International Journal of Scientific Engineering and Research (IJSER)
ISSN (Online): 2347-3878
Impact Factor (2020): 6.733

# An Analysis of Homomorphic Encryption in Latest Technologies

**Karan Chawla**

Ashoka University

**Abstract:** ***A particular time-consuming evaluation algorithm is supported by homomorphic encryption, a type of encryption. This approach enables specific operations to be performed on the ciphertext without the need for a secret key. This review article looks at the most recent technologies that can safeguard data via homomorphic encryption such as Vehicular Ad Hoc Networks, Internet of Things for Mobile and Internet of Things for Cloud Computing and Internet of Medical Things. A safe computing solution for vehicle data has been devised employing partial homomorphic encryption, or Fully Homomorphic Encryption (FHE), for the majority of protocols. Only homomorphic addition or homomorphic multiplication is supported by partial homomorphic encryption, and implementing these operations requires additional rounds of interaction. This is a concern because the unusually long execution time of homomorphic multiplication makes it difficult to maintain real-time communication on VANETs. Use of Partial or Full homomorphic encryption for real-time communication in VANETs might be a good option since it ensures both addition and multiplication to take place an infinite number of times. It is crucial to stress that while permitting third-party cloud computations, data privacy are preserved. However HE comes at a higher expense in terms of processing because of its inherent complexity. Data traffic increases as ciphertext size increases, increasing the cost of transmission in terms of energy utilization and fees per transmitted byte. Activities in IoMT must be performed directly on network nodes that healthcare services manage and that are situated closer to the device layer in order to reduce latency. Similar research is needed to reduce the distance between the healthcare services and the device layer in order to reduce latency. The current study does not address the issue of a secure communication link between the device and base station for the Internet of Medical Things.***

**Keywords:** Homomorphic Encryption, Technology, Vehicular Ad Hoc Networks, Internet of Things, Cloud Computing

## 1. Introduction

An encryption method known as homomorphic encryption works using a specific evaluation algorithm. This approach enables specific operations to be performed on the ciphertext without the need for a secret key.

From privacy homomorphism, which Rivest proposed for financial applications in 1978, homomorphic encryption was born. The final ciphertext produced by homomorphic encryption can be decrypted to produce the same outcome as performing the same procedures on the plaintext. There are three main types of homomorphic encryption, depending on the kinds and quantities of homomorphic operations. Partial homomorphic encryption, which was the first type of homomorphic encryption, only allows for homomorphic addition or homomorphic multiplication. A limited set of homomorphic addition and homomorphic multiplication operations are supported by somewhat homomorphic encryption. After that, fully homomorphic encryption (FHE) provides an endless number of homomorphic addition and homomorphic multiplication operations. Homomorphic encryption allows for perfect analysis of vehicle data by an untrusted third party without disclosing any personal information about users. The user then receives the encrypted result. The user's own secret key can be used to access the analysis's findings. The key to securely analyzing vehicle data is to create an effective and secure homomorphic encryption technique. There is no effective way to build an efficient secure computation method based on homomorphic encryption since homomorphic operations have a poor level of efficiency. It is also necessary to investigate various forms of secure computation.

With the assistance of many technologies, vehicular ad hoc networks (VANETs) are expected to increase transportation efficiency, reduce accidents, offer better mobility service opportunities, and reduce environmental harm. Many sectors and facets of daily life are fast recognising the value of the Internet of Things (IoT). The Internet of Things (IoT), which is aiding the creation of more complex applications, is transforming a number of industries, including wearable technology, smart cities, and so-called Industry 4.0.

### Vehicular Ad Hoc Networks

Vehicular ad hoc networks (VANETs) are anticipated to improve transportation effectiveness, decrease accidents, provide excellent mobility service possibilities, and lessen environmental damage with the aid of several technologies. Because of advancements in communication, wireless sensor, and infrastructure technologies, VANETs will continue to grow consistently and gradually over the coming ten years. One of the largest marketplaces in the world, the worldwide VANETs market is anticipated to reach $1.5 trillion in 2030. The creation of usable VANETs is being accelerated by numerous nations and significant automakers.

In VANETs, the raw vehicular data is initially gathered and must be processed by computing software from a third party. The final computation's output has a variety of uses; for instance, some helpful vehicle data might be provided to the user in response to their query's specifications. Data aggregation is another application that can be used to transmit, compress, and filter vehicle data.

Vehicle data includes authentic and original user information, such as location and biometric data. The processing of data frequently affects people's right to privacy, the security of their property, and even their life. A

mathematical model needs to be created in order to analyze vehicle data. Additionally, because vehicle data is given to an unreliable third party for computation, it is likely that vehicle data will be obtained unlawfully, falsified, altered, or abandoned during the data distribution and computation processes.

We can encrypt vehicle data using a conventional encryption process to safeguard user privacy. Unfortunately, encrypted vehicle data is inflexible and difficult to evaluate.

Homomorphic encryption enables the analysis of encrypted user data by an untrusted Cloud server without the need for decryption. The cost of communication between the user and the cloud server is also minimal. The secure analysis of vehicle data, the secure prediction of teen dropout risks, and the secure distribution of power in smart grids are all made possible by homomorphic encryption.

The following is a description of various partial homomorphic encryption techniques. The RSA cryptographic method, which enables homomorphic multiplication, was first presented in 1978. The factorization of a big integer forms the foundation of its security. Created the homomorphic addition-supporting GM probabilistic encryption method in 1982. Its security is predicated on the quadratic residue hypothesis. Based on the discrete logarithm issue, a cryptographic method that enables homomorphic multiplication was developed in 1985. Under the premise of decisional composite residuosity, a cryptographic method that permitted homomorphic addition was built in 1999. A cryptographic technique that allowed for an unlimited number of homomorphic additions and one homomorphic multiplication operation was initially proposed in 2005.

