Securing the Next Generation Cloud: A Survey of Emerging Technologies and their Impact on Cloud Security

Ibrar Ahmad[*], Fazal Qudus Khan[†], Mansoor Qadir[‡], Suleman Shah[§], Muhammad Atif[**], Muhammad Islam[††], Sadeeq Jan[‡‡]

Abstract

Cloud computing is considered as the current market leader and future trend in computing resources. However, security is one of the main issue due to a large number of data saved on the cloud. There exist many traditional security techniques for the protection of data. This research explores various tools and techniques used in traditional cloud security and discusses the future prospects of securing data in the context of cloud computing. Within this investigation, key domains of security are explored, i.e., cryptography, data security, cyber security, steganalysis, and steganography. A notable contribution of this paper is a comparative analysis of the most widely used security algorithms in cloud computing. These algorithms, comprising 90% of the study, are evaluated in conjunction with other techniques and models. Furthermore, this research examines into novel approaches like the 2D Baker's map, employing piecewise linear chaotic maps (PWLCM) to improve security and sensitivity. This paper noticed the precedence of the Advanced Encryption Standard (AES) as the most used algorithm for encryption and decryption in cloud security and proposes its enhancement by integrating Attribute-Based Encryption (ABE) and Role-Based Access Control (RABS), Embedded Least-Significant Bit (LSB) and SHA-256 for image security. It also discovers innovative security measures, and blockchain technology to ensure robust security and privacy for data exchange in a cloud computing and IoT environment. For data encryption, Elliptic Curve Cryptography (ECC) is recommended and further techniques are explored to fortify system security, with a focus on Optical Amplitude Modulation (OAM) for enhanced security during Orthogonal Frequency-Division Multiplexing (OFDM)

[*] Department of Computer and Software Technology, University of Swat, Shangla Campus, Shangla 19100, Pakistan, ibrar.ahmad@uswat.edu.pk

[†] Department of Computer and Software Technology, University of Swat, Shangla Campus, Shangla 19100, Pakistan, fazal.qadus@uswat.edu.pk

[‡] Corresponding author, Department of Computer Science, CECOS University of IT & Emerging Sciences, Peshawar 25000, Pakistan, mansoor.qadir@hotmail.com

[§] Sarhad University of Science & Information Technology, Peshawar, KPK, Pakistan, suliman15505@gmail.com

[**] Department of Computer and Software Technology, University of Swat, Shangla Campus, Shangla 19100, Pakistan, muhammadatifshangla2003@gmail.com

[††] Department of Computer and Software Technology, University of Swat, Shangla Campus, Shangla 19100, Pakistan, muhammadislamk77@gmail.com

[‡‡] National Center for Cyber Security, Department of Computer Systems Engineering, University of Engineering & Technology, Peshawar, Pakistan, sadeeqjan@uetpeshawar.edu.pk

transmission. This research paper offers a comprehensive overview of the ever-evolving landscape of cloud security, encircling a wide spectrum of algorithms, techniques, and models. It serves as an invaluable resource for practitioners, researchers, and policymakers seeking to navigate the complexities of cloud security and stay level of emerging trends and strategies for ensuring data protection in cloud computing environments. Frequent system updates and patches are vital for a secure cloud environment.

Keywords: Cloud computing, Cloud security, Data and information security techniques, Cryptography, steganalysis and steganography.

Introduction

The pervasive adoption of cloud computing in the domain of information technology highlights its numerous advantages, including scalability, cost-efficiency, and accessibility. Cloud computing is an Internet-based model that offers on-demand access to shared information, software, and resources (Yamin, M., & Tsaramirsis, G., 2012). Likewise, (Khan et al., 2014) stated that cloud computing provides access to abundance of digital resources, making education limitless and just-in-time. In this context, digital literacy becomes pivotal, ensuring user friendly in navigating rare cloud interfaces (Jan et al., 2019). However, the development of cyber technology, especially in Internet banking, brings cybersecurity challenges that require the application of machine learning techniques for improved security assessments (Khattak et al., 2021). Moreover (Almshari et al., 2020) explained that laboratory computers face challenges from disfavored applications, influencing performance and security due to background processes, and privacy policies may retard active monitoring.

