Survey on Homomorphic Encryption and Address of New Trend

Ayman Alharbi[1]
Umm Al-Qura University
Dept. of Computer Engineering
Makkah, Saudi Arabia

Haneen Zamzami[2]
Umm Al-Qura University
Dept. of Computer Science and Engineering
Makkah, Saudi Arabia

Eman Samkri[3]
Umm Al-Qura University
Dept. of Computer Science and Engineering
Makkah, Saudi Arabia

***Abstract*—Encryption is the process of disguising text to ensure the confidentiality of data transmitted from one party to another. Homomorphic encryption is one of the most important encryption-related processes which allows performing operation over encrypted data. Using different public key algorithms, homomorphic encryption can be implemented in any scheme. There are many encryption algorithms to secure operations and data storage, which after calculations can obtain the same results. While there is a considerable contribution and enhancement in the field of homomorphic encryption for various performance metrics, there is still an necessity to clarify the applications dealing with this technology. Recently, many distinguished research papers have been filed to address the need for various applications of homomorphic encryption. Recently, many distinguished research papers have been filed to address the need for various applications of homomorphic encryption. Example of these applications but not limited to : Vehicle to Vehicle (v2v) secure communication, cloud security, Vehicular ad-hoc networks (VANET), Blockchain, E-Voting, Data mining with privacy preserving and healthcare sector. This article aims to introduce a literature survey to close the gap in homomorphic encryption systems and their applications in the protection of privacy. We focus on above-mentioned applications and present our recommendations for future work.**

***Keywords*—Homomorphic encryption; cloud computing; V2V; VANET; blockchain**

I. Introduction

Over one billion devices are connected to the Internet and this number will continue to grow. Security is of the utmost importance especially since the Internet is being used for data storage. The purpose of encryption is to hide information from unauthorized parties and to ensure both the confidentiality and integrity of date. Data can be stored in an encrypted format; however, it must be decrypted before being processed. This can make the data vulnerable and susceptible to attack. Recently, modern cryptology has been able to directly compute encrypted date similar to computations on plaintext using homomorphic encryption (HE). Homomorphic stems from the ancient Greek (homos) meaning "the same" and (morphe) meaning "shape". Homomorphic encryption allows direct computing or processing of data without the need of decryption while enabling one to perform operation on the already encrypted data without knowing anything about it's real value. The homomorphic encryption used in untrusted third parties provides privacy and security for data processing and it offers effective data protection and solves important privacy issues. The concept of HE can be explained metaphorically by using the jewelery shop example: Alice owns the jewelery shop and she does not trust her workers with her jewelery, so, she gets an impenetrable box, hands it off to someone only by using special gloves, and she is the only one who locks it. When Alice wants to make a new piece of jewelery, she locks the materials inside the box. The employees can work on the material inside the box but cannot get it out. Once the work is finished, Alice opens the box with her key and takes out the finished jewelry. This way, the workers produce the jewelery from raw materials without every truly accessing it themselves. In terms of homomorphic encryption, HE is the impenetrable box and the key to the jewelery box is like ciphering the data. The gems represent the data or plaintext and is processed via special gloves without every getting access to the initial data.The final product, such as a ring,represent the initial data.From a historical perspective, the concept of HE was first proposed in 1978 by Rivest, Ronald L., Len Adleman, and Michael L. Dertouzos [1]. Craig Gentry's in 2009 constructed in Ph.D. thesis the first fully homomorphic encryption (FHE) scheme [2]. In 2010,Smart and Vercauteren presented optimization in FHE scheme with smaller chiphertext and key[3]. The remainder of this paper consists of surveying the homomorphic encryption is Section 2, the classification of HE in Section 3, and discusses the homomorphic application is Section 4.

II. Related Work

Homomorphic encryption has been reviewed by [4], [5] earlier. Recently, authors in [6] reviews the state-of-art techniques for incorporating Homomorphic encryption in cloud security. They highlights Homomorphic challenges and limitations for applying HE methods on encrypted data for cloud. Authors in [7] details the required background and related knowledge of HE schemes. Authors in [8] presents an overview of how HE can be utilized for Big data computations. They point out related challenges, opportunities and future enhancements. In [9] summarized the fully homographic encryption properties, applications and techniques. HE libraries were reviewed by [10] as well as an overview of all supporting languages of these libraries. Moreover, the study mentioned the potential applications used by such libraries. Authors in [11] presented a systematic review for HE and illustrates current demand applications and future prospective including security and privacy. In this survey we highlight more potential

application which has not been covered by abovementioned reviews.

III. Operation on Homomorphic Encryption

HE is used to perform operations on encrypted data without decrypting it. The client is the only holder of the secret key. After decryption, the result of any operation is the same as if it was calculation on raw data.

A. Addictive

Encryption schema is called addictive Homomorphic Encryption if

$$E(m_1 + m_2) = E(m_1) + E(m_2) \quad \forall m_1, m_2 \in M$$

Where E is encryption algorithm, M is set of all possible massage and without knowing m_1 or m_2.