The on-board device communicates with other on-board units or road-side units using the IEEE 802.11p radio protocol. It is frequently included in vehicles. A user interface, a particular interface that can be used to connect with other on-board units, a network facility that can be used for short-range wireless communication and resources like random access memory for data storage and retrieval are all found in an on-board unit.

The on-board device can offer wireless radio access, ad hoc and geographic routing, network congestion control, dependable message delivery, data security, and internet protocol mobility, among other services.

Typically, the application unit is integrated inside a vehicle. It could be a specialized gadget used for certain secures applications, or it might be a more broad device like a personal digital assistant. Only through the roadside unit, which manages all mobility and network activities, can the application unit connect with the network. A wired or wireless channel is used for communication between the application unit and the roadside unit. It could share a physical cell with the roadside unit.

The road-side unit is frequently installed as a wave device along both sides of the street or at specific locations, including at intersections or next to parking lots. It may be utilized for some security applications, such as early warning of traffic accidents or low bridges, as well as to broaden the communication range of VANETs by dispersing messages to other on-board units and broadcasting messages to other road-side units. It may also be used to access the Internet, in addition.

This domain includes the application unit and on-board unit. Wireless or wired communication is both possible. The wireless U. S. B. or ultra-wideband technology is the foundation for wireless communication. The on-board unit also provides a communication pathway for the application unit.

There are several vehicles assigned with on-board units and the road-side unit in the ad hoc domain. There are also two other types of communications in this field, and they are explained as follows.

Inter-vehicle communication is useful for enhancing the visibility of on-board gadgets, driving efficiency, and traffic safety in general. As a result, it has caught the interest of academic scholars and businesses, particularly those in the United States, the European Union, and Japan. Vehicles are linked together in inter-vehicle communication using on-board components. A car and another vehicle can speak to one another if a wireless link is present between them. Communication between vehicles simply involves one hop. Instead, a particular routing protocol must be used for communication between two vehicles; only then may multi-hop communication be used.

The infrastructure domain can be linked to the roadside unit. The on-board device can then access the infrastructure domain after that. Moreover, some hosts can be reached by the on-board device through cellular radio networks such the universal mobile telecommunications system (UMTS), WiMAX, high-speed downlink packet access, and general packet radio service.

Studying fundamental operations like comparison, division, inner product, set operations, etc. is important in order to construct homomorphic encryption-based safe computing for VANETs. The following is a list of some secure basic operations that are available. An encoding method that can change a private set into a private vector was initially proposed by research. The secure subset issue may then be converted to calculations involving private vectors. The authors created a unique and effective private subset computing protocol based on this encoding method and the Paillier scheme. This protocol is secure in both malicious and semi-honest models.

An innovative encoding method that may transform user input into a unique vector is first proposed by research. Research suggested a secure minimal protocol for the computation of the minimum of many integers privately based on this encoding approach. Under the partially honest model, this protocol is secure. Moreover, the maximum and union of sets may be securely computed using this protocol. A vector encoding technique that can transform an integer into a vector was developed by research. The computation of the vector can then be used to solve the comparison

problem.

Modular multiplications are necessary for this approach, where L is the vector's length. This protocol has a maximum communication cost of two rounds. The authors developed a protocol that makes use of a geometric technique to safely compare rational values.

Information theory, this protocol is secure.

$6L + 4$

Modular multiplications are necessary for this approach, where L is the vector's length. This protocol has a maximum communication cost of two rounds. The authors developed a protocol that makes use of a geometric technique to safely compare rational values. Information theory, this protocol is secure.

Others have converted the greater-than issue into the calculation of the vector using the vectorization approach. The authors then created a secure protocol based on the Paillier algorithm that could resolve the greater-than issue in a single iteration. Modular multiplications are necessary for this protocol, where q is the Paillier scheme modulus and s is the vector's dimension.

This protocol just requires one round of communication. A technique to calculate the area of a triangle, which is formed by three private points, was originally developed, and it was inspired by computational geometry. It might be used to solve problems involving the comparison of two rational values. The authors suggested a safe comparison procedure for rational numbers based on this technique and the Paillier algorithm. Low computational complexity characterizes this protocol.
A secure routing report technique in VANETs was developed to preserve the privacy of vehicles. There are four entities in the network model of this mechanism, which are the department of motor vehicles, the traffic control center, roadside units, and cars.

WiMAX, 4G, or similar quick communication technology connects the traffic control center with the roadside equipment. Roadside units are provided with segment-based encrypted routing data. In addition, vehicle data are combined by road-side units using the Paillier method. The traffic control center will then get the aggregated data and calculate the number of cars in each section without disclosing any personal information about the individual vehicles.

In 2018, researchers suggested a safe task recomposition solution for crowdsensing in a vehicle fog computing system based on the Paillier algorithm. The vehicular fog node, the Cloud service provider, the trusted authority, and cars with restricted communication and compute capabilities are all depicted in the method's architecture. These entities can communicate with one another via dedicated short-range communication networks and 5G mobile communication technologies. Together hybrid subtasks form a ciphertext. By using the Paillier method and a sophisticated encryption standard, each perceived subtask is encrypted (AES). After that, it is sent to a nearby vehicular fog node. Thereafter, only the Paillier method is used to encrypt newly created ciphertexts from encrypted subtasks. All of the gathered subtasks will be combined by the vehicular fog node. The cloud service provider receives the compiled result. The cloud service provider recovers the aggregation of each subtask and evaluates the dependability based on the obtained aggregated results. The experimental findings demonstrate that the suggested technique has reasonable computational and communication costs.

In 2016, vehicle-to-grid networks suggested a secure data management system based on Ozdemir's homomorphic encryption technique for the security of data aggregation and dissemination in smart grids. The technique contains clients, a database proxy, a central database server, and an embedded database, as indicated in the framework's architecture. The integrated database is useful for keeping electrical vehicle data that has been encrypted. Then these encrypted data are subjected to local aggregation. The central database server then determines the ultimate aggregate result based on these local aggregation results. The database proxy will conceal sensitive information in a query sent by the client to the main database server.