Cyber-attacks targeting financial web systems accentuate the importance of regular security testing and varied security techniques (Tauqeer, O, B et al., 2021). (Rahman, S, et al., 2020) stated that steganography hides messages with applications ranging from military communication to financial transactions, require data security during transmission. Cloud computing introduce network security risks due to third-party service distributor, needing careful control over privacy and data security (Ouda, A et al., 2022). In the Internet epoch, ensuring data security during image transmission is crucial for conserving personal privacy, commerce secrets, and national security (Chai, X et al., 2018). The fast increase in data generated by different applications requires secure storage solutions, with cloud computing arising as the key technology to address this need while amplifying the quickness of safeguarding data against potential threats (Thabit, F et al., 2021).

This research paper offers a comprehensive overview of the developing landscape of cloud security, encircling a wide spectrum of algorithms, techniques, and models. It serves as a valuable resource for practitioners, researchers, and policymakers seeking to navigate the complexities of cloud security and stay level of emerging trends and strategies for ensuring data protection in cloud computing environments.

The subsequent sections of the paper are structured as, section two conducts the cloud security algorithm, section three examines security techniques in cloud computing, and section four investigates cloud computing security across layers and analyzes the security aspects of various cloud services models. Conclusively, section five peer the future of security in cloud computing, exploring emerging trends and technologies that promise to shape the future of safeguarding data in the cloud.

Cloud Security Algorithm

The wide range of data exchanging and its manipulation at the clouds area are very helpful and effective for the users. These data are present in different formats and shapes such as in text form or an image form. It’s very difficult to maintain their Confidentiality and integrity. Because there is a huge chance that some unauthorized access has been made to your privacy. To make this confidentiality more efficient and secure we advocate the methods of Encryption and Decryption Algorithm in order to maintain the integrity of information. There are numerous collections of data Encryption Algorithms that provide security and confidentiality to privacy. Every Encryption algorithm is used for the purpose of safeguarding the data but the best algorithm is one that has less time consumption, better execution speed, convenience with the environment, and the best degree of security.

(Wang et al., 2018) proposed an encryption algorithm in Body Area Networks (BANs) to precisely secure physiological information’s. However, this encryption algorithm is built on combine chaos. The logistic chaotic model and Kent mapping approach are used to generate two sub-matrices. After that, the XOR operation is performed on the original data to attain a single matrix of encryption. Comparatively, it is attained from the experimental analysis that the suggested algorithm has good adaptability, responsiveness to attack, high key space, and is effectively applicable for most BAN systems. The initiative for further advancement to make it more efficient and reliable regarding every technique and also make it applicable for many fields of life.

Moreover, (Chai et al., 2018) introduced an algorithm for Encryption that based on Memristive Chaotic System (MCS), Compressive Sensing (CS) and Elementary cellular automata (ECA). MCS overcome the consumption of energy during data transmission, ensure large key space, respond to brute force attacks, and make high alert sensitivity, and high resistance towards threats. However, this algorithm takes a large time in decryption from several algorithms. So, the future enhancement is to increase their processing speed to be reliable for many applications. Besides, (Modal et al., 2018) proposed an effective well-secured image encryption algorithm that was designed on a 2D Baker's map. The procedure steps contain permutation that applies to the original image and diffusion under XORing that securely encrypts the image.

The proposed scheme has been analyzed by the top security recognizers such as PSNR, NPCR, UACI, MSE, Entropy, etc. This algorithm provides high key sensitivity, and resistance to threats and smoothly runs in a low computational platform. (Luo et al., 2018) built an image encryption algorithm structured by a piecewise linear chaotic map (PWLCM) and a Four-dimensional hyper-chaotic map (FDHCM). Four chaotic sequences are generated, which control the flow of diffusion and permutation. The analyzed result shows a better execution rate, good security providence, and sensitivity alerts to the medium.

Likewise, (G. Abood et al., 2018) made a survey on cryptography Algorithms on the basis of their performance, speed and time complexity, security, and effectiveness. The survey consists of cryptography algorithms such as DES, AES, TDES, EEE, and CR4, etc. The final results of the research find that Symmetric algorithms are more reliable and faster than Asymmetric algorithms such as AES can be seen in Table 1. in terms of flexibility, speed encoding, decoding, and key space. In another study, (Alloghani et al., 2019) assembled an inspection recap of Homomorphic Encryption via research papers. The proposed survey is based on the PRISMA checklist and Cochrane's class estimation to retrieve reviews from different assets.