B. Multiplicative

Encryption schema is called multiplicative Homomorphic Encryption if

$$E(m_1 * m_2) = E(m_1) * E(m_2) \quad \forall m_1, m_2 \in M$$

Where E is encryption algorithm, M is set of all possible massage and without knowing $m_1$orm_2. For notation in HE it only allows addition and multiplication operations functionally complete set. For any Boolean circuit can design only via XOR gate performs the addition and AND gate performs the multiplication.

IV. Classification of Homomorphic Encryption

A. Partially Homomorphic Encryption (PHE) Schemas

PHE was first attested use of homomorphic encryption introduce by Rivest in 1976.but it was called "privacy homomorphism" [1]. PHE which allows performing single operation either addition or multiplication 'n' number of times on encrypted data, that mean which allows any type of operation without any limitation. There are several algorithms well-knowing for PHE [12] such as:

1) RSA Algorithm (1976):

- Key Generation:
  Step 1: select p and q primes random numbers.
  Step 2: calculate $n = p.q$ and $\phi(n) = (p-1)(q-1)$.
  Step 3: select e such that $gcd(e, \phi(n)) = 1$.
  Step 4: determine d such that $e.d \equiv 1 mod \phi(n)$.
  Step 5: the public key $pk = (e, n)$ and secret key is $sk = (d)$
- Encryption:
  Compute $c = E(m) = m^e(\mod n)$
- Decryption:
  Compute $m = D(E) = c^d(\mod n)$
- Homomorphic Property:
  The homomorphic property of RSA shows following $E(m_1 * m_2)$ directly without ever decrypting it. The RSA is only support homomorphic over multiplicative, it does not support homomorphic over addictive of chiphertexts. Suppose $m_1, m_2 \in M E(m_1) * E(m_2) = [m_1^e(\mod n)] * [m_2^e(\mod n)] = (m_1 * m_2)^e(\mod n) = E(m_1 * m_2)$

2) Elgamal Algorithm (1985):

- Key Generation:
  Step 1: create an efficient cyclic group 'G' of order 'q' with generator 'g'.
  Step 2: choose a random value $x \in \{1, 2, \ldots q-1\}$.
  Step 3: compute $h = g^x$.
  Step 4: the public key is$pk = (G, h, q, g)$ and x as private key.
- Encryption:
  Step 1: chose random number$r \in \{1, 2, \ldots q-1\}$.
  Step 2: compute $c_1 = g^r$and calculate the shared secret key is $S = h^r$.
  Step 3: convert the secret massage m into $m^{'} \in G$.
  Step 4: calculate $c_2 = m^{'} * S$
  Step 5: the ciphertext pair are $c = E(m) = (c_1, c_2) = (g^r, m^{'} * h^r) = (g^r, m^{'} * (g^{x^r})$
- Decryption:
  Step 1: compute shared secret key $s = c_1^x$where x is secret key
  Step 2:$D(E) = c_2.s^{-1} = mg^{xr}.g^{-xr} = m$
- Homomorphic Property:
  $E(m_1) * E(m_2) = (g^{r_1}, m_1^{'}.h^{r_1}) * (g^{r_2}, m_2^{'}.h^{r_2}) = g^{r_1+r_2}, m_1^{'} * m_2^{'} h^{r_1+r_2}) = E(m_1 * m_2)$

3) Pallier Cryptosystem (1999):

- Key Generation:
  Step 1: choose p and q prime random number equal length such that $gcd(pq, (p-1)(q-1)) = 1$
  Step 2: compute $n = pq$ and $\lambda = lcm(p-1, q-1)$ the lcm means Least Common Multiple
  Step 3: choose integer random $g \in Z^*$ such that $gcd(L(g^{\lambda} mod n^2), n) = 1$ with L function define as follow $L(u) = (u-1)/n$
  Step 4: the public key $pk = (n, g)$ and secret key is $sk = (p, q)$
- Encryption:
  Step 1: select random number $r \in Z^*$
  Step 2: compute $c = E(m) = g^m r^n(\mod n^2)$
- Decryption:
  Compute $m = D(E) = (L(c^{\lambda}(mod n^2))/(L(g^{\lambda}(mod n^2))$
- Homomorphic Property:
  $E(m_1) * E(m_2) = [g^(m_1) r_1^n (mod n^2)] * [g^(m_2) r_2^n (mod n^2)] = g^(m_1 + m_2)(r_1 + r_2)^n (mod n^2) = E(m_1 + m_2)$

B. Somewhat Homomorphic Encryption (SWHE) Schemas

SWHE allows performing different operations with limited number of times. There are several SWHE well known examples such as BGN encryption scheme which was the first practical SWHE developed by Beneh-Goh-Nissim BNG Algorithm (2005)

C. Fully Homomorphic Encryption (FHE) Schemas

FHE combines the advantage of PHE with SWHE, which allows to perform unlimited amount of operation for unlimited

