https://rijournals.com/engineering-and-physical-sciences/

RESEARCH INVENTION JOURNAL OF ENGINEERING AND PHYSICAL SCIENCES 3(1):80-88, 2024

©RIJEP Publications ISSN: 1597-8885

Advanced Cryptographic Protocols Using Homomorphic Encryption

[1,2]Val Hyginus Udoka Eze

[1]Department of Publication and Extension Kampala International University Uganda

[2]Department of Electrical, Telecommunication and Computer Engineering, Kampala International University, Western Campus, Ishaka, Uganda

***Corresponding Author: Val Hyginus Udoka Eze, udoka.eze@kiu.ac.ug, Department of Electrical, Telecommunication and Computer Engineering, Kampala International University, Western Campus, Ishaka, Uganda (ORCID: 0000-0002-6764-1721)**

ABSTRACT

Homomorphic encryption (HE) is a revolutionary cryptographic technique that enables computations on encrypted data without decryption. This paper provides a comprehensive overview of HE, its fundamental concepts, types, and applications, especially in privacy-preserving computations. This paper discusses the history, principles, and technical challenges of homomorphic encryption, alongside its practical implications in fields like secure data sharing, privacy-preserving data analysis, and machine learning. This paper also explores future research directions and potential advancements in homomorphic encryption technology.

Keywords: Homomorphic Encryption, Privacy-preserving Computation, Fully Homomorphic Encryption, Partially Homomorphic Encryption and Secure Multi-party Computation

INTRODUCTION

Homomorphic encryption (HE) is a transformative cryptographic technique that allows for computations on encrypted data without needing to decrypt it first [1, 2]. This capability is crucial for maintaining data privacy and security, particularly in cloud computing and multi-party data analysis scenarios. The core principle of homomorphic encryption is that operations performed on ciphertexts translate directly to operations on the corresponding plaintexts upon decryption. This property enables secure data processing and analysis while preserving confidentiality [3, 4]. Fully homomorphic encryption (FHE) allows for both addition and multiplication operations on encrypted data, which means any computation can, in theory, be performed on encrypted data. However, the high computational overhead and complexity have limited its practical applications [5, 6]. There are different levels of homomorphic encryption, including partially homomorphic encryption (PHE) and somewhat homomorphic encryption (SHE), each supporting different sets and complexities of operations. PHE supports a single type of operation (either addition or multiplication), while SHE supports a limited number of operations before needing re-encryption. Homomorphic encryption is particularly beneficial in scenarios where data privacy is paramount, such as medical data analysis, financial transactions, and secure outsourcing of computations. By enabling secure computations on encrypted data, HE offers a powerful tool for maintaining data privacy in an increasingly data-driven world [7-9].

Introduction to Homomorphic Encryption

The homomorphic encryption (HE) algorithm fulfills the recreation of the decryption operation from the set of plug operations in terms of the corresponding read operations [10, 11]. A cryptosystem is claimed to be homomorphic if the ciphertext permits the execution of operations on it. Every operation over the ciphertext gets reflected in the decrypted message at the time of decryption. A mathematical function f (.) with x and y as input and output respectively is said to be commutative if f(x., y) = f(y, x). E.g., the operations of x+ y are commutative while x- y are not, so the former is homomorphic and the latter is not when ciphertext needs to be x- y type functions. Homomorphic cryptosystems allow scientific computations conducted in a cloud without decrypting the inputs [12-14]. It provides a remedy for addressing challenges faced in data sharing. The ability to perform computation on encrypted data is the ultimate goal of this encryption scheme. Without compromising on the encryption data privacy homomorphically constructed ciphertexts can be utilized in computation. This is particularly important in the scientific application use case where private sensitive inputs can be computed without decryption. In this way, new privacy objectives can be achieved. Homomorphic encryption, one of the tools of privacy-preserving computation, enables one to perform mathematical operations over the encrypted message [15-18]. This means that one can pass their encrypted message to someone else and allow them to be a part of some computation without the risk of the message being exposed. The concept of homomorphic encryption was introduced by Rivest et al. in the year 1978. However, the breakthrough in the world of homomorphic cryptography is to combine re-linearization and bootstrapping operations in both FHE and TFHE [19-20].

Basic Concepts and Definitions

Fully Homomorphic encryption (FHE) has been the holy grail of cryptography, but the basic principle can also be used for other levels of homomorphic encryption such as partially homomorphic. Two specific circuits are generally considered for this kind of homomorphic encryption - those that only enable the XOR operation and those that only enable the NAND operation. Gimli is a low-level cryptographic permutation that is a competitor to AES and is being considered for some post-quantum cryptographic systems. It is faster than AES (1.5 cycles per byte) and is a bit less secure and conservative than AES. The S-box of this permutation is closer to being dent, and there are more attacks based on different types of collisions. This applies to most lightweight cryptographic primitives and not just block ciphers, but here we demonstrate it [21-23]. Homomorphic encryption allows operations to be performed on encrypted data in such a way that when decrypting the results of these operations, it matches the corresponding output it would produce with no knowledge of the encryption key. Therefore, representatives of a corporation, in correspondence with someone from another company, can execute operations on encrypted data and decrypt results without either revealing the raw data each started with or intermediate results to anyone else. They can keep the full computative process and results fully private unless they choose to disclose them. Homomorphic encryption is a type of encryption that allows people to compute encrypted data without extracting decrypted data. The result of the computation is still an encrypted form of the answer. That is, the result does not need to be decrypted before it can be used for further computation. The result of the computation is not of the same form as the original plaintext, but rather an encryption E(m'), where m' is some function of m [24-26].

