme to Number Theory Research Unit (NTRU) with modulus switching and NTRU-based scale invariant encipherment scheme [88, 74, 14, 15]. Most of the current research address subexponential time attacks and the modification of 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 [33, 30, 40]. First, the sizes of the public-keys were too large ranging between 69 megabytes and 2.25 gigabytes for lattice dimensions of 2048 and 32768 respectively. Secondly, the scheme mandated multiplication of very larger numbers and that became the major issue with the system [36, 37, 41]. As per journals or publications from which the articles were retrieved, the 44 articles were distributed as shown in Table 1.

From Table 1, most of the articles are from IJARCS (7) and IJCNIS (4), which specializes in computer science, network and information technology research. The 15 articles from IEEE also focuses on different novel approaches to data security in big data and cloud computing and it emerged from the full text review that most of the articles (26) had data security, especially homomorphic encryption as the objective and the rationale was based on the big data growing demand. Regarding the quality of the articles, three items were reported by less 38 percent of the articles, which included explicit statement of research objectives, procedure recognition and sources of funding used in the study. Furthermore, the reviewers did not find evidence supporting quality variation based on authors from different geographical locations. However, it was noted that most articles on FHE are published in the US and the UK with the other papers from the rest of the regions appearing in other journals. The failure to meet these requirements reflected the type of the journal in which the articles were published or poor quality of the papers. It is also imperative to note the different distribution of the articles per publication. Even though FHE was first proposed in 2009, it has undergone rapid development and it has been implemented in encipher data in different applications and sectors.

Table 1
Distribution of the 44 Articles

Journal or Publication	Articles
International Journal of Advanced Research in Computer Science	7
International Journal of Computer Network and Information Security	4
Applied Mechanics and Materials	3
BMC Medical Genomics	3
International Journal of Distributed Sensor Networks	2
International Journal of Information Security	2
EURASIP Journal on Advances in Signal Processing	1
Information Systems Frontiers	1
International Journal of Advanced Computer Research	1
International Journal of Communication Networks and Information Security	1
International Journal of Computer Engineering and Information Technology	1
International Journal of Electrical and Computer Engineering	1
International Journal of Modern Education and Computer Science	1
International Journal on Information Sciences and Computing	1
International Journal of Pervasive Computing and Communications	1
Journal of Cloud Computing	1
IUP Journal of Computer Sciences	1
Journal of Applied Mathematics	1
Journal of Internet Services and Applications	1
Mathematical Problems in Engineering	1
Journal of Medical Systems	1
Scientific Reports (Nature Publisher Group)	1
Nature Communications	1
Multimedia Tools and Applications	1
Pacific Journal of Mathematics for Industry	1
TELKOMNIKA	1
Sensors	1
The Scientific World Journal	1
The Scientific World Journal	1

6.1. Thematic Modeling

The most common key words used in the reviewed articles included Biometric Identification, Cloud Computing, Computer Communication Networks, Computer Security, Confidentiality, Electronic Health Records, Genomics, Theoretical Models, Monitoring, Physiologic Privacy, Remote Sensing Technology and Wireless Technology. However, the other commonly repeated key words included Algorithms, Biomarkers, Biomarkers or metabolism, Computer Security or instrumentation, Cryptography, data aggregation, Data division, data integrity, Data Mining or related methods, Electrocardiography, Feasibility Studies, fully homomorphic encryption, Genome privacy Genome-Wide Association Study, Healthcare, Homomorphic encryption, message authentication code, Privacy, Remote Sensing Technology or instrumentation, wireless sensor networks and Wireless Technology or instrumentation. Figure 4 shows word cloud based on word frequencies from the retrieved articles and the key words are indicative of the key concern areas addressed in the reviewed papers, and of interest was all these related to homomorphic encryption and other cryptographic technologies. A word