Consequently, (Lu et al., 2018) proposed an encryption algorithm, consisting of Polarization codes and chaotic sequences that have a uniqueness in correlation to each other because the chaotic sequences are in frozen bits of Polar codes. If the frozen bits are not recognized by eavesdroppers, then it would be harder to decode the encrypted sequence. To make it more secure we advocated building chaotic sequences by channel state data. (LI et al., 2020) formulated an algorithm for image encryption under the mechanism of logistics and Two Dimension Lorenz.

Chaotic sequences are generated with the help of a chaotic model to disorganize the image from its original shape.

(Hariss et al., 2020) made an enhancement work on Homomorphic Encryption (HE) to highly enrich the vulnerability and Security of Symmetric Algorithms. This developed configured framework is applied to Domingo Ferrer's symmetric HE strategy to reduce their abnormalities and harmfulness. (Ahmad et al., 2018) elaborated on the Security concern of an Image Encryption algorithm for Body area network (BAN) system. The Algorithm is based on Combine Chaotic Sequences to efficiently convert the image into a Cipher pattern. The adaptation and performance of an Algorithm is well-founded but the conservative analysis determined some Security threat concerns that conceal its ability.

To overcome these challenges a new enhanced version is suggested with advanced encryption techniques, using secure hash algorithm SHA-512 as labeled in Table 1 for single time keys implementations along with this a 4D hyper-chaotic system is accomplished to access the level of integrity and confidentiality.

Table 1

Most Widely Used Encryption Algorithms in Cloud Computing

Reference No	Algorithm Name
Ref. [15]	Systematic Encryption Algorithm (AES)
Ref. [19]	Homomorphic Encryption (HE)
Ref. [20]	Secure Hash Algorithm (SHA-512)
Ref. [53]	Blowfish and Two fish
Ref. [58]	Advanced Encryption Standard (AES)
Ref. [58]	Rivest-Shamir-Adleman (RSA)

Table 1. mention a list of most prominently used Encryption algorithms for data security in Cloud Computing world. The Encryption algorithms efficiency depend on certain factors such as operating speed, flexibility, compatibility, responsiveness, key length and Security requirements. A survey report (G. Abood et al., 2018) states that Symmetric algorithms are more effective than Asymmetric algorithms. Moreover, AES symmetric algorithm is the most widely used and appropriate encryption algorithm on the basis of performance and security. Different applications need for variety of algorithms to accomplish their desired requirements. Figure 1 shows the complete mechanism of Encryption and Decryption in a transmission channel. The motive to establish Encryption and Decryption Algorithm is to ensure the integrity of data. At the initial level, the data is allocated in its original understandable format known as Plain text. This is preceded by an Encoder via an Encryption Algorithm to convert the plain text into Cipher text using secret Encryption Key. Cipher text is a

disorganized locked form of data that is inaccessible without a Decryption key. Meanwhile, when the data reaches to its terminal point (receiver) a Decryption Algorithm with a decryption key is applied to the decoder and retrieves the data from Cipher text to its original Plain text format.

