Technoarete Transactions on Internet of Things and Cloud Computing Research
Vol-2, Issue-2, June 2022
e-ISSN: 2583 - 0805

Role and Importance of Cryptography Techniques in Cloud Computing

Lionel G. De Lazo[1*], Dr. Pasupuleti Venkata Siva Kumar [2]

[1] Don Honorio Ventura State University, Philippines
[2] VNR Vignana Jyothi Institute of Engineering and Technology, India
*Corresponding Author Email: [1]lioneldelazo@gmail.com

Abstract

The study has depicted the evaluation of the impact of the cryptography techniques in cloud computing in the IT sector. Secondary data collection methods and thematic data analysis process have been used in this study on the basis of peer reviewed journals published after 2019 that increase the reliability and validity of the study. Concept of cryptography and cloud computing have been focused over here to depict the importance of the cryptography in cloud computing. Different kinds of techniques under cryptography methods to secure data including storing and transmitting data have been depicted over here. Confidentiality, integrity along with authentication and authorisation of encrypted data has been highlighted here considering pros and cons of cryptography technology. Security aspects also have been focused in this study to meet the goal of the study with informative justification. Importance of cryptography in cloud computing also has been depicted in this study to prevent challenges in cloud computing prioritizing data security.

Keywords

Cryptography, data, confidentiality, cloud computing.

INTRODUCTION

Cloud Cloud encryption prioritises the cryptography techniques to secure data along with access and share data with advanced secured technology. Cryptography plays an important role in making a sustainable IT infrastructure of the corporate companies by secures data information with cloud computing. Encryption of plain text into a cipher textis the key feature of cryptography. Integrity of data information has been driven by the crypto graphical interference in cloud computing [1]. Algorithms and massages digests have been driven by the crypto graphical engagement in the cloud computing of the globalised IT sector. Codes and digital implication in the cryptographic function enhance the data authentication considering the genuinely of senders and receivers. Depending on the challenges faced by data information security various kinds of cryptographic methods can be used such as symmetric key cryptography, public key cryptography that ensures the data security including storage initiatives.

Integrity, confidentiality and security of the data are the most influential impact of cryptography in cloud computing. On the other hand, instant accessibility of computer based resources including storage services, database, networking, software, analytics and intelligence can be defined as cloud computing. Cryptography integrates the functions of cloud computing with providing advancement in security assurance of data information. Most impacting five functions of cryptography are the key generating and exchanging ability of cryptography along with encoding and decoding of objects of cloud computing, data encryption and decryption also an effective function of cryptography that accelerates the process of cloud computing [2]. Hash and digital signature are the new implications of cryptographic functions that protect data information privacy.

Asymmetric and symmetric cryptography are mostly relevant to cloud computing as it makes the entire procedure of data storing along with security simpler. Main principles of cryptography are integrity, authentication, authorization and confidentiality. Communication based security of data integration, detection of unauthorised data alteration and confirming of identity of senders have been focused by the principles of cryptography [3]. Non repudiation also has been highlighted by the cryptography. Advanced encryption standard, Rivest Shamir alderman have been followed by the data cryptography in cloud computing.

METHODS AND MATERIALS

The study has followed secondary research types to conduct the study and secondary data collection procedures also have been used in this study to collect relevant data to the subject that helps to justify the study. Peer reviewed journals have been used in this study to make the concept more authentic and reliable for the readers. Existing data information is making a study more valuable along with enhancing the quality of the study. Thematic data interpretation has been done in this study depending on the secondary collected data that helps to reach the study goal in a consecutive manner. Time and cost saving approach of the secondary data collection methods and thematic data analysis procedure accelerates the completion of the study with informative justifications [4]. Peer reviewed journals are included in this study whereas survey and interview procedure for data collection has been excluded from this study.

Quantitative research design has been excluded from this study and the qualitative research design has been selected by the writer of the study. Themes are developed on the basis of

e-ISSN: 2583 - 0805

existing data information combined with the writer's realistic observation regarding the subject of the study [5]. On the other hand, a flexible and independent approach of writing helps the study to conclude with a significant justification of the study. The writer of the study has selected these procedures considering the consistency and accuracy of the subject. In recent days, cryptography is an advanced application to secure data and storing data maintaining the data with confidentiality and the writer of the study has selected the peer reviewed journals to focus on the general observation retrieved from the realistic world. Thematic data analysis has the scope to meet the objectives of the study in a simpler exposure pathway. On the basis of the subject requirement, a secondary research type has been followed by the writer to conduct the study without any interruption considering justification of the study.