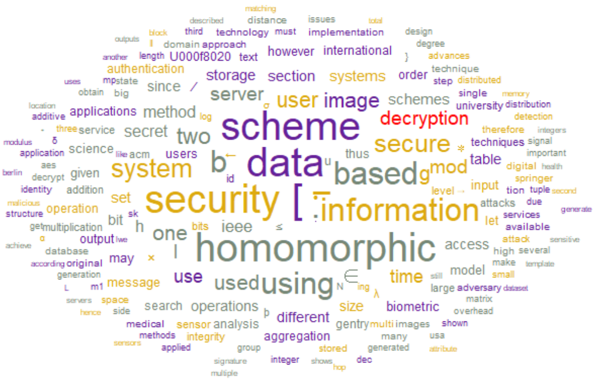

Figure 4: Word Cloud based on Word frequencies from the retrieved articles

cloud summarizing the key words shown in Figure 4 reveal that security, scheme, information, decryption, and homomorphic are among the commonly used words in the article. In specific, the word cloud presented in Figure 4 consists of 1802 appearances of the word homomorphic alongside 1538, 1461, 1122 and 827 number of words for security, scheme, information and secure keywords. The major themes from the reviews were depicted in Figure 4 of the word cloud. As Figures 3 and 4 show, research on homomorphic encryption has been rising since its inception 2009 and as part of the developments comes different areas of application. In instances, homomorphic encipherment and data security were addressed in the context of big data [30, 89, 42, 90].

7. Conclusion

The role of big data as well as that of cloud computing in 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. The papers also addressed the application of homomorphic encryption in healthcare and electronic voting systems. However, prospects and application of FHE will include and rely on quantum computing. Other authors reiterate, quantum computing techniques based on Gaussian displacement and squeezing operations will improve the computing power used in encryption and allow for the creation of larger bit cipher texts. Finally, most of the reviewed papers met over 4 items and sub-items of the PRISMA checklist, and the qualitative assessment of the theoretical representations and derivations of homomorphic encryptions were also consistence in cases where they were present. As such, the presented examples of application and the discussed encryption algorithms were based on high quality information.

8. Acknowledgment

We give special gratitude to LJMU's Faculty of Engineering and Technology for the valuable feedback about the paper.

References

[1] Tejashree B Patil, Girish Kumar Patnaik, and Ashish T Bhole. Big Data Privacy Using Fully Homomorphic Non-Deterministic Encryption. In *Proceedings - 7th IEEE International Advanced Computing Conference, IACC 2017*, pages 138–143, 2017. ISBN 9781509015603. doi: 10.1109/IACC.2017.0041.

[2] P. Ravi Kumar, P. Herbert Raj, and P. Jelciana. Exploring Data Security Issues and Solutions in Cloud Computing. In *Procedia Computer Science*, volume 125, pages 691–697. Elsevier B.V., 2018. ISBN 9781466683877. doi: 10.1016/j.procs.2017.12.089.

[3] Dipti Singh Galav, S M Ghosh, and Praveen Shrivastav. *International Journal of Advanced Research in Computer Science U6 number = 1, pages = 5697, title = Data Confidentiality for Secure Cloud Computing Through Homomorphic Encryption, volume = 6, year = 2015.*

[4] C. L. Philip Chen and Chun Yang Zhang. Data-intensive applications, challenges, techniques and technologies: A survey on Big Data. *Information Sciences*, 275:314–347, 2014. ISSN 00200255. doi: 10.1016/j.ins.2014.01.015.

[5] Abbas Acar, Hidayet Aksu, A Selcuk Uluagac, and Mauro Conti. A Survey on Homomorphic Encryption Schemes. *ACM Computing Surveys*, 51(4):1–35, 2018. ISSN 03600300. doi: 10.1145/3214303.

[6] Dinesh Singh, Dayanand ., and Arushi Arya. Security Challenges in Big Data. *International Journal of Computer Sciences and Engineering*, 6(7):981–985, 2018. doi: 10.26438/ijcse/v6i7.981985.

[7] Ajay K. Gupta and Udai Shanker. SPMC-CRP:A Cache Replacement Policy for Location Dependent Data in Mobile Environment. In *Procedia Computer Science*, volume 125, pages 632–639. Elsevier B.V., 2018. doi: 10.1016/j.procs.2017.12.081.