The client receives the encrypted query result once the processed query has been executed by the central database server. Also, this framework's security was examined under a number of well-known cyberattacks, such as the replay assault, interface attack, known plaintext attack, etc. The experimental outcomes demonstrated the effectiveness of the suggested framework.

**Cloud Based IOT Systems**

The Internet of Things (IoT) is quickly becoming a significant asset in several industries and aspects of daily life. The Internet of Things (IoT) is revolutionizing a variety of industries, from wearable technology to smart cities to so-called Industry 4.0, by opening up new market opportunities and facilitating the development of more sophisticated applications. According to a Gartner report, there will be over 20 billion gadgets linked to the Internet in 2020, creating a huge quantity of data in the process. All of that data must be acquired and evaluated in order to provide useful information for future decision-making; as a result, the cloud is rapidly becoming a crucial component of the IoT ecosystem.

With the IoT's quick development, several problems and worries start to surface. Security and privacy concerns rank as the top IoT barriers, according to a poll by International Data Corporation (IDC). As there are more linked devices, the security dangers increase, necessitating greater protection. The necessary security level is significantly greater when actuators are being monitored remotely. The importance of cybersecurity has increased, and well-publicized hacks on major corporations. In addition to major organizations, Small-and Medium-sized Enterprises (SMEs) are another target of these attacks. Latency problems are also brought on by the rise of real-time IoT applications, particularly in the healthcare and industrial sectors. They require an instantaneous response and, as such, it is crucial to minimize communication delays among smart devices.

Homomorphic Encryption (HE), a novel encryption technique, is gaining ground as a remedy for privacy problems. HE permits operations on encrypted data, in contrast to traditional encryption algorithms like Advanced Encryption Standard (AES) or Rivest-Shamir-Adleman (RSA). IoT data flow privacy from end to end is provided by this feature. Data may be safely stored in public clouds using HE, and computations like Machine Learning (ML) predictions can be made there without gaining access to the user's data. This method does, however, result in an increase in computing cost and packet size, which suggests a rise in network delay. Network Coding is a potential approach to deal with latency problems (NC).

Its characteristics make it possible to enhance the resilience and decrease the latency of various topologies. In particular, it enhances distributed storage system redundancy effectiveness and wireless sensor network (WSN) connections, as well as data download speed.

It is made up, as indicated, of end-point devices that are in charge of gathering data and a multi-cloud environment that stores and analyzes the information obtained. An intermediary network connects the multi-cloud environment and end nodes. Last but not least, end users have access to end-point device data via cloud services. Moreover, HE is capable of offering end-to-end privacy, where data is encrypted on the devices and decrypted at the destination.

They are sent through the WSN and the Internet to a multi-cloud environment, where sophisticated calculations may be done on the encrypted data while still ensuring user privacy. The installation of NC across the design addresses the non-negligible increase in packet size and computational cost, and therefore, the rise in delay. As a result, it may be utilized not just via the WSN but also for the upload, recovery, and acquisition of multi-cloud data.

It may be claimed that this vision is supported by a number of research projects that are pointing in the direction of this overall design. The advantages of implementing both NC and HE across the entire vertical of the architecture are numerous: it gives IoT applications end-to-end data privacy, enables end users to use public cloud computing services and storage without running the risk of compromising sensitive data, and decreases latency.

NC departs from the conventional store-and-forward transmission paradigm by allowing any network node to combine received packets into coded packets that may be decoded at the destination in addition to storing and forwarding them. Random Linear Network Coding (RLNC), one of the most popular schemes, linearly mixes packets using coefficients selected at random from a finite field.

In order to deliver considerable gains in terms of communication resilience, stability, throughput, and latency, RLNC takes advantage of the peculiarities of the broadcast nature of wireless medium, which encourages node collaboration.

One of RLNC's most important characteristics is that it is rateless, which eliminates the requirement for a specific packet as the receiver simply needs to receive enough linearly independent packet combinations to restore the original data. As a result, the coupon collector issue is resolved. As a result, distributed storage systems like P2P or multi-cloud settings benefit greatly from using RLNC as a tool. It is possible to decrease the additional data download time required under heavily loaded situations and to increase the storage's redundancy efficiency.

They are sent through the WSN and the Internet to a multi-cloud environment, where sophisticated calculations may be done on the encrypted data while still ensuring user privacy. The installation of NC across the design addresses the non-negligible increase in packet size and computational cost, and therefore, the rise in delay. As a result, it may be utilized not just via the WSN but also for the upload, recovery, and acquisition of multi-cloud data.

HE is a ground-breaking encryption method that is based on asymmetric or public key cryptography that allows computation over encrypted data owing to its homomorphic characteristic. It enables the execution of specific operations over the ciphertext that yield an encrypted result that, when decoded, is identical to what would have been achieved had the operation been executed in plaintext. It differs from traditional encryption methods like AES, RSA, the International Data Encryption Algorithm (IDEA), and Twofish due to the aforementioned.

Based on the operations that each algorithm supports, there are three separate algorithms. Gentry developed Fully Homomorphic Encryption (FHE), which permits arbitrary calculations on ciphertext. A system called Slightly Homomorphic Encryption (SHE) may assess functions with a modest level of complexity or depth. The operations that Partially Homomorphic Encryption (PHE) can carry out on ciphertext are constrained.

In a wide range of applications, HE may be a potent instrument for assisting in the protection of data privacy. Data may be processed and stored safely on the cloud. It may be helpful for distant electronic or online voting, for instance. HE also lets in outsiders who can offer a variety of computing services and statistical analysis, including ML prediction, of private data, such that used in medical applications or sensorized machine defect detection.