RESULTS

Concept of cryptography in cloud computing

Cryptography is the process to secure communications between sender and intended recipient regarding message content through implications of various techniques. The general conceptualization of cryptography is to scramble messages for storing or transmitting messages. The technological application of cryptography is to transform plain text into cipher text that plays a vital role in securing data in cloud computing in the IT sector [6]. Cloud computing is the pillar of the IT sector to access and retrieve informational data for project execution. However secure data retrieval in cloud computing has become a major requirement in the IT sector and cryptography with its advanced techniques to some extent fulfil the needs of cloud computing providing a strong data confidentiality. Coding method of cryptography is capable enough of protecting information and communication between the responsible individuals for information. Confidentiality of the communication has been positively impacted with the implication of cryptography.

This particular technique also maintains the integrity of data information considering preventing un-authorization alteration of communication. Authenticity of data information also improves with the engagement of cryptography in cloud computing. Non repudiation feature of cryptography confirms the receiving of communication of data information. There are different keys or techniques which have a comprehensive impact on secure data information such as secret key cryptography, public key cryptography and hash functions. Main objectives of cryptography are to encrypt and decrypt data information according to the utilization of needs of data information [7]. Depending on the purpose of the cryptography, symmetric and asymmetric encryption methods of cryptography have significant advantages for the data security in cloud computing considering recent era.

Modern cryptography focuses on the reliability of cryptography keys, utilization of short strings of text, encoding and decoding messages considering the cryptographic algorithms. Different types of encryption algorithms under cryptography are used in cloud computing such as AES, Triple DES, RSA, Blowfish, Twofish and others. Python programming language is most popular for the implication of cryptographic technology in cloud computing. Accessibility of programming languages also highlights the Ruby, C++, Java and PHP that ensure the understanding of cryptographic algorithms [8]. Secrecy of information has been driven by the advanced implication of cryptographic interpretation of data.

Different negative consequences have been generated in using cryptography in cloud computing to secure data information that can be a crucial crisis for the IT sector to maintain the data storing and transmitting in favour of the company. Hence more modification and advanced technology has to be combined with the technological efficiency of cryptographic algorithms. Crypto programming language with a specific domain has been introduced to improve the conception of cryptography that ensure more prominent data security and encryption of the data storing along with transmission [9]. Authentication protocols and digital certification under cryptographic manner also emphasize the data security standard in the IT sector.

Importance of cryptography in cloud computing

Different consequences of cryptography highlight the efficient importance of it in various technical fields, especially in cloud computing such as ensuring data integrity. Accountability of senders and receivers is also determined by crypto graphical interference in data encryption considering confidentiality of data. Easy availability and retrieval of data also have been driven by the encryption of data with a cryptographic approach [10]. Implication of cryptography strategies also ensure the upholding of information security. Authorization along with authentication of receiver and senders confirms the integrity of data that helps to develop the technical aspects of IT sectors considering data information utilization. Use of AES algorithms in cryptography following some particular steps enhance the data security and ensure the data storing capability and transmission of data information in cloud computing.

Technoarete Transactions on Internet of Things and Cloud Computing Research
Vol-2, Issue-2, June 2022
e-ISSN: 2583 - 0805