[8] Shahzaib Tahir, Liutauras Steponkus, Sushmita Ruj, Muttukrishnan Rajarajan, and Ali Sajjad. A parallelized disjunctive query based searchable encryption scheme for big data, jun 2018. ISSN 0167739X.

[9] Christos Stergiou, Kostas E. Psannis, Brij B. Gupta, and Yutaka Ishibashi. Security, privacy & efficiency of sustainable Cloud Computing for Big Data & IoT. *Sustainable Computing: Informatics and Systems*, 19:174–184, jun 2018. ISSN 22105379. doi: 10.1016/j.suscom.2018.06.003.

[10] Dario Catalano and Dario Fiore. Using Linearly-Homomorphic Encryption to Evaluate Degree-2 Functions on Encrypted Data. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS '15*, pages 1518–1529, 2015. ISBN 9781450338325. doi: 10.1145/2810103.2813624.

[11] Chen Li, Rongxing Lu, Hui Li, Le Chen, and Xiaoqing Li. Comment on 'a novel homomorphic MAC scheme for authentication in network coding'. *IEEE Communications Letters*, 18(12):2129–2132, 2014. ISSN 10897798. doi: 10.1109/LCOMM.2014.2361805.

[12] Mengxing Li, Quan Feng, Jian Zhao, Mei Yang, Lijun Kang, and Lili Wu. Minutiae Matching with Privacy Protection Based on the Combination of Garbled Circuit and Homomorphic Encryption. *The Scientific World Journal*, 2014:1–13, 2014. ISSN 2356-6140. doi: 10.1155/2014/525387.

[13] W. Wang, D. Liu, X. Liu, and L. Pan. Fuzzy overlapping community detection based on local random walk and multidimensional scaling. *Physica A.*, 392:6578–6586, 2013.

[14] Joppe W. Bos, Craig Costello, Michael Naehrig, and Douglas Stebila. Post-quantum key exchange for the TLS protocol from the

ring learning with errors problem. In *Proceedings - IEEE Symposium on Security and Privacy*, 2015. ISBN 9781467369497. doi: 10.1109/SP.2015.40.

[15] Joppe W. Bos, Kristin Lauter, and Michael Naehrig. Private predictive analysis on encrypted medical data. *Journal of Biomedical Informatics*, 50:234–243, 2014. ISSN 15320464. doi: 10.1016/j.jbi.2014.04.003.

[16] Zengpeng Li, Chunguang Ma, and DIng Wang. Towards Multi-Hop Homomorphic Identity-Based Proxy Re-Encryption via Branching Program. *IEEE Access*, 5:16214–16228, 2017. ISSN 21693536. doi: 10.1109/ACCESS.2017.2740720.

[17] Shubham Singh and Surmila Thokchom. Public integrity auditing for shared dynamic cloud data. In *Procedia Computer Science*, volume 125, pages 698–708. Elsevier B.V., 2018. ISBN 0018-9340. doi: 10.1016/j.procs.2017.12.090.

[18] Javier Andreu-Perez, Carmen C.Y. Poon, Robert D. Merrifield, Stephen T.C. Wong, and Guang Zhong Yang. Big Data for Health. *IEEE Journal of Biomedical and Health Informatics*, 19(4):1193–1208, 2015. ISSN 21682194. doi: 10.1109/JBHI.2015.2450362.

[19] Shetty Annapoorna, Shetty Shravya, and K Krithika. A Review on Asymmetric Cryptography âĂŞ RSA and ElGamal Algorithm. *International Journal of Innovative Research in Computer and Communication Engineering*, 2(Special issue 5):98, 2014. URL `http://ijircce.com/upload/2014/sacaim/13{_}Paper8.pdf`.

[20] Rafael Dowsley, Antonis Michalas, Matthias Nagel, and Nicolae Paladi. A survey on design and implementation of protected searchable data in the cloud, 2017. ISSN 15740137.

[21] Wenxiu Ding, Zheng Yan, and Robert H. Deng. Encrypted data processing with Homomorphic Re-Encryption. *Information Sciences*, 409-410:35–55, oct 2017. ISSN 00200255. doi: 10.1016/j.ins.2017.05.004.