The typical IoT scenarios are made up of a lot of devices, like WSN, that send their data to the cloud where it is processed for real-time or in-rest analysis. Thereafter, any client or end-user can see the data or remotely monitor it. Cloud computing offers high levels of scalability and flexibility, Big Data management, and the capacity to do advanced data analytics that enable acquiring insightful data. As a result, it is increasingly indispensable for Industry 4.0 and Internet of Things applications.

The characteristics of NC are very helpful for improving the reliability and cutting down on delays in WSN communications. The authors demonstrated the advantages over direct communication strategy and developed a cooperative NC-based transmission technique for spectrum

and energy efficiency in Wireless Body Area Networks (WBANs). When it comes to vehicular ad-hoc networks (VANETs) and the Internet of Vehicles (IoV), NC can increase transmission reliability and restore the original message in the case of a problem or message loss.

Regarding cloud deployment, a multi-cloud strategy offers fault tolerance and high availability to the system since it enables the use of redundancy to more effectively restore lost data when employing NC. NC may also be used to distribute data around several clouds, with those that have superior circumstances in terms of cost, download speed, or congestion, among other things, benefitting. For instance, data is dispersed over the clouds in order to lower the cost of storage and improve system stability. The data is also stored based on the cost of the cloud resources. To cut down on total download time, data may also be spread based on each cloud's pace of download.

As previously stated, HE can guarantee complete privacy. WSN sensors and gateways may conduct operations like spatiotemporal correlation, which can be utilized to drastically minimize data traffic, by making use of these qualities. As demonstrated in, HE can also be a useful technique for data aggregation in Vehicle-to-Grid (V2G) networks. As the data aggregation simply calls for additive operations, PHE is sufficient to meet the privacy protection criteria. By using cloud-based infrastructures, HE makes it possible to do robust data analytics in the cloud and remote monitoring while protecting the privacy of sensitive medical data, for instance. Moreover, it enables secret ML algorithm execution.

For instance, to apply deep learning to data stored in several third-party clouds without jeopardizing secrecy, the authors introduced a multi-key FHE technique.

The advantages of merging these technologies have been examined in the literature, given the advantages that NC and HE each offer to cloud-based IoT designs. The authors showed how secure cloud storage and secure NC are related. To prevent data and tag pollution attacks in RLNC, for example, homomorphic Message Authentication Code (MAC) techniques can be used. The authors suggested a homomorphic signature-based NC-based secure cloud storage system that allows public data auditing and is resistant to data loss, pollution assault, and repetition attack. On the other hand, the authors suggested a new approach to guaranteeing data and tag privacy.

For RLNC in Smart Grids, they provide a distributed privacy-preserving method. The packet's tag, or coefficient, is encrypted using a HE function in addition to its data, which are encrypted using a traditional encryption technique. By taking use of the homomorphic characteristic, forwarder nodes can recode the coefficients without revealing the data or the coefficients themselves.

Because there are more ways to attack the network as there are more smart devices, security and privacy issues are growing along with the exponential expansion of IoT devices linked to the Internet. As a result, ensuring device trust is one of the criteria in IoT contexts, which may be particularly difficult given how varied and large-scale these networks are. Data privacy must be protected in order to deliver reliable and secure systems. Illegal users or hackers who get access to IoT devices and have the ability to remotely view or manipulate those devices may endanger data privacy. Also, businesses like banks or cloud providers have simple access to the confidential information of their customers.

The validity, integrity, and privacy of data must be guaranteed, as well as secure communication between all parties involved, because data security threats might arise at any time.

End-to-end security hence becomes important and may be handled by using the algorithms. Data only needs to be decrypted at the end-user because of their characteristics, even if they need to execute operations on them. Moreover, NC would be shielded from threats from pollutants. Although HE has undeniable potential, one significant drawback is its high computational cost. Even for simple tasks, it involves extremely sophisticated computations, and the encryption process generates ciphertexts of vast size. This is a serious issue, especially for IoT protocols and applications that often use devices with limited resources.

From the lowest provided privacy level to the greatest, the privacy level is shown on the one hand in ascending order. A scale from 1 to 5 is used to reflect the likelihood that operations can be carried out on encrypted data, with 1 indicating that fewer operations are possible and 5 indicating that any operation may be carried out on encrypted data. On the other hand, the metrics for the amount of the ciphertext generated by the encryption method, as well as its complexity and execution time, are shown from their greatest level to their lowest level in descending order. Using the complexity measure as an illustration, we can see that the complexity level drops as we approach the graph's edge.

With the employment of more potent approaches, it can be seen that the size of the encrypted data, as well as the complexity and execution time of the algorithm, grow. If the data are in plaintext, any operation is possible in terms of permitted operations. The RSA/AES methods, on the other hand, do not permit calculating encrypted data. HE approaches provide for a variety of operations depending on the algorithm. Just summing encrypted data is permitted by Paillier, FV may only conduct operations of restricted depth, and FHE permits any operation but is constrained by its complexity. In terms of privacy, if we don't use data encryption, we don't provide any data protection. The employment of HE algorithms, on the other hand, offers complete data privacy.

Traditional algorithms, on the other hand, provide a middle level of security because they need to be decrypted in order to be used for any activity.

Instant problem detection is essential to averting major catastrophes in applications like factory automation, where the machinery and systems of production lines are controlled in real-time, or autonomous driving, where immediate

vehicle-to-vehicle communications and environment detection are necessary. Even non-instantaneous feedback applications need to respond almost instantly. These systems depend on their choices on the data they have acquired, thus the data must be gathered, sent, and analyzed quickly.

In both heavily loaded cloud installations and congested networks, NC helps reduce latency. However, the adoption of NC creates certain difficulties in the future with regard to the latency specifications of real-time applications. While using NC, intermediate nodes must be able to carry out activities quickly enough to recode and send received data to the following node in real time. IoT devices have limited processing capability, therefore using them might cause additional delays if the procedure is very complicated. As a result, simpler coding techniques and algorithms will be needed.