Types of Homomorphic Encryption Schemes

A somewhat homomorphic encryption scheme supports multiple operations over encrypted data but with bounded complexity. An example of SWHE is the ElGamal encryption scheme. It is known to be additively homomorphic under the random or standard assumption. The Ciphertext-Policy Attribute-Based Encryption (CP-ABE) uses ElGamal's properties also to encrypt data for a specific attribute. The learning parity with noise (LPN) problem is computationally assumed hard, and ElGamal consists of a DDH tuple (g, X = gx, Y = gy, Z = xy) and ciphertext (c1 = gr, c2 = M.yxmod p) for a message M. The exponentiation of ElGamal's cipher text also hides the encrypted messages, but re-encryption is essentially considered for effective order, magnification, and complexity reduction. Fully Homomorphic Encryptions (FHE), initially proposed by Rivest-Shamir-Wagner (RSW) in 2009, support addition and multiplication directly [27-29]. It may carry out computation over encrypted data without a clear-cut interface to the plain-text domain. There are mainly two types of FHE schemes, the Ring-LWE-based FHE scheme and the Learning with Errors (LWE)-based FHE scheme. Homomorphic encryption enables the testing of encrypted data for the presence of a pattern without decrypting it, thus preserving privacy. In this section, we describe the types of homomorphic encryption schemes. A partially homomorphic encryption scheme supports only one operation over encrypted data, i.e. either addition or multiplication. An example of partially HE is the Paillier encryption scheme. It supports additively homomorphic operations on encrypted data. Let (pk, sk) be the public key and private key of some user, and E(pk, m1) and E(pk, m2) are the encryptions of m1 and m2 respectively, the Paillier encryption algorithm E(pk: m) returns the encryption of a message m. This encryption scheme is partially additive and not multiplicatively homomorphic. Compounded operations can be executed in serial over the pallier-encrypted cipher text. However, this technique usually fails to deliver the desired precision loss error [30, 31].

Applications of Homomorphic Encryption

It would be possible to design privacy-preserving protocols with various cryptographic techniques (pseudorandom function, garbled gates, symmetric key encryption-based techniques, untrusted cryptography), considering the available privacy, performance, complexity, and flexibility (key parameters for protocol design for medicine) and their operating assignments (when to apply the key protocols in the lifecycle of genomic analysis) to achieve the best operational privacy, performance, and computational and storage complexity in specific genomic analysis. Homomorphic encryption will be in line with current targets for the largest-scale medical data processing, after that, graph-based encryption/decryption needs to be considered for computational efficiency and integrated into multicomponent medicine-information frameworks and functionalities. Furthermore, there are opportunities to develop advanced privacy-enhancing technologies, including protocol chaining and multiencryption technologies, to further enhance the operational privacy of genomic analysis. There will be chances for the integrated developments of cryptographic protocols with other privacy-enhancing technologies, considering challenges in the medical sectors. Homomorphic encryption (HE) allows computation on encrypted data without the need for decryption [32-34]. It could be considered ideal for secure third-party operations, with no need for the revealing of the content of data. Fully homomorphic encryption schemes, which permit the evaluation of even multivariate functions securely, are still computationally impractical because of high storage and computational overhead [35, 36]. Restricted homomorphic encryption schemes, known as limited computation schemes, for example, polynomial operations on encrypted data, are relatively mature for real-world practical uses, including the operational genomic analysis case. There are instances where plain-text operation is inevitable, yet PAE technologies are less useful. Therefore, other advanced cryptographic protocols, which provide better privacy but still apply the parallel computing paradigm, are needed [37, 38].

Privacy-Preserving Data Analysis

We then outline fundamental cryptographic techniques and systems to build privacy-preserving data analysis systems based on secure multi-party computation (MPC). Later, observing that secure MPC can achieve more than homomorphic operation on encrypted data, we highlight cryptographic techniques that do not provide homomorphic computation [39, 40]. We then turn our focus to building practical privacy-preserving data analysis systems using homomorphic encryption. We provide an overview of homomorphic encryption implicit in the problem setters and bring out undisclosed techniques and optimizations required before they lead to practical data analysis systems. We then cover cryptographic (lattice-based) systems from which practical schemes are built. Modern enterprises frequently have to compute confidential user data for functions like predictive modeling and personalization. However, sharing such data with third parties for analysis might violate data use agreements [41, 42]. Cryptographic systems such as Homomorphic Encryption (HE) enable privacy-preserving data analysis via secure multi-party computation and allow untrusted servers to use confidential user data for analysis. Among its recent developments is practicality achieved through optimizations and performance enhancements, driven by industrial adoption and open-source tooling [43, 44]. We start by introducing cryptographic concepts relevant to privacy-preserving data analysis and then gather HE schemes proposed in the literature before surveying recent developments on improving the practicality of HE-based data analysis. We bring out HE's research challenges and open problems [45].