[22] Naina Emmanuel, Abid Khan, Masoom Alam, Tanveer Khan, and Muhammad Khurram Khan. Structures and data preserving homomorphic signatures, 2018. ISSN 10958592.

[23] Tamara Dugan and Xukai Zou. Privacy-preserving evaluation techniques and their application in genetic tests. *Smart Health*, 1-2:2–17, 2017. ISSN 23526483. doi: 10.1016/j.smhl.2017.03.003.

[24] David Nuñez, Isaac Agudo, and Javier Lopez. Proxy Re-Encryption: Analysis of constructions and its application to secure access delegation, 2017. ISSN 10958592.

[25] Nesrine Kaaniche and Maryline Laurent. Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms, 2017. ISSN 01403664.

[26] Sudesh Sharma. A Review of Security of Data Storage and Retrieval on Cloud using Homomorphic Encryption. 8(5):796–800, 2017.

[27] Vidyavathi Vivekanand. Security Challenges in Big Data: A review. *International Journal of Advanced Research in Computer Science*, 2015.

[28] Mahmoud Fahsi, Sidi Mohamed Benslimane, and Amine Rahmani. A Framework for Homomorphic, Private Information Retrieval Protocols in the Cloud. *International Journal of Modern Education and Computer Science*, 7(5):16–23, 2015. ISSN 20750161. doi: 10.5815/ijmecs.2015.05.03.

[29] Alisha Rohilla. Homomorphic Cryptosystem. (May):44–51, 2017. doi: 10.5815/ijcnis.2017.05.06.

[30] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (Leveled) Fully Homomorphic Encryption without Bootstrapping. *ACM Transactions on Computation Theory*, 6(3):1–36, 2014. ISSN 19423454. doi: 10.1145/2633600.

[31] Sharad Barkataki and Hassan Zeineddine. On achieving secure collaboration in supply chains. *Information Systems Frontiers*, 17(3): 691–705, 2015. ISSN 13873326. doi: 10.1007/s10796-013-9448-3.

[32] Zheng Jingli, Hu Zhengbing, and Lu Chuiwei. A Light-weight Symmetric Encryption Algorithm Based on Feistel Cryptosystem Structure. *International Journal of Computer Network and Information Security*, 7(1):16–23, 2015. ISSN 20749090. doi: 10.5815/ijcnis.2015.01.03.

[33] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In *Proceedings - Annual IEEE Symposium on Foundations of Computer Science, FOCS*, 2011. ISBN 9780769545714. doi: 10.1109/FOCS.2011.12.

[34] Payal V.Parmar, Shraddha B. Padhar, Shafika N. Patel, Niyatee I. Bhatt, and Rutvij H. Jhaveri. Survey of Various Homomorphic Encryption algorithms and Schemes. *International Journal of Computer Applications*, 91(8):26–32, 2014. ISSN 09758887. doi: 10.5120/15902-5081.

[35] Payal V.Parmar, Shraddha B. Padhar, Shafika N. Patel, Niyatee I. Bhatt, and Rutvij H. Jhaveri. Survey of Various Homomorphic Encryption algorithms and Schemes. *International Journal of Computer Applications*, 91(8):26–32, 2014. ISSN 09758887. doi: 10.5120/15902-5081.

[36] Craig Gentry. a Fully Homomorphic Encryption Scheme. *PhD Thesis*, 2009. ISSN 07378017. doi: 10.1145/1536414.1536440.

[37] Craig Gentry. A fully homomorphic encryption scheme. *System*, 2009. ISSN 07378017. doi: 10.1145/1536414.1536440.

[38] Sophia Yakoubov, Vijay Gadepally, Nabil Schear, Emily Shen, and Arkady Yerukhimovich. A survey of cryptographic approaches to securing big-data analytics in the cloud. In *2014 IEEE High Performance Extreme Computing Conference, HPEC 2014*, 2014. ISBN 9781479962334. doi: 10.1109/HPEC.2014.7040943.