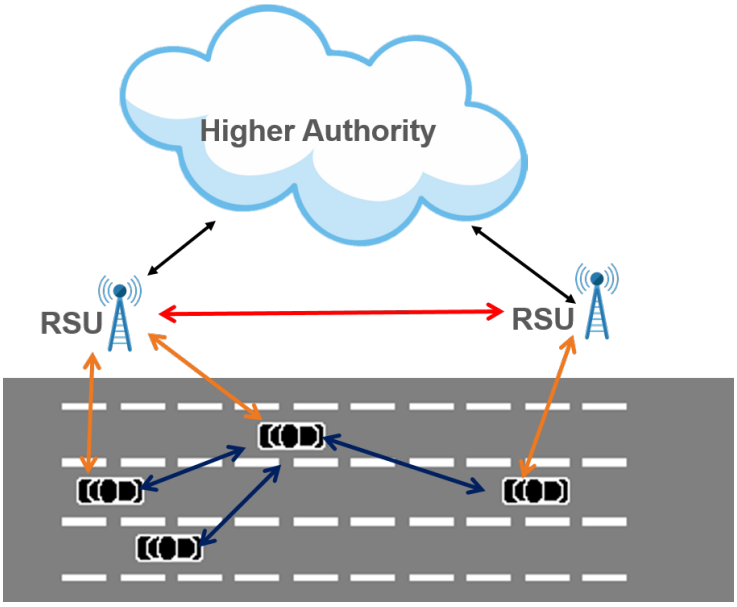

Fig. 1. VANET Communication

number of times. FHE was first practically proposed by Craig Gentry in 2009.

V. Applications of Homomorphic Encryption

A. Vehicle Communication

Among the things right now in the world of technology is a change in the way out the machines that we use interact it. It used to be that the machines we use were just thinks where a button is pushed and something would happen, but now they have progressed to be able to interact with themselves. Imagine a future where vehicles are able to communicate with each other that are known as Vehicle to Vehicle (V2V) technology. V2V provides drivers with warning of potential crash to avoid 60 percent of road accidents according to some statistics. The V2V, also known as Vehicular Ad-hoc NETworks (VANET) technology, uses vehicles as nodes in network [13]. Each vehicle node is equipped with WAVE IEEE 802.11p standard protocol [14], On-board side units (OBDs),the road static infrastructure units called Road Side Unit (RSU)[14] [15]. The three types of vehicular networks most used are Vehicle to Vehicle (V2V), RSU to RSU (I2I) and Vehicle to RSU (V2I). The vehicular network based on wireless protocol is called Dedicated Short Range Communications (DSRC) protocol. The fundamental VANET network scenario is shown below in Fig. 1.

1) VANET applications: are not limited to avoiding road accidents and traffic congestion notifications. The VANET applications are classified according to their purpose

- Safety Applications reduce road accidents and aim to make it easy for helping the driver in specific situations, such as detecting traffic congestion and warning of potential traffic jams. They enhance road safety via such things as collision avoidance by providing emergency alerts in up-to half a second before a crash occurs, which would lead to an avoidance of up-to 60 percent of accidents. Also the vehicle will cooperate by exchanging messages for slow/stopped/post-crash-notification to other vehicles to avoid potential accidents.
- Commercial Applications The main aim of commercial applications is to provide value added services entertainment as web access, travel guidance show the detail location of the nearest restaurant and petrol station, streaming audio and video, and can even provide weather information.

2) Entities in VANETs Security:

- The driver: Responsible for movement of vehicle by making vital decisions and is the most important part of VANET safety chine.
- The vehicle (OBUs): Includes all type of vehicle like cars, bus or truck. The vehicle or nodes in VANET network provide two kinds of normal vehicles that exist in network nodes and the malicious vehicle created by an attacker.
- The infrastructure: It includes RSU which operates in normal way and malicious infrastructure node maybe act as RSU terminal.
- The third party: It includes all direct stakeholders for the system, it may be trusted or semi-trusted third parties. Third party refers to traffic police, the transport regulator, vehicle manufactures and judges. The HE is used to encrypt data so to not be visible for third party but able to process it.
- The attackers: The attacker wants to smash security of normal vehicles to achieve a goal. And it includes external attackers or internal attackers such as authorized vehicles of network VANET.

3) VANETs Security:

- Vehicle privacy: The location of the vehicles should be ensured as much as possible preventing other entities [16]. If the vehicle route leaked, the attacker can trace vehicles which affects driver's safety and privacy.
- Third parties: While third party might needs process the data of entity, it should be secured from malicious usages.
- Authentications: authentication must be supported in VANETs because entities cannot detect if a received massages is normal or malicious [17]. In addition the received data must be consistent with latest data version.
- Real-time availability: Due to a high request of vehicles in the network, it needs to be able to react in real time to various events [18]. And it necessary to have other forms of communication even in the presence of strong communication channels to react with denial of service attacks.

B. Cloud Computing

Before cloud computing, traditional business applications were very complicated. It required a variety amount of tools, hardware, and software and needed an entire team of IT experts to install, update, and maintain them. The "outsourcing" and "server hosting" different names already existed under the cloud computing but the poor performance of processors used, expensive costs of the materials used and slowed internet connections. However the recent advances in technology paved the way for operations with faster processing. The Cloud Computing in simple terms is the offering applications of IT services which are provided by a third party hosted on the internet [19]. The most common service models in cloud computing which are defined in the NIST document Platform as a Service (PaaS) provide a client hosts the hardware and software on its own infrastructure and usually needed for application development over the internet. The user can focus on creating running applications and data sets, Infrastructure as a Service (IaaS) a cloud provider hosts the infrastructure include servers, storage and networking hardware. Software as a Service (SaaS) means delivering software to multiple clients on-demand over the internet. The first priority for researchers is the security challenges and the issue for organizations is to consider moving to the cloud which is the biggest concern.