Also, current packet scheduling and routing methods may need to be reexamined in order to improve transmissions between intermediate nodes and decrease latencies of distributed systems while satisfying the strict requirements of real-time scenarios. Data encryption causes extra latency because intermediate nodes must first decode packets they receive before recombining them. As data are only decrypted at their final destination and it frees the intermediate nodes from this burden, the usage of HE will play an enabling role in this respect.

IoT designs must continue to function even if the entire system or a component of it malfunctions. Robustness is a crucial quality, particularly in industrial and medical applications. The system needs to offer services that are self-configurable and capable of handling external disturbances without impacting the application. For dispersed systems where data is sent between several distinct devices across the network, reliable communication is also essential between gateways, cloud services, and applications. In order to fulfill the needs of real-time applications, continuous data availability is also crucial. Cloud service providers provide redundancy and backup alternatives to meet application demands. Yet, the entire infrastructure might malfunction.

As stated above, transferring NC-based data combinations into a multi-cloud environment can increase the architecture's dependability and availability. Because of extra data combinations positioned in the remaining clouds, it will be possible to restore lost data even if the entire cloud infrastructure collapses. As a result, reliance on a single cloud provider is lessened, and system autonomy is increased. Nevertheless, data download speed may suffer in an effort to guarantee dependability. Designing new codes and distribution systems that can maintain a trade-off between reliability and performance may thus be essential. Data migration across various cloud platforms also poses a substantial issue. Data transfer and distribution strategies will first require further work. Second, switching from one cloud provider to another may prove challenging owing to vendor lock-in.

**Internet of Medical Things (IOMT)**

Internet of Things (IoT) sensors are commonly used in intelligent healthcare systems in smart cities to monitor patient health. Human sensor devices include smart thermometers, Q-bands, pacemakers linked to medical alert systems, which monitor and alarm during cardiac arrests, proximity tracers, which look for possible new clusters of infectious diseases, and smart thermometers, which record a patient's body temperature. Hospital plasma storage is monitored by temperature sensors, which are also used for upcoming research. These gadgets are among the few medical sensors that keep an eye on a person's wellbeing. There is always a chance that hackers aiming to steal personal data and hold hospitals and medical research institutes to ransom will intercept confidential patient information.

Doctors and nurses were forced to switch to pen and paper and deal with urgent issues as a result of ransomware attacks on hospitals like Universal Health, which prevented them from accessing vital and necessary patient data. In the USA, more than 250 hospitals and clinics were impacted, which led to a delay in reactions from crucial machines that measure things like blood pressure, oxygen levels, and heart rate. In addition, the prevalence of ransomware attacks on public servers exposes private data processing to risk of data loss and compromises patient healthcare.

The significance of this work is in protecting the privacy of the computations made by healthcare apps on public servers and securing the data generated by medical devices. Healthcare systems need to make decisions quickly for high-risk patients who are dealing with the consequences of a diagnosis. Yet, due to the enormous amount of processing and storage resources available, much current research relies on doing computations on the cloud layer. As findings are sent from the Cloud back to devices, latency increases cause diagnostic delays for patients, who need to make decisions quickly for their health.

Because medical data is processed and exchanged often and in significant volumes in the context of healthcare services, communication overhead between the Cloud-IoT channel also rises as the volume of medical data does. In order to enable real-time applications, data analysis at the edge layer, which includes base stations, moves computing closer to the device layer by lowering latency, bandwidth, and network delay. Moreover, Multi-Access Edge Computing prevents network bottlenecks and congestion caused by the lengthy transmission channel from the device layer to the cloud layer (MAEC).

The cloud layer has a number of security flaws that allow hackers to access data and change or manipulate it as a result of cyberattacks like ransomware. Moreover, data analysis on the Cloud necessitates computing on servers owned by independent developers and businesses. On the dark web, information is sold to third-party vendors by marketing and advertising companies. Some malevolent people purchase data to launch frauds, create false adverts, and keep information hostage. Attackers are prevented from accessing confidential medical information by utilizing homomorphic encryption to encrypt data. Moreover, data analysis does not necessitate data decryption at the server-side, preventing unauthorized parties from accessing data supplied by

Internet of Medical Things (IoMT) devices.

When a user or an intelligent healthcare application lacks control over the privacy of the data, secret sharing is the best option for completing computations safely and confidently on unreliable Cloud servers.

The foundation of homomorphic encryption is the idea that data may be processed without the need to decode it. One of the guiding principles for using the encryption system in untrusted server systems is data confidentiality. In contrast to other encryption methods, homomorphic encryption treats encrypted data as plaintext and permits algebraic operations like addition and multiplication on it directly.

Current work on protecting IoMT data focuses on homomorphic encryption, which protects data privacy. Others recommended an incentive-based technique to persuade users to exchange data with the healthcare network and provided a novel privacy-enhanced data fusion mechanism for homomorphic encryption of data. The procedure combines mobile edge computing (M. E. C.) with IoMT, with a number of M. E. C. servers supporting COVID-19 applications, storing data, processing requests, and doing analyses. All data computation is done at the edge layer rather than using resources from the cloud layer. To conduct neural network operations directly on floating-point data with little computing complexity, some developed a completely homomorphic encryption technique. The key is susceptible to decryption in the proposed Matrix Operation for Randomization or Encryption-based homomorphic encryption scheme.

Data security and confidentiality problems can come from an attacker determining the encryption key utilizing an optimisation problem and a huge collection of key pairs. For security, raw data is uploaded to a private, external server on the Cloud, however the suggested solution does not safeguard it during transmission. Others have put up a federated learning verification-based paradigm for protecting patient privacy. In order to protect the privacy of medical information while data learning is carried out both centrally and locally, the model integrates homomorphic encryption, blockchain technology, and federated learning. The local dataset that each client, user, or device collects and sends to the central server is used to train the model. A framework for medical image security has been suggested by several. Several studies encrypt IoMT data using other algorithms, including the Elliptic Curve Digital Signature Algorithm (ECDSA), and technologies like blockchains.

