Borneo International Journal eISSN 2636-9826; Vol. 4 (2); 2021; 25-32
Published by *Majmuah Enterprise*
www.majmuah.com

A Study On The Current Trends of Homomorphic Encryption

ABDULLAH ABDUL HALIM[1] and ZOLKIPLI MOHAMAD FADLI[2]

School of Computing, Universiti Utara Malaysia(UUM),Sintok, 06100 Nukit Kayu Hitam,Kedah, MALAYSIA
Email:halim.mozac99@gmail.com[1], m.fadli.zolkipli@uum.edu.my[2]

Received: July 02, 2021
Accepted: July 05, 2021
Online Published: July 07, 2021

Abstract

Encryption is a means to hide text to maintain document confidentiality. One of the key-encryption techniques is homomorphic encryption, which permits operations. Algorithms support heteromorphic encryption of any scheme. Different encryption techniques would get the same result after long computations. Although homomorphic encryption has benefited a great deal, the applications using this invention must be shown. Several fundamental studies have been published lately on the utility of homomorphic encryption systems. More papers on homomorphic encryption have been produced to respond to the requirement for many implementations. This section also includes vehicle-to-encryption (v2v2V) and distributed blockchain networks and healthcare and data industries developments. This article seeks to consolidate current findings on homomorphic encryption and approaches to protecting confidentiality. The major priority is the above implementations.

Keywords: Cloud computing, Managing medical systems, Encryption methods, Homomorphic encryption, blockchain

1. Introduction

The number of internet-linked devices is currently estimated at over one billion due to the amount of data that the internet uses. Encryption helps to guarantee records are confidential and secretive. Data may be retained but must be decrypted before analysis. As a result, there may be serious concerns about safety. Detailed data may be performed in the same way as plaintext calculations with sophisticated calculations in homomorphic encryption (HE) derived from the Greek terms "homo" and "morph." Data may be processed in plain text form without decryption using homomorphic encryption. Hybrid third-party encryption secures all data, which is the anonymity that answers the difficulties of trust.

The HE definition may be represented with a jewelry shop metaphor. Alice runs a jewelry business and does not want to commit its jewels to the staff. As a consequence, she got a mystery package that she only gives to individuals who had special gloves. When Alice finishes her jewelry, her materials are screened within the shell. Employees are doing their job, but they are not erasing things. When Alice opens the box with her ring, raw materials are used without touching them. The finished jewelry is supplied. HE is the riddle, then, and data encryption is the concealed package. Jewelry reflects raw data or plaintext; it is handled with simple gloves. The resultant item, like a bell, is the source. According to his Ph.D. thesis 2009, Rivest, Ronald L., Adleman, and Dertouzos proposed the word for the first time in 1978, generating the first completely homomorphic encryption. In 2010, Smart and Vercorreen created lightweight encryption. Section 2 concentrates on homomorphic encryption, while Section 3 addresses the implementation of HE.

2. Homomorphic Encryption

In this section, we will discuss multiple research comparing the efficiency of several encryption methods and the new Blowfish model. AES has been shown to be faster and more stable than alternative encryption methods. However, the effectiveness of various symmetric key systems is insignificantly different, given that data transfer is considered. Cytomorphic encryption has already been investigated. The latest cloud-based homomorphic encryption techniques have recently been examined. The problem and danger of homomorphic encryption of encrypted data are addressed. They investigate the context and the starting point. According to the authors, HE will carry out significant Big Data computations. They discover issues, possibilities and examine how they might be addressed. The techniques for encryption were extensively specified and patented. We have put up a list of all HE libraries. Possible uses for these libraries have also been considered. An in-depth HE examination, encompassing new perspectives and possibilities, was undertaken. Finally, we highlight more applications that you may not have applied for yet.

3. Operation On Homomorphic Encryption

a) Addictive

It is addictive Homomorphic Encryption if

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

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

b) Multiplicative

It is multiplicative Homomorphic Encryption if

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

4. Classification of Homomorphic Encryption

a) Vehicle Communication

The interaction between our devices is becoming a prominent topic in the realm of technology. Previously, the robots we utilized believed it would happen by clicking a button, but they can connect immediately. Consider a world in which automobiles converse, a phenomenon known as communication between vehicles and vehicles (V2V). V2V notifies drivers of the likelihood of an accident according to a number of estimations, preventing 60% of traffic casualties. Vehicles operate as nodes in the V2V network, known as ad-hoc vehicle networks (VANET). Each vehicle node with the standard protocol WAVE IEEE 802.11p, onboard side units, and roadside units, which constitute static road infrastructure units (RSU). Figure 1 shows the whole VANET network setup.