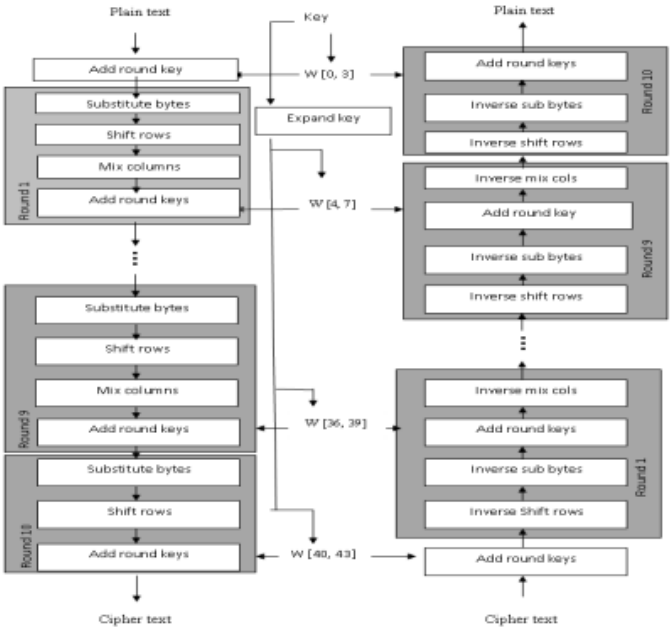

Figure 1: AES technological implication

The process starts with adding a round key and sub byte, mix column, shift row are followed by a cryptographic algorithm and finally end with adding round key again. The entire process has enhanced the security level of data encryption in cloud computing to maintain the data availability considering data storing and transmission. The impact of cryptographic encryption in cloud computing has increased the profit of the IT sector day by day. This reflects on the market size of cloud computing with 156.4 billion dollars revenue collection worldwide [11]. Therefore, the importance of data security and advanced implication of data information in the IT sector using cryptographic algorithms considering cloud computing have an influential aspect. Software engineering in the IT sector also has been benefited with the implication of advanced technology of cryptography. Securing outsourced data and arbitrary computations also has been affected by the cryptographic algorithms considering lower latency. Prioritizing all beneficial aspects of cryptography in cloud computing it has been shown the intensity of the techniques that increase the demand of the adoption of the technique in the cloud computing segment of the IT sector.

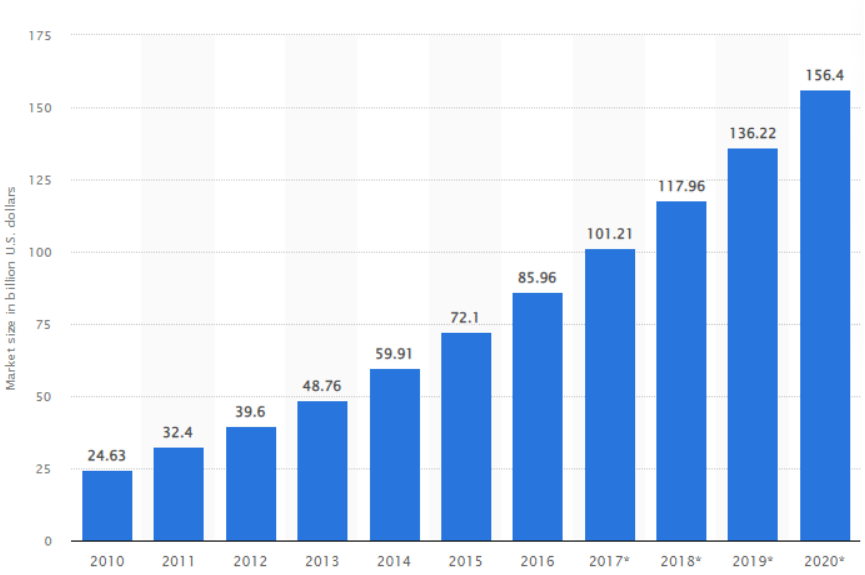

Figure 2: Impact of cryptography in cloud computing

Cloud computing are providing computing services using the internet that helps to connect networks for exchanging data information and generate databases that can be used for further progression of IT based organizations. Therefore security factors play a vital role in maintaining the integration

e-ISSN: 2583 - 0805

and confidentiality of the data. Cryptography methods ensure the data security and authentication of exchanging data in cloud computing that widen the scope of storing data and transmission of data in a cost effective manner [12]. Encrypted data sources maintain the privacy of data with a particular authorization that lowers the risk of data loss.

The Elliptic curve of cryptography algorithms also determines the security of cloud computing applications through controlling data encryption in cloud computing. Hybrid cryptographic approach in cloud computing accelerates the process in an agile manner considering the time saving aspect. Asymmetric and symmetric both cryptographic methods are used in hybrid encryption in cloud computing that increase the security conception of data information [13]. Overall evaluation of the cryptography application in cloud computing has highlighted the beneficiary aspects of cloud computing in the IT sector.

Advantages and disadvantages of cryptography

Consecutive perceptions of cloud computing, positive and negative in both aspects have been reflected that confidentiality is the main comprehensive advantage of cryptography application in cloud computing. Unauthorized revelation can be avoided by the implication of cryptographic algorithms in cloud computing in the IT sector. MAC and digital signature techniques under cryptography can protect information from spoofing and forgeries with an efficient manner in cloud computing. Authentication protocol of data information in cloud computing also has been driven by cryptographic interference [14]. Communication protocols also have been protected by the advanced implication of cryptographic application that protects accessibility of resources of data and data at rest. Encryption of data in a fast and efficient manner considering a large amount of data can be secured using the cryptographic methods in cloud computing. On the other hand, lack of proper system design management cryptography can be harmful for securing data information in cloud computing.