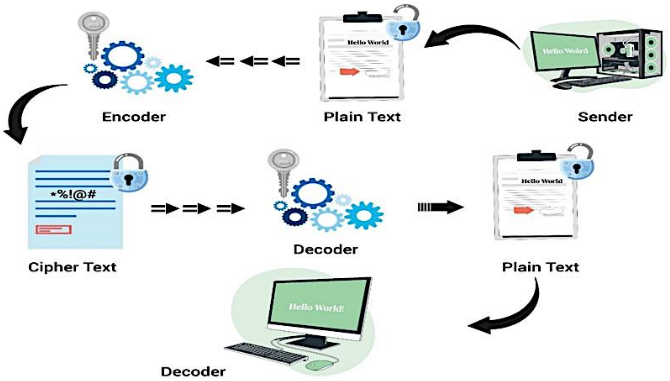

Figure 1: Data Encryption and Decryption Process

Security Techniques and Cloud Computing

Cryptography and cloud Computing

In this context, (Li et al., 2019) reviewed nearly all image cryptanalysis research from 2018, highlighting intricate challenges in designing and evaluating these encryption schemes. By shedding light on these challenges, the paper aims to propel advancements in fortifying image data security in the digital landscape. Furthermore, (Sirichotedumrong et al., 2019) introduced a privacy-preserving approach for deep neural networks (DNNs). Likewise, (Namasudra et al., 2020) introduced a DNA-based encryption scheme for safeguarding multimedia files in cloud computing. It employs a 1024-bit DNA-generated secret key along with user attributes and password. In a collision attack, a malicious user discovers distinct inputs that yield identical hash values. (Mohamed et al., 2020) introduced a novel encryption and decryption algorithm which combines hybrid chaotic processes and the mitochondrial deoxyribonucleic acid (mtDNA) diffusion method to enhance security while reducing hardware complexity. The algorithm's effectiveness is proven against various attacks, including chosen/known plain text, brute-force, and image-based attacks. Furthermore, (Vaseghi et al., 2021) described a chaotic secure communication technique for encrypting and transmitting satellite images through a channel with unknown time-delay propagation. The method combines chaotic keys, including multi-shift cipher encryption and chaotic masking of Quadrature Amplitude Modulation (QAM) symbols, to enhance the security of wireless Orthogonal Frequency Division Multiplexing (OFDM) transmission. The proposed technique demonstrates effectiveness against various attacks, offering robustness, simplicity, and security.

(Li et al., 2020) introduced an image encryption algorithm that employs a classical chaotic model. This model generates two sets of chaotic sequences, which are then utilized for image encryption. (Teh et al., 2020) emphasized the increasing interest in chaos-based cryptography but limited practical implementation compared to traditional cryptography. They recommend several key implementation practices, including precise mathematical definitions, integration with established cryptographic paradigms, simplicity, flexibility, and rigorous security assessment. (Faiz et al., 2022) explained that Cloud computing's decentralized nature exposes it to various security vulnerabilities. Homomorphic encryption offers a solution for safeguarding data accessed from cloud servers. The proposed hybrid technique is implemented through MATrix LABoratory (MATLAB). The particle swarm optimization (PSO) technique enhances the encryption key. Hybrid homomorphic encryption methods employ particle distributions based on quality assessments, leading to improved outcomes. Simulation results demonstrate the effectiveness of the proposed hybrid encryption approach. Likewise, (Artiles et al., 2019) elaborated an encryption strategy that involves the integration of a binary chaotic sequence into the SubBytes and sub-key generation units of the AES algorithm. (Amsyar et al., 2020) stated that utilizing blockchain enhances data security, its value is indeterminate, and it operates as a decentralized digital currency. Cryptocurrency enables swift transactions due to the absence of intermediaries, and its data remains tamper-proof due to permanent storage on the blockchain network.

Traditional Data Security and Cloud Computing:

(Hasan et al., 2022) contend that the progressions within the Internet of Things (IoT), artificial intelligence, wearable sensors, and the increase of Internet of Medical Things (IoMT) applications mark significant advancements. This landscape is further complicated by recognized attack vectors in IoMT, including (Steinbart et al., 2018) emphasized in their article the increasing financial impact of cybercrime and the need for improved information security management. Correspondingly, (Ring et al., 2019) stressed the significance of accurate network-based datasets for training and evaluating Network Intrusion Detection Systems (NIDS) to uncover activities like botnets, port scans, and brute force attacks. A detailed analysis of 34 datasets, defining 15 essential characteristics across five categories: General Information, Nature of the Data, Data Volume, Recording Environment, and Evaluation Process was conducted. The overview not only outlines dataset attributes and attack scenarios but also addresses the shortage of publicly accessible datasets, and encourages proactive research contribution in this area.

(Li et al., 2023) highlighted the importance of accurate wind power prediction in modern power systems due to the volatility of renewable energy sources. They proposed a solution called FedDRL (Federated Deep Reinforcement Learning) to address concerns about data privacy and isolation associated with conventional centralized techniques. (Hao et al., 2019) highlighted the rise of Industrial Artificial Intelligence (IAI) in Industry 4.0, addressing complex industrial challenges. (Gruschka et al., 2018), (Purtova, N., 2018), and (Tikkinen-Piri et al., 2018) highlighted the complexities of handling sensitive information within the realm of big data, highlighting the risks to privacy and legal consequences, particularly focusing on the General Data Protection Regulations (GDPR). The study illustrated the impact of data protection on large data projects through two cases, one addressing biometric data privacy concerns and the other facing challenges in data analysis due to extensive anonymization. (Vinoth et al., 2022) emphasized the importance of careful planning, risk awareness, and security solutions for successful cloud adoption.