The security concerns: can be categorized into data security, third party control and finally privacy and legal issues.

- Data security, this is the risk created from losing physical, personal and logical control of data . Such as launching attacks across tenant accounts and also for data remembrance remains as issue due to the replication and distribution of data even after a user has left a cloud provider[20].
- Third-party control, this is the most prime cause of concern for security in the cloud [20]. Third party access to the value of corporate information can lead to a potential loss of intellectual property by enabling a service provider company malicious insider who accesses rights to secret corporate information.
- Privacy and legal issues, data in the cloud is usually globally distributed which raises concerns about data exposure and privacy.

1) Using Homomorphic Encryption in cloud computing: To solve issues in security concerns requires that data stored in the cloud provider are encrypted [21] . However, the client (user) would not be able to use the cloud power to compute outsourcing data because the data would be in an encrypted from. The cloud provider needs to decrypt it to execute the required calculations which affect the data privacy and confidentiality, to perform the computation in encrypted data without ever needing decryption of homomorphic encryption. Since the client is the only holder of the secret key, the result of any operation, it is same as the used in actual data.

C. Signal Processing

A "signal" describes how some physical quantity varies over time or space. Signals can be any function of space or time (sounds waves, images). "Signal Processing" is manipulating a signal to change its characteristics or extract information. Signal processing algorithms can be offloading the computations and computationally intensive to a computationally powerful server may be essential. However, the problem is to perform secure computations of a signal-processing algorithm so that the server does not know the data and does not know the algorithm used if possible.

1) Recent advances in homomorphic encryption:

- In [22] authors suggested ways to solve the privacy related issues through homomorphic encryption. **Paillier's** (1978 to 2008) published several homomorphic encryption schemes to process encrypted data at the same time with only one type of operator. The first broken FHE scheme has been proposed by Gentry in 2009, which is involved with cryptosystems to process both multiplications and additions in the encrypted domain.
- Processing signals in the encrypted domain is a significant challenge. Recently, a lot of researchers achieved specific tailored solutions concerned with many applications. FHE scheme Construction requires the management of the remaining random part called noise to ensure decryption by keeping it below a certain limit. Bootstrapping is the first way to solve this noise problem and was used in Gentry's first FHE scheme.
- Authors in [22] concluded that The Brakerski-Gentry-Vaikuntanathan (BGV) is an asymmetric bits encryption scheme. It is based on lattices, like most FHE schemes. the cryptosystem divided into two versions: first, dealing with integer and second one with integer polynomials [the security associated with ring-learning hardness with errors.
- Homomorphic operations affect times that we need to call the functions Rescale and SwitchKey. Working with FHE schemes hinders us in higher-level programming terms to programs or algorithms that have input limits and a control flow that is independent of encrypted data.
- An experimental study was conducted with an Intel dual core 2 GHz processor on a laptop, using the aforementioned parallel depth cache and SwitchKey. It was found that despite the reality that cryptosystems in the BGV style offer very powerful theoretical safety characteristics, practical parameter setting for both the BGV scheme and its brothers is an issue that still requires further theoretical studies. These numbers are representative as one of the first applications of a fully homomorphic cryptosystem was acquired.

Finally, several measures have been taken to bridge the divide between non-trivial algorithms and their practical, comparatively seamless, FHE systems execution. We can perform easy algorithms on BGV-style cryptosystems homomorphically in a sensible moment in the future. Nevertheless, we have shown that the performance achieved is still far from allowing more computationally engaged algorithms to be executed at a non-prohibitive time. Nevertheless, there is hope that theoretical progress has been

fast since 2009 and that study is only just starting on the "FHE-friendlyness" algorithm, compilation, as well as ad hoc optimized execution, allows for these cryptosystems. As we have suggested in this paper, these latter areas of study can be anticipated to add considerably to the efficiency changes needed to render homomomorphic encryption-based computations, especially in the signal processing sector, are a practical reality.

2) Secure signal processing in the cloud: In [23] authors presented some challenges that multimedia clouds tackle to be fully operational. Cloud services can be introduced in feature of infrastructure, platform as a service and software as a service. There are three types of signal processing apps that highlight the cloud's privacy issue: outsourced biometric identification, e-health, and outsourced adaptive or cooperative filtering. Attaining differential privacy arises at the service provider's expense of a decreased utility as the calculation results are degraded by noise. For cloud applications, this should be evaluated and regarded. In a cloud situation, many signal processing in the encrypted domain (SPED) problems must be faced in order to improve effective privacy-preserving alternatives. Coordination should therefore be improved in the following dimensions: level of privacy, precision, computing load and communication. These freedoms materialize in the technological need for a generic non-interactive alternative for the outsourcing of personal processes, for which cloud computing is a paradigm situation and poses actual difficulties. Defining and quantifying privacy in the cloud is the first and most important problem. There is a wide variety of cloud applications, from very simple spreadsheet apps to synthetic image images rendering. The design of effective FHE that enables the practical use of non-interactive homomorphic processing is the primary region of studies that can contribute to viable alternatives such as the effective personal execution of nonlinear tasks, the effective mixture of outputs from various clients.