[39] Carmit Hazay, Gert Læssøe Mikkelsen, Tal Rabin, Tomas Toft, and Angelo Agatino Nicolosi. Efficient RSA Key Generation and Threshold Paillier in the Two-Party Setting, 2018. ISSN 14321378.

[40] Marten Van Dijk and Craig Gentry. Fully homomorphic encryption over the integers. *Advances in CryptologyâĂŞ . . .*, 2010. ISSN 00200255. doi: 10.1007/978-3-642-38348-9_20.

[41] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the 41st annual ACM symposium on Symposium on theory of computing - STOC '09*, 2009. ISBN 9781605585062. doi: 10.1145/1536414.1536440.

[42] Manish M. Potey, C.A. Dhote, and Deepak H. Sharma. Homomorphic Encryption for Security of Cloud Data. *Procedia Computer Science*, 2016. ISSN 18770509. doi: 10.1016/j.procs.2016.03.023.

[43] Q. Chen, T. T. Wu, and M. Fang. Detecting local community structure in complex networks based on local degree central nodes. *Physica A.*, 392:529–537, 2013.

[44] Vincent Migliore, Cédric Seguin, Maria Méndez Real, Vianney Lapotre, Arnaud Tisserand, Caroline Fontaine, Guy Gogniat, and Russell Tessier. A High-Speed Accelerator for Homomorphic Encryption using the Karatsuba Algorithm. *ACM Transactions on Embedded Computing Systems*, 16(5s):1–17, 2017. ISSN 15399087. doi: 10.1145/3126558. URL `http://dl.acm.org/citation.cfm?doid=3145508.3126558`.

[45] Moayad Aloqaily, Safa Otoum, Ismaeel Al Ridhawi, and Yaser Jararweh. An intrusion detection system for connected vehicles in smart cities. *Ad Hoc Networks*, 2019. ISSN 1570-8705. doi: https://doi.org/10.1016/j.adhoc.2019.02.001. URL `http://www.sciencedirect.com/science/article/pii/S1570870519301131`.

[46] S. Otoum, B. Kantarci, and H. Mouftah. Adaptively supervised and intrusion-aware data aggregation for wireless sensor clusters in critical infrastructures. In *2018 IEEE International Conference on Communications (ICC)*, pages 1–6, May 2018. doi: 10.1109/ICC.2018.8422401.

[47] Jung Hee Cheon and Jinsu Kim. A hybrid scheme of public-key encryption and somewhat homomorphic encryption. *IEEE Transactions on Information Forensics and Security*, 10(5):1052–1063, 2015. ISSN 15566013. doi: 10.1109/TIFS.2015.2398359.

[48] Masaya Yasuda, Takeshi Shimoyama, and Jun Kogure. Secret computation of purchase history data using somewhat homomorphic encryption. *Pacific Journal of Mathematics for Industry*, 6(1):1–9, 2014. doi: 10.1186/s40736-014-0005-x.

[49] Nilotpal Chakraborty and G K Patra. Functional Encryption for Secured Big Data Analytics. *International Journal of Computer Applications*, 107(16):19–22, 2014. doi: 10.5120/18836-0359.

[50] W. Liu, M. Pellegrini, and X. Wang. Detecting communities based on network topology. *Sci. Rep.*, 4:5739, 2014.

[51] Xia Jie and Rui Jun Jing. On-Line Decrypting: A Homomorphic Realization for Network Coding. *Applied Mechanics and Materials*, 543-547:2728–2732, 2014. ISSN 1662-7482. doi: 10.4028/www.scientific.net/amm.543-547.2728.

[52] Dan Wang, Bing Guo, Yan Shen, Shun Jun Cheng, and Yong Hong Lin. A faster fully homomorphic encryption scheme in big data. In *2017 IEEE 2nd International Conference on Big Data Analysis, ICBDA 2017*, pages 345–349, 2017. ISBN 9781509036189. doi: 10.1109/ICBDA.2017.8078836.

[53] Nektarios Georgios Tsoutsos and Michail Maniatakos. Efficient detection for malicious and random errors in additive encrypted computation. *IEEE Transactions on Computers*, 67(1):16–31, 2018. ISSN 00189340. doi: 10.1109/TC.2017.2722440.