Complexity of cryptography algorithms can be unreadable for the legitimate user. The entire concept of cryptography is dependent on the complex mathematical algorithm that causes tough accessibility of data information considering its security factors. Technical failures also create troubles for encryption of data maintaining the security in cloud computing such as key leakage, software bugs, and holes in operating systems, impact of social engineering, phishing attacks, and side channels attacks. Failure of cryptographic encryption can create severe consequences in cloud computing. Asymmetric technique of cryptography slows the process of data encryption where symmetric technique is quite faster [15]. The private key encryption technique of cryptography has a most crucial disadvantage that requires new individuals to access the data information key.

These disadvantages delay the process of encryption of data along with delay the whole procedure. Modern advanced cryptography technology is quite expensive and has restricted cloud computing to adopt the application to secure the data information. Communication availability in symmetric cryptographic techniques is the most significant drawback that enhances the sharing of data information with third parties [16]. Single and secret key symmetric technique of data also creates barriers for encrypting and decrypting data information in cloud computing. It slows down the procedure of data storing and transmission along with lowering the data security efficiency.

Using a single key feature of symmetric technique, the secrecy of the key on both side of sender and receiver increases the probability of decryption of secret messages considering data loss. However, symmetric techniques also accelerate the data encryption process and reduce the time of securing data information [17]. Considering both consequences of cryptographic encryption of data it can be evaluated that the more modifications in cryptographic techniques has to be implicated to improve the confidentiality of data efficiency that can help to develop cloud computing systems in the IT sector.

Security aspects of cryptography in cloud computing

Authentication, authorization and accounting are the basic principles of security that have been followed by the cryptography technology in cloud computing. Collaboration, cooperation and coordination of data information have been prioritized by the cryptographic approach in cloud computing to manage the data security along with storing and transmitting of data [18]. Security concept has been developed focusing on the people, processes, policies and technologies. Considering competitive aspects in the IT sector, data security adopts the advanced technology of cryptography that ensures the protection of data information in an integrated manner. Virtualization, high reliability, versatility are the basic characteristics of cloud computing and on the basis of it cryptography algorithm is the most appropriate technology that can secure data information with comprehensive efficiency. Cryptography technology helps to implicate the governance policies in the organizations considering secured data information.

Compliance of organizations also has been focused by the cryptographic approach with the interpretation of integrated data implication. Malicious insiders can be avoided by this technique to maintain the security standard of data information and also ensure faster and secured data storing and transmission. Accountability of service hijacking in cloud computing in the IT sector also improves with the implication of cryptographic data encryption. Hypervisor vulnerabilities are the major issues that can devastate the cloud computing system and cryptographic algorithms prevent these kinds of vulnerabilities to determine the security of data information in cloud computing [19]. Implication of symmetric technique under cryptography processes faster the procedure of transformation of cipher text followed by the Data Encryption Standard. Advanced data encryption standard and triple DES also have been used in cloud computing through cryptographic manner according to the need of the data encryption process.

e-ISSN: 2583 - 0805

Cryptography creates a high layer of security that determines the protection of data breach considering data restoration and transmission in the cloud. Cryptographic primitives and protocols prioritizing crypto analytics and cryptanalytic engines as security tools for user authentication, controlling data access along with data storage and data transfer management considering data security [20]. Probability of service attacks, data leakage, accidental exposure of credentials, improper incident responses focusing on the data confidentiality can be protected with the implication of cryptographic technology in cloud computing. Legal and regulatory compliances in IT based organizations have been followed by the authorization and authentication features of cryptography algorithms that ensure the data security of an organization.

Data sovereignty, residency and controlling aspects also have been maintained by the cryptography process in cloud computing prioritizing the data encryption without any data loss. The entire cloud also has been protected with the integrated application of cryptography improving cloud computing efficiency in the IT sector. Confidentiality, integrity and availability are the prior concern of cryptography applications that ensure cloud computing based security [21]. Three models of cloud security, private, public and hybrid have been focused by the cryptography approach maintaining the integrity, authorization and authentication of encrypted data. Avoiding data breach is the prior concern of cryptography technology that ensures the comprehensive data security in cloud computing of the IT sector.