Secure Outsourcing of Computations

A powerful approach to protect the privacy of sensitive information while allowing useful computations to be performed based on it is to use secure hardware devices such as HSM – Hardware Security Modules or Secure Co-Processors. Such devices are used to run security-critical computations without exposing the data involved. Data is sent encrypted to the device and returned encrypted. Homomorphic encryption can be seen as a mechanism to implement a similar privacy protection. It is quite inefficient for intense computation and pales in comparison to secure hardware devices in run-time efficiency. However, the capabilities it puts in the hands of users compared to secure hardware are very interesting. Secure hardware typically allows for only very limited computation, while homomorphic encryption allows for very computationally heavy computations [46, 47]. Historically, for the most part, encryption techniques were mainly designed to provide confidentiality and privacy against unauthorized access [48, 49]. As a result, cryptographic primitives and protocols aimed to provide integrity, non-repudiation, and authentication were designed. However, over the past twenty years, there has been a growing importance of privacy protection in the context of data processing [50]. People want to make use of the benefits of others processing their data (virtual assistants, translation services, ...), but at the same time want to have their privacy protected. Several cryptographic protocols employ homomorphic encryption to preserve privacy, and at the same time rely on the zero-knowledge property of the used cryptosystem to prove that they have not cheated [51].

Homomorphic Encryption in Machine Learning

We are currently working to make these advanced privacy-preserving tools for machine learning accessible also to those interested in Internet-of-Things settings, that is, in low computational resources devices that interact with each other over LAN (see our GitHub Repo for a prototype on this). We believe that this kind of technology represents a very promising way to preserve privacy in the months and years to come, given the difficulty of changing laws fast enough to regulate today's overwhelming data collection devices and the resulting use of such data for user profiling in a climate of total opacity. Its adoption by industrial partners will help establish trust, giving their attention to the ease of use and user experience. Our international research activity's ultimate goal is to make the privacy-friendly alternative become the only viable, competitive option even for the data-hungry sectors today lagging in protection and accountability, a goal that we believe is feasible on both regulatory and technical sides simultaneously [52, 53]. Successfully incorporating concepts like filtering and feature extraction into the machine-learning code, it may be possible to avoid using expensive or unrealistic fully homomorphic encryption techniques by downsampling, projecting, or otherwise abstracting data to allow the fully homomorphic technique to be feasible or practical. An encrypted deep-learning prediction service was presented. The trick reduces encryption time, and serial-inference time, and increases parallelism and batch size, making practical prediction times and cost. An interactive framework was presented that explores the behavioral differences between users to keep a diverse ensemble of classifiers in the cloud. The intention is not to train an ensemble within the encrypted domain but to use a third party to perform the black box computation upon receiving encrypted queries from users and then return the results in such a way that the client can decrypt only the results successfully if and only if she too generated the encrypted query [54, 55].

Homomorphic Encryption Techniques for Neural Networks

Here, we have a model with multiple linear (affine) transformations between the layers. HE supports encrypted addition & encrypted multiplication, which makes it more challenging for non-linear activations, such as Rectified Linear Unit (ReLU) or the Sigmoid function. We can use non-linear activation functions like ReLU or Sigmoid with homomorphic encryption. The ReLU is a piecewise linear function that becomes an identity for positive input. Because ReLU is a piecewise linear function, we can also use it on the encrypted input in the encrypted domain. The HE library is used to get an encrypted version of the image input in the DNN. The Tanh function is a non-linear activation function derived from the Sigmoid function [56, 57]. The Sigmoid function is a non-linear function generally used in the computation of the probability. The sigmoid function can also be calculated securely in the homomorphic domain of an encrypted dataset if we consider the Taylor expansion of the sigmoid function around 0. This concludes our homomorphic encryption of the DNN architecture in this domain. Significant work has been done to apply homomorphic encryption to various machine learning models, such as linear models & decision trees [58, 59]. However, one of the significant challenges here is to enable DNN inference using homomorphic encryption, due to its complex operation & size of model parameters. To obtain privacy-preserving machine learning methods using homomorphic encryption (HE), weight functionalities in a DNN are computed in HE- the encrypted domain. Due to the linearity of homomorphic encryption, only a limited set of functions, such as multiplication, addition, rounding, & comparison, can be computed exactly [60, 61]. This restricts the function of interest in neural network layers, i.e., fi, to be compatible with the homomorphic operation. One of the major difficulties in using neural networks with HE is the multiplication of the weight & activation as well as the summation of the results to generate output.