[54] Rokade Geetanjali and Sarode Sambhaji. Implementation of Privacy Preserving Model for Shared Data in the. 8(9):179–183, 2016.

[55] Jia Kai Chou, Chuan Kai Yang, and Hsing Ching Chang. Encryption domain content-based image retrieval and convolution through a block-based transformation algorithm. *Multimedia Tools and Applications*, 75(21):13805–13832, 2016. ISSN 15737721. doi: 10.1007/s11042-015-2917-6.

[56] Tristan Daladier Engouang, Liu Yun, and Zhen Jiang Zhang. Pallier Based Homomorphic Encrypted Data Aggregation in Wireless Sensor Networks. *Applied Mechanics and Materials*, 543-547:3017–3022, 2014. ISSN 1662-7482. doi: 10.4028/www.scientific.net/amm.543-547.3017.

[57] J Josepha Menandas and J Jakkulin Joshi. IJARCCE Secure Big Data Processing Through Homomorphic Encryption in Cloud Computing Environments. *International Journal of Advanced Research in Computer and Communication Engineering*, 5, 2016. doi: 10.17148/IJARCCE.2016.5347.

[58] Ovunc Kocabas, Tolga Soyata, and Mehmet K. Aktas. Emerging Security Mechanisms for Medical Cyber Physical Systems. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 13(3):401–416, 2016. ISSN 15455963. doi: 10.1109/TCBB.2016.2520933.

[59] Antonis Papadimitriou, Ranjita Bhagwan, Nishanth Chandran, Ramachandran Ramjee, Andreas Haeberlen, Harmeet Singh, Abhishek Modi, and Saikrishna Badrinarayanan. Big Data Analytics over Encrypted Datasets with Seabed. *12th USENIX Symposium on Operating Systems Design and Implementation (OSDI '16)*, pages 587–602, 2016.

[60] Vijey Thayananthan and Aiiad Albeshri. Big data security issues based on quantum cryptography and privacy with authentication for mobile data center. In *Procedia Computer Science*, volume 50, pages 149–156. Elsevier Masson SAS, 2015. doi: 10.1016/j.procs.2015.04.077.

[61] Dhruva Gaidhani. A SURVEY REPORT ON TECHNIQUES FOR DATA CONFIDENTIALITY IN CLOUD COMPUTING USING HOMOMORPHIC ENCRYPTION. *International Journal of Advanced Research in Computer Science*, 8(8):389–394, 2017. doi: 10.26483/ijarcs.v8i8.4746.

[62] Lei Wei and Michael K. Reiter. Toward practical encrypted email that supports private, regular-expression searches. *International Journal of Information Security*, 14(5):397–416, 2015. ISSN 16155270. doi: 10.1007/s10207-014-0268-3.

[63] A. Lancichinetti and S. Fortunato. Benchmarks for testing community detection algorithms on directed and weighted graphs with overlapping communities. *Phys. Rev. E.*, 80:016118, 2009.

[64] Laicheng Cao and Hao Zhou. A New Reversible Date-Hiding Algorithm for Encrypted Images. *Mathematical Problems in Engineering*, 2016:1–11, 2016. ISSN 1024-123X. doi: 10.1155/2016/4313580.

[65] Ebenezer Daniel. Optimum Wavelet-Based Homomorphic Medical Image Fusion Using Hybrid Genetic-Grey Wolf Optimization Algorithm. *IEEE Sensors Journal*, 18(16):6804–6811, 2018. ISSN 1530437X. doi: 10.1109/JSEN.2018.2822712.

[66] Hao Tian Wu, Yiu Ming Cheung, and Jiwu Huang. Reversible data hiding in Paillier cryptosystem. *Journal of Visual Communication and Image Representation*, 40(Part B):765–771, 2016. ISSN 10959076. doi: 10.1016/j.jvcir.2016.08.021.