DISCUSSION

Interpretation of evaluated results has shown that the cryptographic algorithm plays a vital role in securing data in cloud computing in the IT sector. Concept of cryptography has highlighted the integrity, authentication, authorization of data encryption considering comprehensive data security. Role of cryptographic algorithms in cloud computing has also been highlighted in the interpretation of results based on cryptographic techniques. Graphical interpretation of evaluating the importance of cryptographic application has depicted that the market size of cloud computing has a revolutionary impact on the IT sector. Different kinds of cryptographic techniques and its characteristics also have been discussed over here to signify the study. Symmetric and asymmetric techniques are mostly used in cloud computing in the IT sector. Different programming languages of cryptographic algorithms such as cryptol, Java and more other languages also have been considered in this study.

Advantages and disadvantages of cryptographic applications also have been analyzed here to determine the positive impact on cloud computing in the IT sector. Unauthorisation encryption of data can be avoided by the implication of cryptographic technology that enhances the probability of data security. Cost effectiveness of this technique also has been highlighted in this study to widen the scope of adoption of this particular technique in cloud computing. Most influential benefit of cryptographic encrypted data is to prevent the data breach. On the other hand, mismanagement of the system design can lead to dangerous outcomes from cryptographic application. Single key factor of the symmetric approach also has created barriers in storing and transmitting data on time. Delaying data encryption lowers the data security along with slows down cloud computing systems.

General overview of cloud computing also has been focused here to establish the correlation between the cryptographic technology and cloud computing. Security aspects of cloud computing through cryptographic encryption also have been highlighted here that helps to protect data loss, accountability vulnerabilities, malicious inside risk in clouding data. AES, DES, TDES and other conceptions of cryptographic techniques also have been depicted in this study to derive the insights of the study. Hybrid cryptography can be considered as the modern v erosion of the techniques that helps to improve the infrastructure of data security and transmission along with storage management without any data loss. Hijacking services in cloud computing also can be controlled by the direct approach of the cryptography techniques. Cryptographic primitives and protocols help to manage the communicative data security along with systematic management of organizations in the IT sector.

Involvement of proper tools of cryptographic analytics helps to integrate data security considering confidentiality and authentication. Perhaps the complexity of mathematical algorithm based cryptography creates obstacles to maintain the efficiency of cryptography. Digital signatures are one of the most influential benefits of cryptography that determines the data security, prioritizing the data storage ability and transmission capability of this particular application. Cryptography in cloud computing has followed the three A of security principles that highlights the authentication, authorisations and accountability. Frequent modification of cryptography technologies including implication of advanced technology is required in cloud computing to lower the risk of data leakage, accidental credential and incidental responses of data information's. Legal aspects and regulatory perceptions of organizations of the IT sector also have been driven by the cryptographic interference on the basis of security of data.

Comprehensive advantages of cryptographic algorithms determine the authentication and communication protocols to create a high layer of data security and encrypted data information in a faster manner to store and transmit data. This specific technique also ensures the availability of data for further betterment of cloud computing in the IT sector. Coding and decoding along with encrypt and decrypts of data are the basic features of cryptography that authorized senders and receivers with authenticated data encryption. Moreover data security management in cloud computing in the IT sector has been determined with the efficient approach of cryptographic encryption of data including storing and transmitting data.

e-ISSN: 2583 - 0805

CONCLUSION

The study has focused on the evaluation of the overall impact of the cryptography techniques in cloud computing to increase the data security along with storing capacity of the data information in the IT sectors. The writer of the study has selected the secondary data collection procedure and thematic data analysis to justify the study with information. Peer reviewed journals are used in this study to enhance the authenticity and reliability to the study along with efficient quality. Advantages and disadvantages of cryptographic encryption of the data in cloud computing have been depicted in this study to reach the goal of the study with informative justification. General conception of cryptography considering cloud computing also has been depicted in this study to showcase the importance of the subject.

Different types of methods under cryptographic algorithms also have been discussed over here such as symmetric and asymmetric techniques with hush functions and its impact on cloud computing also have been highlighted in this study. Complexity of cryptographic techniques has shown here as a drawback of this technology whereas cost effectiveness and time saving aspects also have been focused here to analyze the consequences of the cryptographic technology in cloud computing in the IT sector. Confidentiality, authorisation, integration, authentication of data considering data storing and transmitting in cloud computing have been highlighted in this study to maintain the data security in cloud computing through effective approach of cryptography.

The pros and cons of this particular technique have depicted that modification of methods can improve the data security proficiency in cloud computing. Importance of cryptographic technology has been discussed over here briefly to meet the goal of the study with informative justification. Security perceptions of cryptography algorithms also have been explored here to justify the subject of the study. Different consequences regarding data loss, data leakage, malicious insights and vulnerabilities in cloud computing have been considered as major issues that create obstacles for retrieval of data information without any data security. Cryptographic encryption of data lowers the risk of data loss and also ensures the data security in cloud computing in the IT sector.