Trust mechanisms are deemed crucial in the cloud's resource-driven environment. Challenges in cloud security encompass data handling, usage risks, semantic gaps, loss of control, trust-building, and the heightened risk of data-driven attacks. (Khan et al., 2019) stated that various encryption methods have been applied for secure data transmission over insecure channels, guarding against data loss and unauthorized manipulation. The research underscores that ECC is not only swift and efficient for safeguarding data in cloud environments but also lowers computational power requirements, ultimately enhancing efficiency. Figure 2 shows the data security in cloud computing using different algorithms and encryptions.

Cyber Security and cloud computing

(Furstenau et al., 2020) emphasized the growing importance of cybersecurity in countering escalating cyber threats, driven by increased attacker intelligence and accessible technology. Similarly, (Srivastava et al., 2022), (Mohammed, I. A., 2020), and (Dunn et al., 2020) highlighted that Artificial Intelligence (AI) outcomes often lack clarity due to their black-box nature, hindering understanding and explanation of decision-making processes.

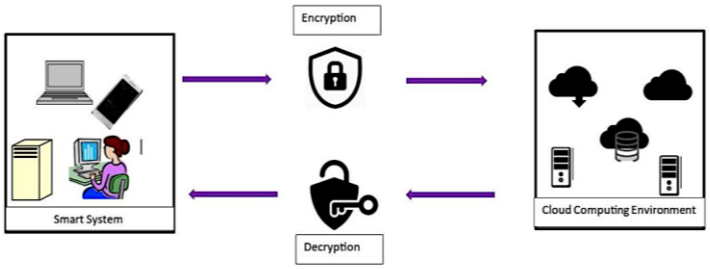

Figure 2: Securing Data in Cloud Computing

Explainable AI (XAI) is a rapidly advancing research area that focuses on extracting information and presenting results in a transparent and understandable manner. It explores healthcare, transportation, and Industry 4.0, delving into cybersecurity implications. The integration of AI and AI-enabled technologies will impact cyber security and state-private actor relationships. Consequently, (Kurt et al., 2018) examined real-time detection of hybrid False Data Injection FDI/jamming attacks in the smart grid. (Alzubaidi, A., 2021) suggested that efforts will extend to all university members beyond the computer science field, along with devising strategies to address phishing emails. (Chapman, J., 2019) highlighted that the security landscape is ever-changing due to the ongoing competition between attackers and defenders. Higher education institutions must continuously enhance their security measures to safeguard students, staff, and research data.

Leaders in higher education should play a key role in managing cyber risks. And emphasized on the importance of a national dialogue involving various stakeholders, including the government, to strengthen the resilience of the university sector against cyber threats. (Fernandez-Caramés et al., 2020) proposed a hands-on approach using Shodan, an Internet search engine, for practical IoT cybersecurity education. Students can perform audits using a web browser, exploring IoT devices. One student's report emphasized that the results highlight Shodan's potency as a cyber-security tool, effectively revealing misconfigurations and vulnerabilities in IoT devices with ease and speed. (Offner et al., 2021) explores global cyberattacks on healthcare, categorizes threats, and proposes protective strategies for a universal electronic health record in Australia. Firstly, the rapidly evolving cybersecurity landscape continually introduces new information. Secondly, due to the emerging nature of this field, there is limited scholarly research available on the topic. Similarly, (Tvaronavičienė et al., 2020) presented solutions of the top five countries by cybersecurity level based on the Global Cybersecurity Index (GCI) 2018: UK, USA, France, Estonia, and Lithuania. The assessment demonstrated the accuracy of the index and highlighted diverse approaches to Critical Infrastructure Protection.

In Table 2. we have employed a diverse range of encryption and security algorithms to address various data protection needs in cloud computing and beyond. Each algorithm brings its unique strengths and applications, catering to specific security needs and scenarios.

Table 2
Most Widely Used Cryptography, Data Security and Cyber Security Algorithms

Reference No	Algorithm Name
[22]	Pixel-based image encryption
[23]	DNA-based encryption
[24]	Novel pixel-based image encryption
[27]	Chaos-based cryptographic algorithm
[28]	Homomorphic encryption
[44]	Cumulative Sum-Based CUMSUM-based attack detection algorithm
[42]	Machine Learning (ML) algorithm

Steganalysis and Stenography in Cloud Computing

For steganalysis and Stenography in Cloud Computing, (Prasad et al., 2022) introduced a procedure under the compliance of Deep learning, Steganography, and Neural networks to explore security for the cloud atmosphere. Unlike watermark and cryptography, steganography developed an over-embedded function to hide secret data images that can be identifiable through Steganalysis's contribution, illustrated in Table 3. Results showed that the proposed method is effective in data mapping and recovery with a high-performance rate. The mechanism has future chances to append some Error codes to the solution. Similarly, (Sharath et al., 2019) analyzed a coherent secured platform for multimedia interaction and transformation in the Cloud Computing world.