Deep Neural Networks (DNNs) have outperformed the top traditional machine learning methods in most domains. The process of learning DNNs requires a vast amount of data, making it necessary to train on a large dataset to achieve optimum accuracy. Moreover, DNNs require a considerable amount of computational power to function. Many industries are considering cloud-based services to meet the computational demand. However, outsourcing the DNN model to the cloud comes with a significant risk to data confidentiality, integrity, & model privacy protection [62, 63]. Homomorphic encryption is a potential solution to protect the input images' privacy by purely cloud-based DNN model inference. On the server side, it can maintain the confidentiality of the client input images & inference results [64].

Challenges and Limitations of Homomorphic Encryption

Noise management is another fundamental challenge in homomorphic encryption; it gets more intense with each addition or multiplication performed on the ciphertext. As a result, the restoration or refreshment level of the ciphertext decides how many arithmetic operations may be supported. Since the noise amount grows linearly. Moreover, a critical point for deployment is the choice of an FHE scheme with symmetric keys; because the symmetric key is less expensive than the public key, further study is required. Another significant obstacle to the practical operation of cryptographic protocols utilizing homomorphic encryption is the legal context. Although several new regulations in recent years have promoted research and development for utilitarian end-to-end encryption, homomorphic encryption has yet to be specifically addressed [65-67]. Homomorphic encryption (HE) allows operations directly on encrypted data, thereby, eliminating the need for decryption. It enables many applications such as secure data sharing, privacy-preserving computing, blockchain, and cloud computing. However, its wide acceptance has been thwarted due to various challenges and limitations. One chief concern is its computational overhead and its low computational efficiency. Many overhead factors affect the performance of homomorphic encryption, most significantly an increase in the size of ciphertext and the computational time with each operation. The size of ciphertext can be lessened through various approaches or schemes of homomorphic encryption [68-70].

Future Directions and Research Opportunities

The third potential research track may be related to further adaptions/ settings of homomorphic encryption particularly from new lattice-based primitive. It is doable, to work on the summary presented in [NKS] and try to apply a specific version of packed HE using something like bit-decomposition primitives or SIMD techniques with recently presented forms of ring-variants of fully homomorphic encryption. Some of the technical features of these schemes were also covered by [NKS] [71, 72]. This work is still in very preliminary stages, the attacks that can be used against current lattice-based approaches can be very efficient, as presented in print [NW20]. If better attacks were developed, one option could be going in the direction of some new type of problems or using LWE with new parameter settings. Tools that could be used in this direction could be presented for instance in work [vDM] for LWE encryption with divisibility assumed to perform attack. Extensions of fundamentally motivated properties from the classical problem should serve as a toolbox for future cryptography techniques for integers. The other, step in a similar direction could be centering future work around the search version of LPN or ring LWE problem. [73, 74]. Another important area of research could be dedicated to reducing the size of the public parameter on which the security of encoding is based. A minimal public parameter needed for encoding is Z=L $\mathcal{L}$. The performance of FHE lattice-based scenarios is influenced both by key size as well as by the size of (typically) public parameter Z. It is hard to find methods to significantly decrease the public parameter Z. An obvious approach could be applying some form of compression. Redistributions of encoding and lattices have been proposed in [Nak12] [75, 76]. One main direction of research might be exploring the concept of selective security based upon attributes of data/ systems being protected by homomorphic encryption. The notion of selective security was first formulated via the notion of inner-product encryption. Named attribute-based encryption (ABE), in a selective secure multi-key setting, some entity is trusted for the setup of the system, and in the challenger's interpretations there are multiple sets of keys and, if necessary, distinct plaintext spaces. In the selective model for ABE, the adversary has access to the system at a static point in time and is unable to learn identities that are created after this point [78, 79].

CONCLUSION

Homomorphic encryption represents a significant advancement in the field of cryptography, offering unique capabilities for secure and private data computation. Despite its challenges, such as computational overhead and noise management, the potential applications of HE are vast and impactful. From secure data sharing and privacy-preserving data analysis to enhancing the security of machine learning models, HE is poised to play a critical role in the future of data security and privacy. Future research should focus on optimizing HE schemes for efficiency, reducing computational overhead, and exploring new applications to fully harness its potential.

REFERENCES

1. W. Archer, D., de Balle Pigem, B., Bogdanov, D., Craddock, M., Gascon, A., Jansen, R., Jug, M., Laine, K., McLellan, R., Ohrimenko, O., Raykova, M., Trask, A., & Wardley, S. (2023). UN Handbook on Privacy-Preserving Computation Techniques. [PDF]
2. Li, H. (2022). Computer Security Issues and Legal System Based on Cloud Computing. ncbi.nlm.nih.gov
3. Bansod, S. & Ragha, L. (2022). Challenges in making blockchain privacy compliant for the digital world: some measures. ncbi.nlm.nih.gov
4. Stephen Ndubuisi Nnamchi, Faith Natukunda, Silagi Wanambwa, Enos Bahati Musiime, Richard Tukamuhebwa, Titus Wanazusi, Emmanuel Ogwal (2023), Effects of wind speed and

tropospheric height on solar power generation: Energy exploration above ground level. Elsevier publisher. 9, 5166-5182.