3) Smart metering systems: In [24] authors illustrated that smart grids have ongoing spread in many countries but it has many challenges as related to technology and business. Signal processing has important challenges as complex utility function, accuracy loss and also private smart meter measurements, however core smart grid function remain intact.Secure signal processing (SSP) is established to prevent the access of private data by untrustworthy entities as utility providers, while enhancing it as a tool to process the smart meter measurements. The distributed setting of the smart meters and its functions in maintaining privacy with hardware constraints constitute a problem domain for the signal processing research community, it benefits from distributed computing experiences, optimization and accurate communication. Regarding privacy protection, researchers recommended that most studies had to invest in cryptography, getting familiar with its utility and limitations.

4) Biometric Identification: In [25] authors represented the application of techniques of secure two-party computation to biometric identification. This enables computing biometric identification algorithms while protecting the privacy of the biometric data. Many secure computation techniques include biometrics including oblivious transfers, garbled circuits, and garbling a circuit. The impact of using secure multiparty computing techniques on biometric identification systems ' computational costs highlights the system's biometric accuracy. In biometric identification systems, simplified versions of the encoding and matching algorithms are also deployed. These simplifications enhance cost reduction, but they also at the same time decrease accuracy. It includes various techniques as iris and fingerprint. As far as fingerprints are concerned, the minute depiction and advanced range measurements result in more outcomes that are accurate. However, for secure multiparty computation (SMC) methods, neither the depiction nor the corresponding algorithms are suitable. Using streamlined depictions with set size and easy measurements, such as Euclidean distance finger code or Hamming distance binary feature maps, improve privacy at a reasonable computational cost at a slightly less accurate price. These binarization methods are also used as blurred engagement for other methods of privacy preservation.

5) Neighbor methods: In [26] authors discussed three classes of privacy-preserving NN (PPNN) methods, illustrating the building blocks as distance computation and minimum finding that can be realized under privacy constrain .It also addressed secure computation for a wider public of signal processing, new theoretical and applied intersection work on signal processing, cryptography and theory of information. Many studies have been made to carry out the fundamental thoughts and primitive activities that make up PPNN search's construction blocks. Signals for processing were used as outputs for PPNN protocols. Signal processing techniques like press fingerprinting and solid hashing often provide privacy on their own, complementing the PPNN protocol. In safe multiparty computing, several intriguing open issues immediately affect the privacy, velocity, complexity, and versatility of PPNN techniques. Progress in doubly homomorphic encryption is particularly useful in the category of cryptographic methods. Specifically, if the text size and the complexity of the encryption and decryption operations can be managed, it would then be possible to encrypt your data and send it to a cloud-based server that returns a single round of PPNN results. There would be no need for intermediate return and decryption of cipher documents in such a truly outsourced computation configuration, so PPNN protocols would be significantly simplified. Many classic collusions or malicious assault privacy guarantees apply only to information-theoretical techniques computing with more than three sides.

D. HealthCare

- Health care systems run in an environment where sensitive data, must hide from external entities. Over the last few years, e-health records have become more spread. A digital record makes it more reliable and easier to access by different medical facilities.
- Analysts need access to medical records to compute some parts of records so they can access them by HE which supports the sharing of information for healthcare applications. It allows such access without sharing full records in the clear, so we avoid the

violations without disrupting the critical applications. HE protects patient and pharmacy privacy by evaluating the treatment process to obtain safe and effective treatment.

- Homomorphic encryption (HE) offers a tool to protect sensitive data, which can solve the problem of privacy worry. Before sending it to the cloud, the clients are given the chance of encrypting their sensitive information. The cloud will then calculate their encrypted data without the need for the decryption key. HE can be used to the encrypt the data measured by portable medical devices by uploading them on the cloud and making them ready to be used by the authorized user.
- Homomorphic encryption allows computing queries over encrypted data, and returns an encrypted answer to the analyst. The analyst then decrypts the answer on a trusted platform. No one know anything about the data or the results of such queries.
- To preserve the patients privacy information and confidentiality and confidentiality and to use fully homomorphic encryption, the Cloud Computing Platform will only conduct operations using encoded data and provide recipients with the results. No information can therefore be revealed during the communication stage [27].

1) HE applications in Genomics:

- Sharing data with privacy is the most critical point in genomics range; it contains sensitive signals (DNA, magnetic resonance images).
- The immediate development of genome sequencing technology allowing accessing of genome datasets may cause high risks for personal privacy. Using homomorphic encryption to solve this problem so that all the computations can be performed in an untrusted cloud without requiring the decryption key saves the privacy of genome data.
- Fully Homomorphic Encryption (FHE) allow encrypted data to be computed directly in the cloud without the need to bring the data back to the computational.
- The use of HE-Cloud based would be highly beneficial for e-health allowing the uploading of different genomic datasets to the cloud while providing precision medicine and therefore improving the health of patients.