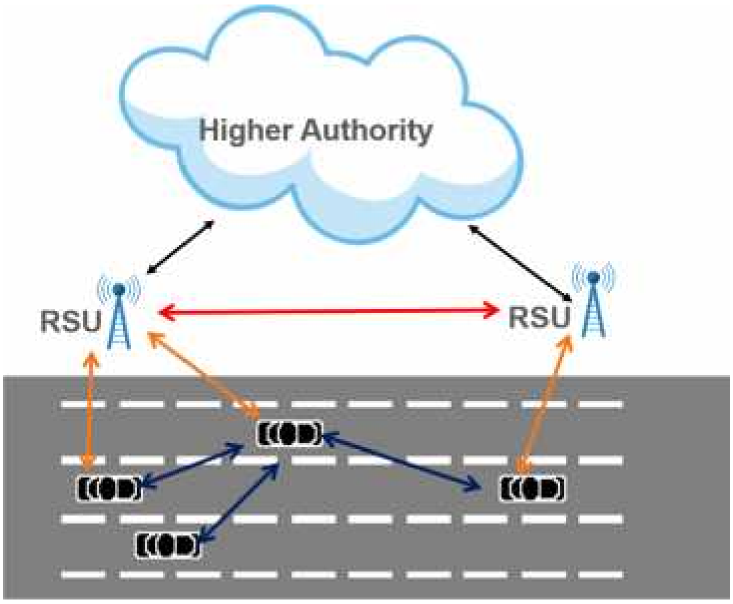

Figure 1: Gurjeevan Singh (2020), VANET Communication, A Study of New Trends in Blowfish Algorithm.

VANET deployments include traffic accident prevention and the provision of congestion alerts for transportation. The VANET applications are thus categorized explicitly in accordance with the intended use:

Safety applications are developed to help drivers avoid road accidents by facilitating their support in particular scenarios. It helps make the route safer by sending emergency alerts in seconds before an accident, possibly averting 60% collisions. The vehicle must also communicate with other automobiles by sending warning messages slow/stop/post-crash.

i) *Entities in VANETs Security*

A driver is a key element in the VANET safety chain, as they ultimately take vital decision-making on the movement of the vehicle.

Vehicle (OBU): All forms of vehicle, including cars, buses, and trucks, are included in this category. This Network, Two types of automobiles or nodes, are supported: normal cars embedded in network nodes and malicious cars produced by an attacker.

RSU is an infrastructural component that usually works, and a node of malicious infrastructure can behave as an RSU terminal.

The direct stakeholders of both schemes are represented by a third party that might be partly trusted or trusted. Third parties include officials of traffic, roads, automobile manufacturers, and judges. The HE is used to encrypt data so as not to be seen by a third party yet to allow processing.

The assailants: To attack a target effectively, the attacker must violate the safety of normal vehicles. It also covers former or internal attackers, such as VANET-approved network vehicles.

ii) *VANET's Security*

Vehicle privacy: To the degree possible, vehicle whereabouts should be kept hidden from others. If a car's path is being disclosed, the intruder tracks it and endangers the driver's security and privacy.

While a third party may process the information of an entity, it has to be protected against harmful usage.

VANETs need authentication because people cannot tell if the communication they receive is intended or harmful. The data obtained must also comply with the latest version of the data.

Due to the enormous demand for automobiles of the network, it must react to diverse occurrences in real-time. Thus, extra communication channels are required to respond to the denial of service assaults, even when communication networks are strong.

b) *Cloud Computing*

Cloud computing is a third-party mechanism that provides IT services through the internet. Security concerns include data security, access by other parties, and privacy and legal challenges. The top objective of researchers in security issues is to examine the most important issue of cloud computing. As cloud data is often disseminated internationally, data exposure, privacy, and privacy problems are raised. The phrases "outsourcing" and "domain hosting" have remained unchanged owing to poor processor efficiency, expensive material costs, and inadequate internet connections. Their usage has become archaic.

i) *Use of homomorphic cloud encryption*

The data of the cloud provider must be safeguarded. As the data is encrypted, however, the customer (user) will not employ cloud computing resources to offshore the data. In order to carry out analyses of encrypted data without having to decrypt it, the cloud provider must address this problem in order to execute the required computations and threaten confidentiality and privacy. Since only the customer has access to the secret key, all actions on correct data are the same.