[67] Haixu Tang, Xiaoqian Jiang, Xiaofeng Wang, Shuang Wang, Heidi Sofia, Dov Fox, Kristin Lauter, Bradley Malin, Amalio Telenti, Li Xiong, and Lucila Ohno-Machado. Protecting genomic data analytics in the cloud: state of the art and opportunities. *BMC Medical Genomics*, 9(1):1–9, 2016. ISSN 17558794. doi: 10.1186/s12920-016-0224-3.

[68] Gizem S. Çetin, Hao Chen, Kim Laine, Kristin Lauter, Peter Rindal, and Yuhou Xia. Private queries on encrypted genomic data. *BMC Medical Genomics*, 10(Suppl 2):1–15, 2017. ISSN 17558794. doi: 10.1186/s12920-017-0276-z.

[69] R. Bocu and C. Costache. A homomorphic encryption-based system for securely managing personal health metrics data. *IBM Journal of Research and Development*, 62(1):1:1–1:10, 2018. ISSN 0018-8646. doi: 10.1147/jrd.2017.2755524.

[70] Xiaoni Wang and Zhenjiang Zhang. Data Division Scheme Based on Homomorphic Encryption in WSNs for Health Care. *Journal of Medical Systems*, 39(12):1–8, 2015. ISSN 1573689X. doi: 10.1007/s10916-015-0340-1.

[71] Miran Kim, Yongsoo Song, and Jung Hee Cheon. Secure searching of biomarkers through hybrid homomorphic encryption scheme. *BMC Medical Genomics*, 10(Suppl 2), 2017. ISSN 17558794. doi: 10.1186/s12920-017-0280-3.

[72] Xun Yi, Athman Bouguettaya, Dimitrios Georgakopoulos, Andy Song, and Jan Willemson. Privacy Protection for Wireless Medical Sensor Data. *IEEE Transactions on Dependable and Secure Computing*, 13(3):369–380, 2016. ISSN 15455971. doi: 10.1109/TDSC.2015.2406699.

[73] J. Paul Gibson, Robert Krimmer, Vanessa Teague, and Julia Pomares. A review of E-voting: the past, present and future, 2016. ISSN 19589395.

[74] Janet Metcalfe. Learning from Errors. *Annual Review of Psychology*, 2017. ISSN 0066-4308. doi: 10.1146/annurev-psych-010416-044022.

[75] Véronique Cortier. Formal verification of e-voting: solutions and challenges. *ACM SIGLOG News*, 2(1):25–34, 2015. ISSN 2372-3491. doi: 10.1145/2728816.2728823. URL https://dl.acm.org/citation.cfm?id=2728823.

[76] V RAJALAKSHMI, SAHAYA AURO STINA, and SANTHIYA S. PRIVATE SEARCHING ON STREAMING DATA BASED ON HOMOMORPHIC ENCRYPTION. *International Journal on Information Sciences and Computing*, 10(2):16–21, 2016. ISSN 0973-9092. doi: 10.18000/ijisac.50162.

[77] A. Lancichinetti, S. Fortunato, and F. Radicchi. Benchmark graphs for testing community detection algorithms. *Phys. Rev. E.*, 78:046110, 2008.

[78] Kannan Balasubramanian and M Jayanthi. A Homomorphic Crypto System for Electronic Election Schemes. *Circuits and Systems*, 07(10):3193–3203, 2016. ISSN 2153-1285. doi: 10.4236/cs.2016.710272.

[79] P. Sun, L. Gao, and S. Han. Identification of overlapping and non-overlapping community structure by fuzzy clustering in complex networks. *Inf. Sci.*, 181:1060–1071, 2011.

[80] Wilson Abel Alberto Torres, Nandita Bhattacharjee, and Bala Srinivasan. Privacy-preserving biometrics authentication systems using fully homomorphic encryption. *International Journal of Pervasive Computing and Communications*, 11(2):151–168, 2015. ISSN 1742738X. doi: 10.1108/IJPCC-02-2015-0012.

[81] Edson Floriano, Eduardo Alchieri, Diego F. Aranha, and Priscila Solis. Providing privacy on the tuple space model. *Journal of Internet Services and Applications*, 8(1), 2017. ISSN 18690238. doi: 10.1186/s13174-017-0070-3.