Others used the ECDSA to create dual digital signatures in order to solve the security and privacy issues with IoMT data. With dual signatures, data transfer from devices to the cloud layer via the edge is validated from reliable sources. Because edge layer resources are more agile and have less resource restrictions than IoMT devices, signature verification is done utilizing edge layer resources. The goal of the research is to stop the edge from accessing encrypted data and the cloud from discovering the identity of the user. Data that has been decrypted at the cloud is vulnerable to hostile cyberattacks and other servers accessing the data.

For greater speed and user privacy, some have suggested a decentralized architecture integrating data sharing and offloading techniques; data computation is done at the M. E. C. This architecture is unusual in that it uses smart contracts to provide authentication and traceability for data exchange. Smart contracts that validate the user's identity remove the need for a central authority or other organization to approve a user access request before the user may submit data. As data is saved in blocks, data integrity is preserved, and any tampering will be reflected in changed hash values. The direct storage of hash values in smart contracts, which enables direct data access in the Interplanetary File System, reduces the amount of time needed to seek for data.

Data Confidentiality: When data is sent from IoMT devices to the edge layer, ownership and control of the data are transferred. When communicated to external network layers, such as the base station at the edge layer, the devices' physical security is compromised. In order to prevent any unauthorized party from reading the data in plaintext, data confidentiality mechanisms must be in place. Information must be encrypted in order to prevent user or device identification in any way. In order to share the data on untrusted edge and cloud servers, devices or apps supporting healthcare systems are required.

Data Integrity: Data transported from IoMT devices to unreliable edge servers are susceptible to infiltration attempts from outside sources, leading to data tampering and lowering the accuracy of the calculation results for patient data. Data integrity must be preserved during calculation and transfer.

Privacy-Preservation: Privacy is a major issue when sending private and sensitive user data across dubious external networks like cloud servers and edge nodes.

Third-party edge and cloud service providers have access to a wealth of sensitive information about the personal data of users and can sell that information for profit. Users experience added stress and financial loss as a result of fraudulent, targeted marketing efforts and scams that are made possible by data sold to other organizations.

It is crucial to encrypt patient identities and medical diagnosis data utilizing public-key encryption methods and pseudo-random permutation.

Data transferred between edge entities is frequently the property of external service providers, who demand that data be encrypted before conducting mathematical calculations. Edge service providers can execute computations using encryption techniques like homomorphic encryption without the need for the user to decode the data.

IoMT devices, such as Bluetooth Low Energy and Low Power Wide Area Network devices that continuously transfer data to the DU, are sensors with low-power batteries and processing capacity. Homomorphic encryption, which enables addition and multiplication operations, is used at the base station to encrypt data.

To carry out computations on the encrypted data, DU

requests the base station. Because of its low processing capacity, a single edge node struggles to perform demanding operational duties. To spread the computation job and assure computation privacy, the proposed approach uses numerous VENs to implement the multi-party computation (MPC) paradigm.

The choice and deployment of various VENs are based on the physical position of IoMT devices; a hospital has hundreds of patients, each of whom uses several sensors dispersed around the facility in different geographic locations. Because physical edge nodes lack the capacity necessary to manage the massive data produced by healthcare apps, they are avoided for data computation tasks. To acquire resources and dynamically supply resources to the DU, several cloud services are employed. A single unreliable third-party service provider is prevented from storing extra and multiplying computing operations and learning the data analysis process by the selection of various cloud services.

The outputs of compute operations performed on homomorphically encrypted data are sent closer to the devices by virtual edge nodes than by cloud services, which reduces the latency of time-sensitive output transmission to the DU.

By offering dynamic node allocation and resource provisioning services, VENs help the DU. Because of the restricted processing resources integrated into base stations, a single or group of close physical edge nodes cannot provide real-time services. This study makes the assumption that the healthcare service would use on-demand payment services in conjunction with cloud-based resource services like Amazon Web Services and Google Cloud. A highly scalable selection of edge nodes is offered by on-demand payment-based services, guaranteeing that complicated processes be completed without delay.

We presume that the neighborhood's physical edge nodes, like a base station, rely on the extensive computational resources of the cloud computing environment's huge computer infrastructure. The limited computing power of physical edge nodes makes it difficult for IoMT devices in the healthcare network to process large amounts of data. The goal is to create a number of virtual nodes that can compute data equally utilizing the homomorphic secret sharing mechanism.

Homomorphic encryption is used to protect the privacy of data stored in local edge nodes and cloud settings. In order to protect user privacy at the data fusion centre, some have conducted a hypothesis test to determine the accuracy of the data that has been acquired. Their study focuses on applying homomorphic encryption to protect patient privacy and ensure the accuracy of data. At nearby physical data centers, where mathematical processes are exposed to other parties, computations of encrypted data are carried out. The crucial issue of concealing operations from unreliable parties is not addressed.

Others employed linear functions and keys to encrypt data. Yet, a hacker can access the keys using a large database of values linked to encrypted keys.

Evaluation findings demonstrate that an optimisation issue exposes the ciphertext data utilized for calculation as plaintext.

## 2. Analysis

In this area, research has mostly concentrated on how to do complex procedures while using fewer computing resources. Secure computing should also support a variety of dataset kinds. The majority of the aforementioned systems used general homomorphic encryption methods. Also, they seldom ever took multiplicative homomorphic approaches' depth and the accuracy of vehicle data into account. As a result, setting up the appropriate scheme parameters is impossible. This is detrimental to the development of a secure calculation technique for vehicle data that is effective and reliable.