5. Yousuf, H., Lahzi, M., Salloum, S.A., Shaalan, K.: Systematic review on fully homomorphic encryption scheme and its application. In: Al-Emran, M., Shaalan, K., Hassanien, A. (eds.) Recent Advances in Intelligent Systems and Smart. Studies in Systems, Decision and Control, vol. 295, pp. 537–551. Springer, Cham (2021)
6. Nazmus Sadat, M., Momin Al Aziz, M., Mohammed, N., Pakhomov, S., Liu, H., & Jiang, X. (2019). A privacy-preserving distributed filtering framework for NLP artifacts. ncbi.nlm.nih.gov
7. Kizito B. W. (2023). An SMS-Based Examination Relaying System: A Case Study of Kampala International University Main Campus. IDOSR JOURNAL OF SCIENCE AND TECHNOLOGY. 9(1), 1-26.
8. Solomon Muyombya Matovu. (2017). On empirical power of univariate normality testsunder symmetric, asymmetric and scaled distributions. International Journal of Scientific & Engineering Research. 8(3), 381-387.
9. Iezzi, M. (2020). Practical Privacy-Preserving Data Science With Homomorphic Encryption: An Overview. [PDF]
10. Elias Semajeri Ladislas. (2023). Personalizing Government Services through Artificial Intelligence: Opportunities and Challenges. Indian Journal of Artificial Intelligence and Neural Networking (IJAINN). 3(5), 13-18.
11. Elias Semajeri Ladislas, Businge Phelix. (2023). FACTORS AFFECTING E-GOVERNMENT ADOPTION IN THE DEMOCRATIC REPUBLIC OF CONGO. International Research Journal of Engineering and Technology (IRJET). 9(3), 1309-1323.
12. Scheibner, J., Louis Raisaro, J., Ramón Troncoso-Pastoriza, J., Ienca, M., Fellay, J., Vayena, E., & Hubaux, J. P. (2021). Revolutionizing Medical Data Sharing Using Advanced Privacy-Enhancing Technologies: Technical, Legal, and Ethical Synthesis. ncbi.nlm.nih.gov
13. Elias Semajeri Ladislas. (2021). Social media and covid19, implications on consumer behavior and social life in uganda. International Journal of Engineering and Information Systems. 5(3), 102-107.
14. Kareyo Margaret Elias Semajeri Ladislas,Businge Phelix Mbabazi,Muwanga Zaake Wycliff. (2020). E-Government Development Review in Africa: an Assessement of Democratic Republic of Congo's Global E-Government UN Ranking. International Journal of Engineering and Information Systems. 4(11), 47-55.
15. Mohammad Lubega, Martin Karuhanga. (2022). On the Eigenvalue problem involving the Robin p(x)-Laplacian. Annals of Mathematics and Computer Science. 7(7), 1-11.
16. Taban James. (2023). An Online Mobile Shopping Application for Uchumi Supermarket in Uganda. IDOSR JOURNAL OF SCIENCE AND TECHNOLOGY. 9(2), 74-82.
17. Akumu Mary. (2023). A Mobile Application to Enable Users to View Bus Schedules and Extend Bus Booking and Reservation Services. EURASIAN EXPERIMENT JOURNAL OF ENGINEERING. 4(1), 84-104.
18. Eze VHU, KCA Uche, WO Okafor, E Edozie, CN Ugwu, FC Ogenyi. Renewable Energy Powered Water System in Uganda: A Critical Review. Newport International Journal of Scientific and Experimental Sciences (NIJSES) 2023. 3(3), 140-147.
19. M. Charles, W. & M. Delgado, B. (2022). Health Datasets as Assets: Blockchain-Based Valuation and Transaction Methods. ncbi.nlm.nih.gov
20. Chikadibia Kalu Awa Uche, Eza Val Hyginus Udoka, Abigaba Kisakye, Kugonza Francis Maxwell, Okafor O Wisdom. Design of a Solar Powered Water Supply System for Kagadi Model Primary School in Uganda. Journal of Engineering, Technology, and Applied Science (JETAS) 2023 5(2), 67-78.
21. Sharma, I. (2013). Fully Homomorphic Encryption Scheme with Symmetric Keys. [PDF]
22. Chikadibia KA Uche, Fwangmun B Wamyil, Tamunokuro O Amgbara, Itafe V Adacha. Engineering properties of concrete produced using aggregates from polyethene terephthalate plastic waste. International Journal of Academic Engineering Research. 2022 6(6), 47-55.
23. Val Hyginus Udoka Eze, Enerst Edozie, Okafor Wisdom, Chikadibia Kalu Awa Uche. A Comparative Analysis of Renewable Energy Policies and its Impact on Economic Growth: A Review. International Journal of Education, Science, Technology, and Engineering. 2023 6(2), 41-46.