c) *Signal Processing*

The term "signal" refers to the physical amount of movement across time or place. Signals can take on any dimension of time or space (sounds, waves, images). In the processing of signals, a sign is modified to modify or extract information from its characteristics. It may thus be important to offload computations from heavy signal processing techniques to a computer-efficient server. However, safe analyses of the signal processing techniques are difficult to do, such that the server is unaware of the data or, if possible, of the approach used.

i) *Recent advances in homomorphic encryption*

Recently, researchers have devised solutions for a number of applications. The creation of the FHE method needs the control of the remaining random variable, called noise. Working with FHE programs makes it more difficult to design programs or algorithms with input limitations and a control flow without encryption. In the future, basic algorithms will be homomorphically executed on BGV-style cryptosystems, but the results gained are not adequate to enable more computer-intensive algorithms to be done time-efficiently. The authors conclude that while research into the FHE-friendliness algorithm, compilation, and ad-hoc optimized execution permits these cryptosystems, it is reasonable to believe that the theoretical progress has been quick since 2009. These later areas of study are expected to contribute significantly to the efficiency of homomorphic encryption.

ii) *Secure cloud signal processing*

The authors examined a number of issues for the effective operation of multimedia clouds. Cloud providers are also infrastructure instances as a service, application as a service, or platform as a service. The three cloud-based signal processing techniques with privacy problems within the cloud are externalized biometric, e-health, and externalized adaptive or cooperative filtering. The authors examined a number of issues for the effective operation of multimedia clouds. Cloud providers are also infrastructure instances as a service, application as a service, or platform as a service. The three cloud-based signal processing techniques with privacy problems within the cloud are externalized biometric, e-health, and externalized adaptive or cooperative filtering. Due to the depletion of the noise-induced computation results, the service provider must compromise its utility to achieve different confidentiality. This should be studied and evaluated for cloud-based software development. Many issues connected to encrypted domain (SPED) signal processing must be resolved to boost the efficiency of cloud-based privacy-preserving solutions.
The following synchronization factors may thus be enhanced: safety, precision, computational load, and connection. Technologically speaking, these freedoms are manifested by the requirement for a standardized, non-interactive method for personal outsourcing systems, for which cloud computing is paradigmatic and dangerous. The main aim is to describe and assess the privacy of the cloud. Many cloud-based programs, from basic tablets to synthetic picture rendering, are available. The immediate field of study may lead to actual choices such as the successful personal realization of nonlinear jobs and convincing output mixtures from many customers for creating strong FHE that allows the practical implementation of non-interactive homomorphic computing.

iii) *Smart metering systems*

While smart grids in several nations gain pace, they confront different technical and commercial hurdles. Complex utility functions, loss of precision, and new private meters are all important difficulties to signal to process. The core operation of the intelligent grid, on the other hand, is unaffected. SSP was developed to stop unsustainable companies such as utility companies from accessing sensitive data while enhancing its intelligent meter measurement processing skills. The distributed smart meter setup and its role in protecting secrecy while operating within hardware constraints are a study topic of distributed computing competence, optimization, and correct communication for signal processing researchers. The experts believe most of the studies should focus on encryption to secure their data and become familiar with the advantages and disadvantages.

iv) Biometric Identification

The authors investigated how stable biometric identification approaches may be deployed by two parties. This facilitates the calculation of biometric recognition algorithms while ensuring the confidentiality of biometric data. Biometrics are employed in many computing procedures, such as blind transfers, twisted loops, and obfuscation direction. The impact of secure multi-party calculation methodologies on the cost of biometric authentication systems reveals the biometric accuracy of the system. Biometric recognition systems also employ easier encoding and matching techniques. Although these simplifications are cost-effective, they forfeit accuracy. It uses a number of approaches, including the recognition of iris and fingerprints. The accurate representation and advanced range calculations guarantee that the results are more dependable in terms of fingerprints. However, neither the specification nor the associated techniques are appropriate for safe multipart computing (SMC). With superficial representations with a constant dimension and basic proportions, such as Euclidean finger distance coding or Hamming binary function mappings, confidentiality may be increased at low calculation costs but with a minor loss of accuracy. Furthermore, these binarization approaches create an uncertain relationship between these efforts and other measures for protecting privacy.

v) Neighbour Methods

The authors examined three distinct approaches to privacy-preserving neural networks (PPNNs). Often, signal processing techniques such as press fingerprinting and robust hashing are combined with the PPNN protocol to increase anonymity. The confidentiality, efficiency, complexity, and adaptability of PPNN techniques are all impacted by some interesting open issues in secure multi-party computing. Numerous established privacy protections against collusion or malicious attack extend only to computing with more than three parties through information-theoretic techniques.

d) Health Care

Health services work in an environment where secret facts must be protected from prying eyes. As a consequence, electronic health records in recent years have become more common. A multimedia format is also more reliable and gives access to a larger range of medical services.