[82] Ahmed A Abu Aziz, Hasan N Qunoo, and Aiman A Abu Samra. Using Homomorphic Cryptographic Solutions on E-voting Systems. *International Journal of Computer Network and Information Security*, 10(1):44, 2018. ISSN 20749090. doi: http://dx.doi.org/10.5815/ijcnis.2018.01.06.

[83] Rifki Suwandi, Surya Michrandi Nasution, and Fairuz Azmi. Secure E-voting System by Utilizing Homomorphic Properties of the En-

cryption Algorithm. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, 16(2):862, 2018. ISSN 1693-6930. doi: 10.12928/telkomnika.v16i2.8420.

[84] Yang Lu and Minghui Zhu. Privacy preserving distributed optimization using homomorphic encryption. *Automatica*, 96:314 – 325, 2018. ISSN 0005-1098. doi: https://doi.org/10.1016/j.automatica.2018.07.005. URL http://www.sciencedirect.com/science/article/pii/S0005109818303510.

[85] Yang Lu and Minghui Zhu. Secure cloud computing algorithms for discrete constrained potential gamesâĹŮâĹŮthis work was partially supported by aro w911nf-13-1-0421 (muri) and nsf grant cns-1505664. *IFAC-PapersOnLine*, 48(22):180 – 185, 2015. ISSN 2405-8963. doi: https://doi.org/10.1016/j.ifacol.2015.10.327. URL http://www.sciencedirect.com/science/article/pii/S2405896315022181. 5th IFAC Workshop on Distributed Estimation and Control in Networked Systems NecSys 2015.

[86] Venkateshbabu Nagendrababu, Shaju Jacob Pulikkotil, Omer Sheriff Sultan, Jayakumar Jayaraman, and Ove A Peters. Methodological and Reporting Quality of Systematic Reviews and Meta-analyses in Endodontics, 2018. ISSN 00992399.

[87] David Moher, Alessandro Liberati, Jennifer Tetzlaff, Douglas G. Altman, Doug Altman, Gerd Antes, David Atkins, Virginia Barbour, Nick Barrowman, Jesse A. Berlin, Jocalyn Clark, Mike Clarke, Deborah Cook, Roberto D'Amico, Jonathan J. Deeks, P. J. Devereaux, Kay Dickersin, Matthias Egger, Edzard Ernst, Peter C. Gøtzsche, Jeremy Grimshaw, Gordon Guyatt, Julian Higgins, John P.A. Ioannidis, Jos Kleijnen, Tom Lang, Nicola Magrini, David McNamee, Lorenzo Moja, Cynthia Mulrow, Maryann Napoli, Andy Oxman, Ba' Pham, Drummond Rennie, Margaret Sampson, Kenneth F. Schulz, Paul G. Shekelle, David Tovey, and Peter Tugwell. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement (Chinese edition), aug 2009. ISSN 16721977.

[88] Oded Regev. The learning with errors problem. In *Proceedings of the Annual IEEE Conference on Computational Complexity*, 2010. ISBN 9780769540603. doi: 10.1109/CCC.2010.26.

[89] Thore Graepel, Kristin Lauter, and Michael Naehrig. ML confidential: Machine learning on encrypted data. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2013. ISBN 9783642376818. doi: 10.1007/978-3-642-37682-5_1.

[90] Deepti Mittal, Damandeep Kaur, and Ashish Aggarwal. Secure Data Mining in Cloud Using Homomorphic Encryption. *2014 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, 2014. doi: 10.1109/CCEM.2014.7015496.

List of Abbreviations

CIA	Confidentiality, Integrity and Availability.
ECC	Elliptic Curve Cryptography
FHE	Fully Homomorphic Encryption.
HERS	Homomorphic Re-encryption Scheme.
HE	Homomorphic Encryption.
IoT	Internet of Things.
IJARCS	International Journal of Advanced Research in Computer Science
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses.
PPDP	Privacy Preserving Data Processing.
RSA	Rivest-Shamir-Adelman encryption