The majority of protocols have been developed based on partial homomorphic encryption, or FHE, with the goal of creating a safe computing mechanism for vehicle data. Only homomorphic addition or homomorphic multiplication are supported by partial homomorphic encryption; the implementation of these operations necessitates extra rounds of interaction. The running time of homomorphic multiplication is unreasonably lengthy even though FHE enables an infinite number of homomorphic addition and multiplication operations. Thus, it is challenging to ensure real-time communication in VANETs. Use of partially or fully homomorphic encryption for real-time communication in VANETs might be a good option since it ensures both addition and multiplication to take place an infinite number of times. Moreover, the transmission of public keys and ciphertext may use up all of the available bandwidth in VANETs due to their huge sizes.

Data aggregation and data searching are often used techniques in the secure computing of vehicle data. Vehicle data must first be encoded before these approaches may be used. As only integers and floats are now supported by the standard encoding techniques, new encoding strategies for more complex data types should be considered. The fast implementation of these methods using homomorphic addition and homomorphic multiplication is a difficulty since homomorphic encryption only enables homomorphic addition and homomorphic multiplication. These algorithms use the Fourier series approach to simplify some challenging operations like exponentiation and logarithms into addition and multiplication. Then, homomorphic procedures may be used to put them into practice. Yet, even with great message accuracy, the efficacy of homomorphic processes cannot be guaranteed. Multi-user data is encrypted into ciphertexts, which are typically under the same secret key, for the secure calculation of vehicle data. Multi-user data security, however, could be compromised. Partial homomorphic encryption can permit operations on the ciphertexts with various secret keys with the aid of additional rounds of interaction. To resolve this problem, we may alternatively employ the secure multiparty computation method. A secure multiparty computation protocol may be created using multi-key FHE and threshold FHE. Although operations on

ciphertexts with various secret keys are supported by multi-key FHE, sadly, the effectiveness of homomorphic operations and ciphertext conversion declines with both the number of parties and the depth of homomorphic multiplication. When compared to multi-key FHE, threshold FHE is more effective. Nevertheless, threshold FHE necessitates more rounds of interaction.

It is important to emphasize that data privacy is maintained when allowing third-party cloud calculations. Because of its innate complexity, HE, however, entails higher computing costs. Data traffic grows as it produces larger ciphertext, which results in higher transmission costs in terms of both energy use and fees per sent byte. It can be difficult to apply this encryption strategy since IoT devices are typically resource-constrained and IoT protocols are frequently lightweight protocols. Yet, given to its enormous privacy advantages, HE is a topic that attracts a lot of attention and is consequently developing quickly. In fact, more efficient algorithms are already appearing. Moreover, SHE or PHE can be employed in applications like vote counting that call for simpler processes.

For the Internet of Medical Things, The absence of a secure communication route between the device and base station is not addressed by present research. To assess and provide results for intelligent healthcare systems, medical data must constantly be computed using a variety of artificial intelligence techniques. Data is exposed to unreliable cloud servers when computer activities are exposed, making it easy to determine the type of data stored in the cloud. Third-party cloud services sometimes rely on selling user data to additional untrustworthy parties who then utilize it for their marketing campaigns or to advertise and support shady business practices. Systems that disperse compute processes across local IoT devices rely on sensor hardware with lax built-in security mechanisms. Cyberattacks like botnet attacks put operations at risk from bad actors. In order to decrease latency, activities must be carried out directly on network nodes that healthcare services manage and are located closer to the device layer.

## 3. Conclusion

Without decryption, homomorphic encryption enables calculations on the ciphertext. Homomorphic encryption is utilized to build the secure computation technique due to its benefits. Hence, safe computing based on homomorphic encryption is researched in VANETs. Majority of the research today in VANETs is focused on generalized homomorphic encryption methods. The majority of protocols have been developed using partial homomorphic encryption, or FHE, with the goal of creating a secure computing method for vehicle data. Partial homomorphic encryption only supports homomorphic addition or homomorphic multiplication, and the implementation of these operations necessitates additional rounds of interaction. This is a problem since it is challenging to sustain real-time communication on VANETs due to the excessively high execution time of homomorphic multiplication.

In IOT applications, the protection of data privacy must be emphasized while permitting third-party cloud computations. However HE comes with greater computational expenses due to its inherent complexity. The latency of the overall design may be decreased by integrating NC throughout. Complex NC systems might introduce extra delays because of the objects' limited processing power, which can be problematic for real-time applications. Despite this, these methods may be modified to work with current IoT protocols, as was indicated above. Due to a lack of standardization, data and application transfer between various cloud providers causes interoperability issues. Also, the heterogeneity of IoT continues to be an obvious issue for the architecture's integration of many technologies. Thus, it is essential to do this type of study in order to develop new platforms and technologies for handling.

## 4. Future Directions

The majority of current VANETs research focuses on generalized homomorphic encryption techniques. Studying multiplicative homomorphic encryption techniques would be a fascinating and useful research area. A good research area would be to look into somewhat and fully homomorphic encryption methods for the application of real-time communication in VANETs.

As mentioned in the IOT applications, homomorphic encryptions may be used for vote counting because they merely call for easier communication. For the architecture's integration of several technologies, the heterogeneity of IoT continues to be a clear problem. So, it is crucial to do this kind of research in order to create new handling platforms and technologies.

In IoMT, in order to decrease latency, Activities must be carried out directly on network nodes that healthcare services administer and that are located closer to the device layer. The current study does not address the lack of a secure communication connection between the device and base station for the Internet of Medical Things, and comparable research is required to shorten the distance between the healthcare services and the device layer in order to minimize latency.