In order to compute certain documentation sections for HE access, analysts require access to medical records to promote data sharing in medical applications. It allows such access without us having to submit whole forms that enable us to avoid infractions while keeping sensitive applications. In addition, HE maintains the privacy of patients and pharmacists by carrying out care evaluation processes to guarantee the provision of necessary and suitable services to patients.

Homomorphic encryption (HE) is a kind of data protection that may reduce privacy issues. Clients may encrypt private data until it is sent to the cloud. Then the cloud would measure its encrypted data without the decryption key. For instance, HE may encrypt data acquired by mobile medical devices and transfer it to the cloud to access it by authorized individuals.
Analysts will query encrypted data and use homomorphic encryption to obtain encrypted responses. Then the analyst decrypts the answer via a secure network. No one knows what the specifics or results of these inquiries are.

The Cloud Computing Platform is confined to executing operations on coded data and providing the data to recipients to ensure the privacy and confidentiality of patients and offer usable homomorphic encryption. As a consequence, during the contact stage, no information may be posted.

i) HE applications in Genomics

The most critical point in genomics is data sharing while maintaining privacy; this requires susceptible signals such as magnetic resonance images and DNA.

The fast advancement of genomic sequencing, which enables access to large databases of human genomes, can create significant privacy risks. Genome data privacy is maintained by resolving this problem with homomorphic encryption, allowing all computations to be done in an untrusted cloud without the decryption key.

FHE allows encrypted data directly to be computed in the cloud so that the data is not returned to the calculator.

The usage of HE-cloud in e-health is very helpful, as it will allow the cloud-based storage of diverse genomic datasets while providing precision medicine and enhancing patient health.

e) E-Voting System

E-Voting System is a means of determining decisions in which electors take their selections via the use of a voting gadget.

There are various advantages to electronic voting versus human polling. Accelerated performance estimates, enhanced dependability, savings in costs, and multilingual assistance are only some of the benefits of reducing the risk of human and technological failure.
Many electronic voting methods help the ballot board in the process (BB). Each voter receives throughout the voting process-specific encoded information. After the survey is complete, all encoded votes are given to the BB, and every individual uses the ticket to make sure their voices are cast.

Electronic voting tends to have a number of different features. An electronic voting system can assure both anonymity, as no one can recall the voting by a single user, and diversity, as each voter may check the appearance of the ballot on the ballot board and that the original count includes the accurate votes of the voters.

i) Secure E-voting using Homomorphic

Voting has developed into a vital practice. When cryptography is used, electronic voting becomes much simpler to enforce. They suggest a sturdily constructed electronic voting protocol capable of handling vast volumes of votes. The homomorphic technology-based scheme is straightforward. The processes are specific and can be carried out in a suitable setting. This is accomplished by luring voters into exchanging untraceable authentic messages through anonymous networks. Thus, the device protects users' privacy and verifiability.

The suggested protocol is split into three phases: a setup phase that establishes the criteria for voter registration, a polling phase that processes the voter's ballot, and a tallying phase that decrypts the verdict.

HE was created as a state-of-the-art electronic voting device. FHE invented and commercialized the automated voting machine that both addition and multiplication operations were performed.

The New Efficient Multiplicative Homomorphic E-Voting scheme was developed to address the limitations of existing voting schemes. ElGamal and distributed decryption techniques are used. Additionally, a valid vote is ensured by the use of an effective and verifiable voting mechanism. It used a clustered tallying method to stop option saturation, with party shuffling to ensure the tallying process stayed confidential.

ii) Cloud-based E-Voting System

The electronic vote infrastructure suggested is divided into voting servers, authentication servers, newsletters, and members. Since the poll server is authentication independent, it may be accessed from any data center or cloud service provider.