E. Electronic Voting

- Electronic voting (known as e-voting) is a form of decision making that uses electronic means, and the voters make their choices by the aid of a computer to take care of casting and counting votes.
- E-voting has many benefits when compared to traditional voting. Some of these benefits are the faster calculations of results, efficiency, reduce costs, supports different languages, and has a lower chance of human risk and mechanical errors.
- Several e-Voting schemes support the tallying process using the bulletin board (BB). During the vote tallying process each voter gets a receipt that includes some information in encoded form. After the voting closes all encoded votes are published on BB, and each voter can verify that own votes have been recorded as cast using the receipt.
- The purpose of electronic voting is to provide several elaborated characteristics. An e-voting protocol should guarantee privacy to avoid anyone recalling a specific user's ballot, and variance to enable each elector to check that their ballot occurs in the bulletin board and to guarantee that the initial count of ballots applies to legitimate electors' ballots.

1) Secure E-voting using Homomorphic Technology:

- Nowadays, voting is one of the most important activities. The encryption techniques facilitate the implementation of electronic voting. They propose a secure protocol for electronic voting which is suitable for huge votes. The scheme based on Homomorphic Technology is simple, the procedures are transparent, and can be implemented in a practical environment. It allows a voter to exchange untraceable authentic messages, and it uses anonymous channels. The scheme ensures privacy, verifiability and efficiency.
- The structure of the proposed protocol is divided into three phases; the set up phase, in which the parameters are set the voters' registration, the voting phase which is the core of the procedure in which the ballot produced by the voter is processed and finally, the tallying phase in which the result is decrypted [28].
- HE raised as a new solution for e-voting systems. FHE used to design and implement an e-voting system, and it used to provide both operations additive and multiplication.
- New Efficient Multiplicative Homomorphic E-Voting scheme is designed to overcome the disadvantage of the existing schemes. It uses the ElGamal encryption algorithm with distributed decryption. In addition, it uses an efficient and verification mechanism to achieve efficient vote. It employed a grouped tallying mechanism to prevent overflow of votes, while shuffling of groups is used to control the privacy of tallying.

2) E-voting using cloud services:

- The suggested e-voting scheme is comprised of parts, voting servers, authentication servers, newsletters and electors. The distinction between the polling server and the authentication server makes it possible to receive the voting server in any data center service or cloud service provider.
- This scheme offers more privacy, which can be calculated in encrypted type by all ballots recorded in authentication server encrypted with FHE. Without compromising system architecture, the scheme could grow rapidly to more cloud servers. Using cloud facilities for a defined election duration restrains each

election cycle purchasing fresh equipment. Therefore, this is cost effective.

F. Blockchain

A blockchain is an increasing array of documents; each block called frames includes the prior blocks' cryptographic hash, timestamp, and transaction data. The suggested system in [29] and homomorphic obligations depended on the mini-blockchain system. The goal is to make the mini-blockchain more private.
Over the past few years, there has been an outbreak of cryptocurrencies and associated study articles attempting to address issues with the mini-blockchain system that altered the initial blockchain in order to decrease its size and promote enhanced block size.

1) Homomorphic Mini-blockchain Scheme: The mini-blockchain (MBC) was intended to use the "account tree" to enhance the initial blockchain to record each account's equilibrium. Therefore, there is no need to store accounts in the blockchain indefinitely, only the latest purchases and the current account tree. Therefore, the mini-blockchain is much more scalable than the initial blockchain since the mini-blockchain only expands when creating fresh accounts. The mini-blockchain consists of three components:

1) Account tree: the account tree is a Merkle tree (a tree where each leaf node is labeled with an information block number), all the records in a block; each account is an information block with an email and balance.
2) Transaction tree: a Merkle tree for all operations in a particular group, each transaction being a shift to a amount of records.
3) Proof chain: is merely a sequence of frames where each block includes a nonce, the account tree's top hash and the prior block's hash.

- The mini-blockchain works very much like the standard blockchain very much. Each miner separately checks the transaction accuracy and produces a transaction tree with the right operations. Each miner also modifies the account tree to represent the transaction modifications.
- The miner may submit nonce for inclusion in the mini-blockchain to the network. The nodes need only maintain a finite amount of account forests and transaction trees so that the account tree and an elderly block's transaction tree will be removed after a fresh block is formed. Only the whole evidence chain has to be recorded. This scheme only tries to change how accounts and transactions are coded into the mini-blockchain, the homomorphic mini-blockchain (HMBC) scheme provided some improvements to minimum output values, multi-signature addresses, and blind signatures on the scheme. The method used by the HMBC system (Address reuse) is a straightforward study to find reused addresses. Therefore, privacy is essential, the HMBC system enforces the use of single-use addresses while making it possible for customers to have a set address. Each transaction has its own provisional address that is not advertised as belonging to a particular individual. Therefore, nobody can connect them to their owner's identity.
- The transaction numbers will be encrypted in all HMBC. Therefore, they cannot be used to link accounts with identity or filter the blockchain transactions. Because of the use of set addresses, screening buttons, indigenous multi-signature help and blind signing. The mini-blockchain system is more personal and scalable than Bitcoin.