## References

[1] Haider, S.; Abbas, G.; Abbas, Z. H.; Boudjit, S.; Halim, Z. P-DACCA: A probabilistic direction-aware cooperative collision avoidance scheme for VANETs. *Future Gener. Comput. Syst.*2020, *103*, 1-13.
[2] Cheon, J. H.; Stehlé, D. Fully homomophic encryption over the integers revisited. In Proceedings of the Advances in Cryptology—EUROCRYPT 2015, Sofia, Bulgaria, 26-30 April 2015; pp.513-536.
[3] Benarroch, D.; Brakerski, Z.; Lepoint, T. FHE over the integers: Decomposed and batched in the post-quantum regime. In Proceedings of the Public-Key Cryptography—PKC 2017, Amsterdam, The Netherlands, 28-31 March 2017; pp.271-301.
[4] Brakerski, Z.; Vaikuntanathan, V. Efficient fully homomorphic encryption from (standard) LWE. In Proceedings of the IEEE 52nd Annual Symposium on

Foundations of Computer Science, Palm Springs, CA, USA, 22-25 October 2011; pp.97-106.
[5] Micciancio, D.; Peikert, C. Hardness of SIS and LWE with small parameters. In Proceedings of the Advances in Cryptology—CRYPTO 2013, Santa Barbara, CA, USA, 18-22 August 2013; pp.21-39.
[6] Chen, Z.; Wang, J.; Zhang, Z.; Song, X. A fully homomorphic encryption scheme with better key size. *China Commun.2***014**, *11*, 82-92.
[7] Brakerski, Z. Fully homomorphic encryption without modulus switching from classical GapSVP. In Proceedings of the Advances in Cryptology—CRYPTO 2012, Santa Barbara, CA, USA, 19-23 August 2012; pp.868-886.
[8] Chen, Z.; Song, X.; Zhao, X. A multi-bit fully homomorphic encryption with better key size from LWE. *J. Comput. Res. Dev.2***016**, *53*, 2216-2223.
[9] Gentry, C.; Halevi, S.; Smart, N. P. Homomorphic evaluation of the AES circuit. In Proceedings of the Advances in Cryptology—CRYPTO 2012, Santa Barbara, CA, USA, 19-23 August 2012; pp.850-867.
[10] Stehlé, D.; Steinfeld, R. Making NTRU as secure as worst-case problems over ideal lattices. In Proceedings of the Advances in Cryptology—EUROCRYPT 2011, Tallinn, Estonia, 15-19 May 2011; pp.27-47.
[11] Bos, J. W.; Lauter, K.; Loftus, J.; Naehrig, M. Improved security for a ring-based fully homomorphic encryption scheme. In Proceedings of the IMA International Conference on Cryptography and Coding, Oxford, UK, 17-19 December 2013; pp.45-64.
[12] Chen, L.; Zhang, Z. Bootstrapping fully homomorphic encryption with ring plaintexts within polynomial noise. In Proceedings of the International Conference on Provable Security, Xi'an, China, 23-25 October 2017; pp.285-304.
[13] Dowlin, N.; Gilad-Bachrach, R.; Laine, K.; Lauter, K.; Naehrig, M.; Wernsing, J. Manual for using homomorphic encryption for bioinformatics. *Proc. IEEE* **2017**, *105*, 552-567.
[14] Chen, H.; Han, K. Homomorphic lower digits removal and improved FHE bootstrapping. In Proceedings of the Advances in Cryptology—EUROCRYPT 2018, Tel Aviv, Israel, 29 April-3 May 2018; pp.315-337.
[15] Cheon, J. H.; Kim, A.; Kim, M.; Song, Y. Homomorphic encryption for arithmetic of approximate numbers. In Proceedings of the Advances in Cryptology—ASIACRYPT 2017, Hong Kong, China, 3-7 December 2017; pp.409-437.
[16] Cheon, J. H.; Han, K.; Kim, A.; Kim, M.; Song, Y. Bootstrapping for approximate homomorphic encryption. In Proceedings of the Advances in Cryptology—EUROCRYPT 2018, Tel Aviv, Israel, 29 April-3 May 2018; pp.360-384.
[17] Vizitiu, A.; Niţă, C. I.; Puiu, A.; Suciu, C.; Itu, L. M. Applying deep neural networks over homomorphic encrypted medical data. *Comput. Math. Methods Med.2***020**, *2020*, 26.
[18] Cheng, W.; Ou, W.; Yin, X.; Yan, W.; Liu, D.; Liu, C. A Privacy-Protection Model for Patients. *Secur. Commun. Netw.2***020**, *2020*, 12.
[19] Yang, Y.; Xiao, X.; Cai, X.; Zhang, W. A secure and high visual-quality framework for medical images by contrast-enhancement reversible data hiding and homomorphic Encryption. *IEEE Access* **2019**, *7*, 96900-96911.
[20] Cano, M. D.; Cañavate-Sanchez, A. Preserving data privacy in the internet of medical things using dual signature ECDSA. *Secur. Commun. Netw.2***020**, *2020*, 4960964.
[21] Mohan, M.; Devi, M. K. K.; Prakash, V. J. Homomorphic encryption-state of the art. In Proceedings of the 2017 International Conference on Intelligent Computing and Control (I2C2), Coimbatore, Tamil Nadu, India, 23-24 June 2017; pp.1-6.
[22] Naehrig, M.; Lauter, K.; Vaikuntanathan, V. Can homomorphic encryption be practical? In Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop, Chicago, IL, USA, 21 October 2011; pp.113-124.
[23] Wang, L.; Li, J.; Ahmad, H. Challenges of fully homomorphic encryptions for the internet of things. *IEICE Trans. Inf. Syst.2***016**, *E99D*, 1982-1990.
[24] Shafagh, H.; Hithnawi, A.; Burkhalter, L.; Fischli, P.; Duquennoy, S. Secure Sharing of Partially Homomorphic Encrypted IoT Data. In Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems, Delft, The Netherlands, 6-8 November 2017
[25] Will, M. A.; Nicholson, B.; Tiehuis, M.; Ko, R. K. L. Secure Voting in the Cloud Using Homomorphic Encryption and Mobile Agents. In Proceedings of the 2015 International Conference on Cloud Computing Research and Innovation (ICCCRI), Singapore, 26-27 October 2015; pp.173-184.