This scheme increases privacy by providing for the calculation of all ballots stored in an FHE-encrypted authentication server. The project could be extended to include more cloud servers without jeopardizing the system architecture. Utilizing cloud providers for a set amount of time reduces the need to buy additional infrastructure during each election cycle. As a result, it is cost-effective.

f) Blockchain

A blockchain is an ever-growing set of documents, each of which contains the cryptographic hash, timestamp, and transaction data from the previous block. The suggested scheme in and homomorphic roles is sponsored by the mini-blockchain method. The aim is to raise the level of mini-privacy. blockchain technology's

Over the past few years, there has been a boom in the number of cryptocurrencies and related academic articles, both of which attempt to solve problems with a mini-blockchain scheme that modifies the original blockchain reduces the size and promotes larger chains.

i) Mini-blockchain homomorphic scheme

The mini-Blockchain (MBC) has been designed to improve the original blockchain using an "account tree" to store individual accounts' balances. As a result, the blockchain needs to store the most recent transactions and the current account tree in perpetuity. As a result, the mini-blockchain is significantly more flexible than the primary blockchain, which only evolves in reaction to new account development. The mini-blockchain consists of three components:

1) The account tree is a Merkle tree (a tree where each node is marked with a block number), and every account is a block with an email address and a balance.

2) It represented all operations within a given category, with Each transaction that represents numerous record updates.

3) A proof chain is just a succession of frames, each with a nonce, the top hash of the account tree, and the last hash of the block.

The MBC architecture is more individualized and scalable. Each transaction is associated with a unique temporary address not reported as belonging to a specific person. As a consequence, they cannot be related to their owner's name. Minimum performance values, multi-signature addresses, and blind signatures have all been improved due to the project.

g) Privacy conservation data mining

Homomorphic encryption is a subfield of modern cryptography that enables any calculation on a ciphertext to be performed. It is still possible to obtain an encrypted result that corresponds to the original text's sequence of operations. It enables the computation of encrypted data in either direction while preserving data protection, confidentiality, and privacy. A homomorphic scheme would have a significant effect on personal computing outsourcing.

ii) Data Mining Privacy

Homomorphic encryption is a contemporary cryptography topic that allows any ciphertext computing to be carried out. It is still possible to obtain an encrypted result that corresponds to the original text's sequence of operations. It enables the computation of encrypted data in either direction while preserving data protection, confidentiality, and privacy. A homomorphic scheme would have a significant effect on personal computing outsourcing.

5. Future Work

HE appears to be a promising technique for conducting functional operations on large amounts of encrypted data on a large scale. We anticipate additional research into how homomorphic schemes can allow scientists to conduct relevant Blockchain transactions tasks to assess financial process flows. Additionally, we think that homomorphic procedures provide an important contribution to the area of safe medical records. Last but not least, further study is necessary to broaden the theory of homomorphic cloud encryption. In the future, we shall examine homomorphic encryption carefully and explain its pros and cons.

6. Conclusions

This article examines HE innovations and their privacy-preserving implementations. We first demonstrated that before widespread adoption of any promising technologies, such as cloud computing, privacy issues must be addressed. However, because they can conduct realistic calculations in an encrypted form with no data decryption, HE schemes were considered extremely valuable for ensuring data privacy, especially when data was outsourced to a distrusted community. Next, we explored the applications of HE that preserve in-vehicle privacy communication, signal processing, healthcare, blockchain, information mining, e-voting, and cloud computing.

Acknowledgments

The authors would like to thank all School of Computing members who were involved in this study. This study was conducted for the purpose of the System and Network Security Research Project. This work was supported by the Ministry of Higher Education Malaysia and Universiti Utara Malaysia.

References

C. Aguilar-Melchor, S. Fau, C. Fontaine, G. Gogniat, and R. Sirdey (2013), "Recent advances in homomorphic encryption: A possible future for signal processing in the encrypted domain," IEEE Signal Processing Magazine

Z. Erkin, J. R. Troncoso-Pastoriza, R. L. Lagendijk, and F. Perez- Gonzalez (2013), "Privacy-preserving data aggregation in smart metering systems: An overview," IEEE Signal Processing Magazine

R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina (2009), "Controlling data in the cloud: outsourcing computation without outsourcing control," in Proceedings of the 2009 ACM workshop on Cloud computing security

A. Nadeem and M. Y. Javed (2005), A performance comparison of data encryption algorithms," Information and Communication Technologies

Afaf M. Ali Al-Neaimi, Rehab F. Hassan (2011), New Approach for Modifying Blowfish Algorithm Using 4-States keys, The 5th International Conference on Information Technology

Diaa Salama Abdul. Elminaam, Hatem Abdul Kader and Mohie Mohamed Hadhoud (2010) Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types, International Journal of Network Security

M.Umaparvathi, Dr. Dharmishtan K Varughese (2010), Evaluation of Symmetric Encryption Algorithms for MANETs, IEEE