24. Chikadibia Kalu Awa Uche, Sani Aliyu Abubakar, Stephen Ndubuisi Nnamchi, Kelechi John Ukagwu. Polyethylene terephthalate aggregates in structural lightweight concrete: a meta-analysis and review. Springer International Publishing. 2023 3(1), 24.
25. Val Hyginus Udoka Eze, Chikadibia Kalu Awa Uche, Ugwu Chinyere, Okafor Wisdom, Ogenyi Fabian Chukwudi. Utilization of Crumbs from Discarded Rubber Tyres as Coarse Aggregate in Concrete: A Review. International Journal of Recent Technology and Applied Science (IJORTAS) 2023 5(2), 74-80.
26. Val Hyginus Udoka Eze, Chikadibia Kalu Awa Uche, O Okafor, Enerst Edozie, N Ugwu Chinyere, Ogenyi Fabian Chukwudi. Renewable Energy Powered Water Supply System in Uganda: A Critical Review. 2023 3(3).
27. Lang, F. & Zhong, Y. (2022). Application of Personal Information Privacy Protection Based on Machine Learning Algorithm. ncbi.nlm.nih.gov
28. Chikadibia K.A. Uche, Tamunokuro O. Amgbara, Morice Birungi, Denis Taremwa. Quality Analysis of Water from Kitagata Hot Springs in Sheema District, Western Region, Uganda. International Journal of Engineering and Information Systems. 2021 5(8), 18-24.
29. Sen, J. (2013). Homomorphic Encryption: Theory & Applications. [PDF]
30. Chikadibia KA Uche, Tamunokuro O Amgbara. Development of Predictive Equation for Evaporation in Crude Oil Spill on Non–Navigable River. Development. 2020 4(8), 169-180.
31. Chikadibia K.A. Uche, Alexander J. Akor, Miebaka J. Ayotamuno, Tamunokuro O.4 Amgbara. Development of Predictive Equation for Dissolution in Crude Oil Spill on Non–Navigable River. International Journal of Academic Information Systems Research. 2020 4(7), 1-8.
32. Newman, M. (2018). Further Limitations on Information-Theoretically Secure Quantum Homomorphic Encryption. [PDF]
33. Tamunokuro O. Amgbara, Ishmael Onungwe, Chikadibia K.A. Uche, Louis A. Uneke. Design and Simulation of Water Distribution Network Using Epanet 2.0 Hydraulic Solver Software for Okochiri Community, Okrika Local Government Area. JOURNAL OF ADVANCEMENT IN ENGINEERING AND TECHNOLOGY. 2020 8(1)
34. Hamza, R., Hassan, A., Ali, A., Bakri Bashir, M., M. Alqhtani, S., Mohmmed Tawfeeg, T., & Yousif, A. (2022). Towards Secure Big Data Analysis via Fully Homomorphic Encryption Algorithms. ncbi.nlm.nih.gov
35. Nnamchi S. N., OD Sanya, K Zaina, V Gabriel. Development of dynamic thermal input models for simulation of photovoltaic generators. International Journal of Ambient Energy. 2020 41(13) 1454-1466.
36. Sanyal, A., J. Kusner, M., Gascón, A., & Kanade, V. (2018). TAPAS: Tricks to Accelerate (encrypted) Prediction As a Service. [PDF]
37. Stephen Ndubuisi Nnamchi, Onyinyechi Adanma Nnamchi, Oluwatosin Dorcas Sanya, Mustafa Muhamad Mundu, Vincent Gabriel. Dynamic analysis of performance of photovoltaic generators under moving cloud conditions. Journal of Solar Energy Research. 2020 5(2), 453-468.
38. Ullah, I., Boreli, R., & S. Kanhere, S. (2022). Privacy in targeted advertising on mobile devices: a survey. ncbi.nlm.nih.gov
39. Nnamchi, S. N., COC Oko, FL Kamen, OD Sanya. Mathematical analysis of interconnected photovoltaic arrays under different shading conditions. .Cogent Engineering. 2018 5(1) 1507442.
40. Oluwatosin Dorcas Sanya. Modification of an Organic Rankine Cycle (ORC) for Green Energy Management in Data Centres. American Journal of Energy Research. 2017 5(3), 79-84.
41. Joe Mutebi, Margaret Kareyo, Umezuruike Chinecherem, Akampurira Paul. Identification and Validation of Social Media Socio-Technical Information Security Factors concerning Usable-Security Principles. Journal of Computer and Communications. 2022, 10(8), 41-63.
42. Sri Sathya, S., Vepakomma, P., Raskar, R., Ramachandra, R., & Bhattacharya, S. (2018). A Review of Homomorphic Encryption Libraries for Secure Computation. [PDF]
43. Monschein, D. & P. Waldhorst, O. (2022). mPSAuth: Privacy-Preserving and Scalable Authentication for Mobile Web Applications. [PDF]
44. Anthon Ejeh Itodo, Theo G Swart. Capacity Enhancement in D2D 5G Emerging Networks: A Survey. Journal of Applied Engineering and Technological Science (JAETS). 2023. 4(2), 1022-1037.
45. Sophia Kazibwe, Fred Ssemugenyi, Agustine Amboka Asumwa. Organizational Complexity and Performance of Commercial Banks in Kenya. International Journal of Engineering Research and Technology. 2019, 7(12), 227-231.