REFERENCES

[1] Olowu, Modebola, et al. "A secured private-cloud computing system." *Applied Informatics: Second International Conference, ICAI 2019, Madrid, Spain, November 7–9, 2019, Proceedings 2*.Springer International Publishing, 2019.

[2] Adee, Rose, and HaralambosMouratidis. "A dynamic four-step data security model for data in cloud computing based on cryptography and steganography." *Sensors* 22.3 (2022): 1109.

[3] Weber, Peter, et al. "Data Security and Data Protection." *Basics in Business Informatics*. Wiesbaden: Springer Fachmedien Wiesbaden, 2022. 281-308.

[4] Özkan, Evin, NedaAzizi, and OmidHaass. "Leveraging smart contract in project procurement through dlt to gain sustainable competitive advantages." *Sustainability* 13.23 (2021): 13380.

[5] Secinaro, Silvana, et al. "Social finance and banking research as a driver for sustainable development: A bibliometric analysis." *Sustainability* 13.1 (2020): 330.

[6] Denis, R., and P. Madhubala. "Evolutionary Computing Assisted Visually-Imperceptible Hybrid Cryptography and Steganography Model for Secure Data Communication over Cloud Environment." *Int. J. Comput. Netw.Appl* 7 (2020): 208-230.

[7] Yazdeen, AbdulmajeedAdil, et al. "FPGA implementations for data encryption and decryption via concurrent and parallel computation: A review." *Qubahan Academic Journal* 1.2 (2021): 8-16.

[8] Wardhan, Harshita, and SumanMadan. "Study On Functioning Of Selenium Testing Tool." *International Research Journal of Modernization in Engineering Technology and Science Www. Irjmets. Com@ International Research Journal of Modernization in Engineering* (2021): 2582-5208.

[9] Chin, Collin, et al. "Leo: A programming language for formally verified, zero-knowledge applications." *Cryptology ePrint Archive* (2021).

[10] Ukwuoma, Henry Chima, et al. "Post-quantum cryptography-driven security framework for cloud computing." *Open Computer Science* 12.1 (2022): 142-153.

[11] Vailshery, S. L. Size of the cloud computing and hosting market market worldwide from 2010 to 2020 (in billion U.S. dollars). *statista*. 16th February, 2022. https://www.statista.com/statistics/500541/worldwide-hosting-and-cloud-computing-market/

[12] Adee, Rose, and HaralambosMouratidis. "A dynamic four-step data security model for data in cloud computing based on cryptography and steganography." *Sensors* 22.3 (2022): 1109.

[13] Chinnasamy, P., et al. "Efficient data security using hybrid cryptography on cloud computing." *Inventive Communication and Computational Technologies: Proceedings of ICICCT 2020*. Springer Singapore, 2021.

[14] Panda, Prabhat Kumar, and SudiptaChattopadhyay. "A secure mutual authentication protocol for IoT environment." *Journal of Reliable Intelligent Environments* 6 (2020): 79-94.

[15] Chowdhary, ChiranjiLal, et al. "Analytical study of hybrid techniques for image encryption and decryption." *Sensors* 20.18 (2020): 5162.

[16] Kalaivani, V. "Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications." *Personal and Ubiquitous Computing* (2021): 1.

[17] Rahman, Ziaur, et al. "Enhancing AES using chaos and logistic map-based key generation technique for securing IoT-based smart home." *Electronics* 11.7 (2022): 1083.

[18] Alshammari, Salah T., AiiadAlbeshri, and Khalid Alsubhi. "Integrating a high-reliability multicriteria trust evaluation model with task role-based access control for cloud services." *Symmetry* 13.3 (2021): 492.

[19] Abdulsalam, YunusaSimpa, and Mustapha Hedabou. "Security and privacy in cloud computing: technical review." *Future Internet* 14.1 (2022): 11.

[20] Kumar, Adarsh, Saurabh Jain, and AlokAggarwal. "Comparative Analysis of Multi-round Cryptographic Primitives based Lightweight Authentication Protocols for RFID-Sensor Integrated MANETs." *Journal of Information Assurance & Security* 14.1 (2019).

[21] Adee, Rose, and HaralambosMouratidis. "A dynamic four-step data security model for data in cloud computing based on cryptography and steganography." *Sensors* 22.3 (2022): 1109.