G. Data Mining with Privacy Preserving

Data mining is a computing instrument commonly used today that seeks to obtain helpful data from multiple databases. Nowadays, with the big quantity of data being generated, stored in a remote database (using cloud computing), data privacy and confidentiality concerns arise due to the lack of secure storage and mining security algorithms. It allows arbitrary computation of encrypted information, which is a solution aimed at preserving safety, confidentiality and information privacy. This offers techniques for ensuring the confidentiality and privacy of fully homomorphic encryption based database mining.
Homomorphic encryption is an area of modern cryptography that enables arbitrary computation to be completed on a ciphertext, the encrypted result matching the sequence of operations performed in the original text is still achieved.
Homomorphic encryption is an area of modern cryptography that enables arbitrary computation to be completed on a ciphertext; and the encrypted result that matches the operation sequence performed in the original text is still achieved.
There are two kinds of homomorphic encryption, some of which are homomorphic, and complete homomorphic encryption. The partially homomorphic encryption is described when the quantity of encrypted information operations is limited. Fully homomorphic encryption, however, is a cryptographic system that enables you to perform an arbitrary set of mathematical operations in the resulting cipher text.
Fully homomorphic encryption can be evaluated homomorphically with any circuit, enabling the creation of programs that can run their input encoding to produce their output encryption. Programs like homomorphic never decode their inputs, untrusted third parties can use them and their input data and internal processes are therefore hard to reveal. The existence of a fully homomorphic and effective cryptographic system would have major practical effects on outsourcing of personal computing.

1) Privacy in Data Mining: Data mining helps to extract helpful understanding from big information sets, However, the processes of collecting and disseminating information may pose an inherent risk of confidentiality and privacy. Some private data about individuals, businesses and organizations must be removed unless such data is encoded before it is communicated or released. It has thus become a very significant problem to preserve privacy in information mining.
The term originated as Privacy Preserving Data Mining (PPDM) which relates to the data mining area to prevent unsolicited disclosure of sensitive information. Methods of mining over traditional information statistically analyze and model the

information, while security against disclosure of personal data records is mainly worried with privacy conservation.

The term Data Mining Data Preservation-PPDM has been implemented. Two basic issues in PPDM: 1) the privacy of information compilation and 2) the privacy of several personal businesses during the mining phase of a partitioned information set [30].

The goal of maintaining information mining privacy (PPDM) is that relevant knowledge must be extracted from large amounts of information while protecting sensitive information. Thus, during data mining, the method of maintaining data privacy and confidentiality needs fresh techniques and advances, particularly in the field of modern cryptography.

The surveys have identified address schemes that use fully homomorphic encryption that can be implemented straight in data mining. Fully homomorphic encryption – based on a feasible, efficient solution that ensures the privacy, confidentiality and integrity of mined data. The FHE is a solution for statistical analysis of encoded data while preserving privacy and confidentiality.

VI. Discussion and Future Work

Homomorphic encryption is a promising technology to enable massive valuable operations on encrypted data. We predict more work on how Homomorphic techniques could lead scientist to perform meaningful operations on Blockchain transactions in order to analyze the flow of financial processes. Moreover, we believe homomorphic operations contribute significantly to the field of secure healthcare records. Finally more work is needed to apply the concept of homomorphic encryption for cloud environment. Our future work will be about illustrating a full systematic review of Homomorphic encryption as well as investigating its opportunities and challenges.

VII. Conclusion

In this paper, we give a review on HE developments and its privacy preserving applications. We first showed that it is essential to address the privacy issues in some promising technologies such as cloud computing before they can be widely adopted. HE schemes were considered highly valuable in ensuring data privacy since they allow meaningful computations to be performed in an encrypted form without decrypting the data, especially for outsourcing data to a distrusted party. We reviewed the HE privacy preserving applications in the field of Vehicle communication, Signal processing, Healthcare, Blockchain, Data-mining, Electronic voting and cloud computing.

References

[1] R. Rivest, L. Adleman, and M. Dertouzos, "On data banks and privacy homomorphisms." foundations of secure computation, ed. by ra demillo, et. al," 1978.

[2] C. Gentry and D. Boneh, *A fully homomorphic encryption scheme*. Stanford university Stanford, 2009, vol. 20, no. 09.

[3] N. P. Smart and F. Vercauteren, "Fully homomorphic encryption with relatively small key and ciphertext sizes," in *International Workshop on Public Key Cryptography*. Springer, 2010, pp. 420–443.

[4] C. Fontaine and F. Galand, "A survey of homomorphic encryption for nonspecialists," *EURASIP Journal on Information Security*, vol. 2007, pp. 1–10, 2007.

[5] P. V. Parmar, S. B. Padhar, S. N. Patel, N. I. Bhatt, and R. H. Jhaveri, "Survey of various homomorphic encryption algorithms and schemes," *International Journal of Computer Applications*, vol. 91, no. 8, 2014.

[6] V. Biksham and D. Vasumathi, "Homomorphic encryption techniques for securing data in cloud computing: A survey," *International Journal of Computer Applications*, vol. 975, p. 8887, 2017.

[7] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes: Theory and implementation," *ACM Computing Surveys (CSUR)*, vol. 51, no. 4, pp. 1–35, 2018.