46. Kiya, H., Nagamori, T., Imaizumi, S., & Shiota, S. (2022). Privacy-Preserving Semantic Segmentation Using Vision Transformer. ncbi.nlm.nih.gov
47. Benjamin Aina Peter, Amos Wale Ogunsola, AE Itodo, SA Idowu, MM Mundu. Reacting Flow of Temperature-Dependent Variable Permeability through a Porous Medium in the Presence of Arrhenius Reaction. Amer. J. Mathem. Comp. Sci. 2019, 4(1), 11-18.
48. Qayyum, A., Ijaz, A., Usama, M., Iqbal, W., Qadir, J., Elkhatib, Y., & Al-Fuqaha, A. (2020). Securing Machine Learning in the Cloud: A Systematic Review of Cloud Machine Learning Security. ncbi.nlm.nih.gov
49. Nabiryo Patience, Itodo Anthony Ejeh. Design and Implementation of Base Station Temperature Monitoring System Using Raspberry Pi. IDOSR Journal of Science and Technology. 2022, 7(1), 53-66.
50. Benjamin Aina Peter, Amos Wale Ogunsola, Anthony Ejeh Itodo, Idowu Sabiki Adebola, Mundu Muhamad Mustapha. A non-isothermal reacting MHD flow over a stretching Sheet through a Saturated Porous Medium. American Journal of Mathematical and Computational Sciences. 2019, 4(1), 1-10.
51. Chiang, J. (2023). Privacy-Preserving 3-Layer Neural Network Training using Mere Homomorphic Encryption Technique. [PDF]
52. George Kasamba, Anthony Ejeh. Enhanced Security Monitoring System for the Pay Card Energy Meter. IDOSR Journal of Computer and Applied Sciences. 2022, 7(1), 109-118.
53. Chialva, D. & Dooms, A. (2018). Conditionals in Homomorphic Encryption and Machine Learning Applications. [PDF]
54. Merenda M, Porcaro C, Iero D. Edge Machine Learning for AI-Enabled IoT Devices: A Review. Sensors (Basel). 2020 Apr 29;20(9):2533. doi: 10.3390/s20092533. PMID: 32365645; PMCID: PMC7273223.
55. Atzori L., Iera A., Morabito G. The Internet of Things: A survey. *Comput. Networks.* 2010;**54**:2787–2805.doi: 10.1016/j.comnet.2010.05.010. [CrossRef] [Google Scholar]
56. Mahdavinejad M.S., Rezvan M., Barekatain M., Adibi P., Barnaghi P., Sheth A.P. Machine learning for internet of things data analysis: A survey. *Digit. Commun. Netw.* 2018;**4**:161–175. doi: 10.1016/j.dcan.2017.10.002. [CrossRef] [Google Scholar]
57. Savaglio C., Ganzha M., Paprzycki M., Bădică C., Ivanović M., Fortino G. Agent-based Internet of Things: State-of-the-art and research challenges. *Futur. Gener. Comput. Syst.* 2020;**102**:1038–1053. doi: 10.1016/j.future.2019.09.016. [CrossRef] [Google Scholar]
58. Neto A.R., Soares B., Barbalho F., Santos L., Batista T., Delicato F.C., Pires P.F. *Anais do XLV Seminário Integrado de Software e Hardware.* SBC; Nashville, TN, USA: 2018. Classifying Smart IoT Devices for Running Machine Learning Algorithms. [Google Scholar]
59. Neapolitan R.E., Jiang X. *Artificial Intelligence.* CRC Press Taylor& Francis Group; Boca Raton, FL, USA: 2018. Neural Networks and Deep Learning. [Google Scholar]
60. Jordan M.I., Bishop C.M. *Computer Science Handbook.* 2nd ed. CRC Press; Boca Raton, FL, USA: 2004. Neural networks. [Google Scholar]
61. Bibri S.E. The IoT for smart sustainable cities of the future: An analytical framework for sensor-based big data applications for environmental sustainability. *Sustain. Cities Soc.* 2018;**38**:230–253. doi: 10.1016/j.scs.2017.12.034. [CrossRef] [Google Scholar]
62. Sajjad M., Nasir M., Muhammad K., Khan S., Jan Z., Sangaiah A.K., Elhoseny M., Baik S.W. Raspberry Pi assisted face recognition framework for enhanced law-enforcement services in smart cities. *Futur. Gener. Comput. Syst.* 2017;**108**:995–1007. doi: 10.1016/j.future.2017.11.013. [CrossRef] [Google Scholar]
63. Zhang T., Chowdhery A., Bahl P., Jamieson K., Banerjee S. The design and implementation of a wireless video surveillance system; Proceedings of the Annual International Conference on Mobile Computing and Networking, MobiCom'15: The 21th Annual International Conference on Mobile Computing and Networking; Paris, France. 7–11 September 2015. [Google Scholar]
64. Rajkomar A., Dean J., Kohane I. Machine learning in medicine. *N. Engl. J. Med.* 2019;**380**:1347–1358. doi: 10.1056/NEJMra1814259. [PubMed] [CrossRef] [Google Scholar]
65. Gharib M., Lollini P., Botta M., Amparore E., Donatelli S., Bondavalli A. On the Safety of Automotive Systems Incorporating Machine Learning Based Components: A Position Paper; Proceedings of the 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops, DSN-W 2018; Luxembourg. 25–28 June 2018. [Google Scholar]

66. Luckow A., Kennedy K., Manhardt F., Djerekarov E., Vorster B., Apon A. Automotive big data: Applications, workloads and infrastructures; Proceedings of the 2015 IEEE International Conference on Big Data, IEEE Big Data 2015; Santa Clara, CA, USA. 29 October–1 November 2015. [Google Scholar]
67. Rublee E., Rabaud V., Konolige K., Bradski G. ORB: An efficient alternative to SIFT or SURF; Proceedings of the IEEE International Conference on Computer Vision; Barcelona, Spain. 6–13 November 2011. [Google Scholar]
68. Transactions E.A.I.E., Health P. Designing wearable sensing platforms for healthcare in a residential environment. *EAI Endorsed Trans. Pervasive Health Technol.* 2017;**3**:12. [Google Scholar]
69. Yazici M., Basurra S., Gaber M. Edge Machine Learning: Enabling Smart Internet of Things Applications. *Big Data Cogn. Comput.* 2018;**2**:26. doi: 10.3390/bdcc2030026. [CrossRef] [Google Scholar]
70. Iero D., Della Corte F.G., Felini C., Merenda M., Minarini C., Rubino A. RF-Powered UHF-RFID Analog Sensors Platform; Proceedings of the 2015 XVIII AISEM Annual Conference; Trento, Italy. 3–5 February 2015. [Google Scholar
71. Della Corte F.G., Merenda M., Bellizzi G.G., Isernia T., Carotenuto R. Temperature Effects on the Efficiency of Dickson Charge Pumps for Radio Frequency Energy Harvesting. *IEEE Access.* 2018;**6**:65729–65736. doi: 10.1109/ACCESS.2018.2876920. [CrossRef] [Google Scholar]
72. Beil J., Perner G., Asfour T. Speech Recognition With Deep Recurrent Neural Networks; Proceedings of the IEEE International Conference on Rehabilitation Robotics; Singapore. 1–14 August 2015; pp. 119–124. [Google Scholar]
73. Haigh K.Z., Mackay A.M., Cook M.R., Lin L.G. *Machine Learning for Embedded Systems: A Case Study.* BBN Technologies; Cambridge, MA, USA: 2015. Technical Report. [Google Scholar]
74. Han S., Mao H., Dally W.J. Deep Compression: Compressing Deep Neural Networks with Pruning, Trained Quantization and Huffman Coding. *arXiv.* 20151510.00149 [Google Scholar]
75. Hinton G., Vinyals O., Dean J. Distilling the Knowledge in a Neural Network. *arXiv.* 20151503.02531 [Google Scholar]
76. Zhao Z., Barijough K.M., Gerstlauer A. DeepThings: Distributed adaptive deep learning inference on resource-constrained IoT edge clusters. *IEEE Trans. Comput. Des. Integr. Circuits Syst.* 2018;**37**:2348–2359. doi: 10.1109/TCAD.2018.2858384. [CrossRef] [Google Scholar]
77. Shi W., Cao J., Zhang Q., Li Y., Xu L. Edge Computing: Vision and Challenges. *IEEE Internet Things J.* 2016;**3**:637–646. doi: 10.1109/JIOT.2016.2579198. [CrossRef] [Google Scholar]
78. Jiang A.H., Wong D.L.K., Canel C., Tang L., Misra I., Kaminsky M., Kozuch M.A., Pillai P., Labs I., Andersen D.G., et al. Mainstream: Dynamic Stem-Sharing for Multi-Tenant Video Processing; Proceedings of the 2018 USENIX Annual Technical Conference (USENIX ATC 18); Boston, MA, USA. 11–13 July 2018. [Google Scholar]
79. Pan M.S., Tseng Y.C. *Sensor Networks and Configuration, Fundamentals, Standards, Platforms, and Applications.* Volume 16. Springer; Berlin/Heidelberg, Germany: 2007. ZigBee and Their Applications; pp. 349–368. [Google Scholar]

CITE AS: Val Hyginus Udoka Eze (2024). Advanced Cryptographic Protocols Using Homomorphic Encryption. RESEARCH INVENTION JOURNAL OF ENGINEERING AND PHYSICAL SCIENCES 3(1):80-88.