[8] B. Alaya, L. Laouamer, and N. Msilini, "Homomorphic encryption systems statement: Trends and challenges," *Computer Science Review*, vol. 36, p. 100235, 2020.

[9] Z. Brakerski, "Fundamentals of fully homomorphic encryption-a survey." in *Electronic Colloquium on Computational Complexity (ECCC)*, vol. 25, 2018, p. 125.

[10] S. S. Sathya, P. Vepakomma, R. Raskar, R. Ramachandra, and S. Bhattacharya, "A review of homomorphic encryption libraries for secure computation," *arXiv preprint arXiv:1812.02428*, 2018.

[11] M. Alloghani, M. M. Alani, D. Al-Jumeily, T. Baker, J. Mustafina, A. Hussain, and A. J. Aljaaf, "A systematic review on the status and progress of homomorphic encryption technologies," *Journal of Information Security and Applications*, vol. 48, p. 102362, 2019.

[12] Y. M. Sirajudeen and R. Anitha, "Survey on homomorphic encryption," in *International Conference for Phoenixes on Emerging Current Trends in Engineering and Management (PECTEAM 2018)*. Atlantis Press, 2018.

[13] M. Saggi and R. Sandhu, "A survey of vehicular ad hoc network on attacks and security threats in vanets," in *Int. conf. on Research and Innovations in Eng. and Technol.(ICRIET 2014)*, 2014, pp. 19–20.

[14] I. A. Abbasi and A. Shahid Khan, "A review of vehicle to vehicle communication protocols for vanets in the urban environment," *future internet*, vol. 10, no. 2, p. 14, 2018.

[15] R. S. Deshmukh, T. S. Chouhan, and P. Vetrivelan, "Vanets model: Vehicle-to-vehicle, infrastructure-to-infrastructure and vehicle-to-infrastructure communication using ns-3," *International Journal of Current Engineering and Technology*, vol. 5, no. 3, 2015.

[16] J. R. Amin and K. J. Panchal, "A literature survey on homomorphic based secure content distribution in vanet," 2014.

[17] R. Kaur, T. P. Singh, and V. Khajuria, "Security issues in vehicular ad-hoc network (vanet)," in *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*. IEEE, 2018, pp. 884–889.

[18] K. Rabieh, M. M. Mahmoud, M. Azer, and M. Allam, "A secure and privacy-preserving event reporting scheme for vehicular ad hoc networks," *Security and Communication Networks*, vol. 8, no. 17, pp. 3271–3281, 2015.

[19] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling data in the cloud: outsourcing computation without outsourcing control," in *Proceedings of the 2009 ACM workshop on Cloud computing security*, 2009, pp. 85–90.

[20] A. A. Atayero and O. Feyisetan, "Security issues in cloud computing: The potentials of homomorphic encryption," *Journal of Emerging Trends in Computing and Information Sciences*, vol. 2, no. 10, pp. 546–552, 2011.

[21] M. Louk and H. Lim, "Homomorphic encryption in mobile multi cloud computing," in *2015 international conference on information networking (ICOIN)*. IEEE, 2015, pp. 493–497.

[22] C. Aguilar-Melchor, S. Fau, C. Fontaine, G. Gogniat, and R. Sirdey, "Recent advances in homomorphic encryption: A possible future for signal processing in the encrypted domain," *IEEE Signal Processing Magazine*, vol. 30, no. 2, pp. 108–117, 2013.

[23] J. R. Troncoso-Pastoriza and F. Perez-Gonzalez, "Secure signal processing in the cloud: enabling technologies for privacy-preserving multimedia cloud processing," *IEEE Signal Processing Magazine*, vol. 30, no. 2, pp. 29–41, 2013.

[24] Z. Erkin, J. R. Troncoso-Pastoriza, R. L. Lagendijk, and F. Pérez-González, "Privacy-preserving data aggregation in smart metering systems: An overview," *IEEE Signal Processing Magazine*, vol. 30, no. 2, pp. 75–86, 2013.

[25] J. Bringer, H. Chabanne, and A. Patey, "Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends," *IEEE Signal Processing Magazine*, vol. 30, no. 2, pp. 42–52, 2013.

[26] S. Rane and P. T. Boufounos, "Privacy-preserving nearest neighbor methods: Comparing signals without revealing them," *IEEE Signal Processing Magazine*, vol. 30, no. 2, pp. 18–28, 2013.

[27] D. Archer, L. Chen, J. H. Cheon, R. Gilad-Bachrach, R. A. Hallman, Z. Huang, X. Jiang, R. Kumaresan, B. A. Malin, H. Sofia *et al.*, "Applications of homomorphic encryption," *HomomorphicEncryption. org, Redmond WA, Tech. Rep.*, 2017.

[28] S. S. Shinde, S. Shukla, and D. Chitre, "Secure e-voting using homomorphic technology," *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, no. 8, pp. 203–206, 2013.

[29] B. França, "Homomorphic mini-blockchain scheme," 2015.

[30] B. R. J. G. B. d. Q. A. Laécio A. Costa1, "The use of fully homomorphic encryption in data mining with privacy preserving," 2014.