The researchers need to focus on enlarging the productivity of crypt-steganography schemes in Cloud infrastructure. (Rahman et al., 2018) and (Kouchay., 2018) used a quantitative methodology to exaggerate the infrastructure security of Data stored in the Cloud. The technique included prominent manners of Blowfish cryptography algorithm and Steganography-based striking embedded algorithm followed by Discrete Cosine Transform (DTC) method, Embedded Least Significant Bits (E-LSB) and finally Hash function SHA-256 algorithm are applied, mentioned in Table 3.

At the initial level, the data is converted to encrypted format and then offered for customization and concealing covering images. The result of the analyzed experiment in Java Programming Language at Eclipse IDE showed better performance reports i.e., stego image with secure key structure, high key sensitivity, security to harm, and best quality of PSNR value were generated. (Kurt et al., 2018) presented conspicuous of Cyber-offenses and Cyber-breaches against Smart Grid. The Assessment showed better solution results as per intention with effective responses to stealthy attacks. Consequently, (Sloan, T., & Hernandez-Castro, J., 2018) dissented the sensitivity effectiveness and security concern of the OpenPuff Steganography approach for PDF files. The disagreement is analyzed based on steganalysis via attack to detect embedded Steganography using the OpenPuff tool in PDF files. The result implication explored the effectiveness of the attack and the vulnerability of the OpenPuff tool, it also finds OpenPuff resemblance with PDF data hiding and past findings regarding MP4 files. It might be useful for small data manipulation.

(Li et al., 2018) involved the Laplacian Smoothing mechanism of different degrees governed by a scale factor and the counts of Laplacian occurrence (k). The experiment claims smoothing parameters. In future determination, the scrutiny is to find an optimal smoothing framework. (Denis, R., & Madhubala, (2020) designed a high level of security approaches for the proposed Visually Imperceptible Hybrid Crypto-Steganography (VIHCS) algorithm. An Adaptive Genetic Algorithm, Optimal Pixel Adjustment (AGA-OPAP) is utilized to strengthen LSB operations and embedding efficiently. The suggested technique grants high defense protocol to cloud data. The future work is to compress this Model with enhanced security for multimedia data. In another article, (Mohsin, A. et al., 2018) conducted a survey to pursue the potential of Biometric Systems in the field of the Biometric system trend in Medical Sciences is discussed. It is used for the purpose of identification of certain vector sets of characteristics and manners such as face and finger recognitions are profoundly used concepts. (Cao, Y, et al., 2018) proposed model hided the useful information's through uncovered phenomena based on Molecular pattern. Histogram Bag of Words (BOW) and pseudo-random sequence of label is presented to recognize the count and locations of sub-images to probably secure each point. In comparison coverless information hiding approach has high level capacity then Zheng's but somehow less than the conventional systems. Table 3. illustrated some convenient steganography approaches been made to security enrollment.

Steganography is a technique developed to enforce concealing information into digital media, which only the desired person can access.

Table 3

Most Progressive Steganography Algorithms

Reference No	Steganography Approaches
Ref. [51]	Steganography without embedding
Ref. [52]	Steganography, Deep learning and Neural based Algorithm
Ref. [53]	E-LSB Steganography Algorithm
Ref. [55]	LSB/DTC (Linear Significant Bits/ Discrete Cosine Transform)
Ref. [58]	VIHCS model

Cloud Computing Security at different Layers

Security at IaaS Layer

Infrastructure as a Service (IaaS), is a cloud computing framework that allows users to instantly utilize computing assets like servers, storage, networking, and virtualization as needed. IaaS providers manage cloud security via a shared responsibility model. (Sriram, G. S., 2022) and (Sadeeq, et al., 2021) highlighted challenges like load balancing, privacy, security, storage, and quality of service (QoS) for the distribution of computational tasks among Virtual Machines (VMs) and the amalgamation of IoT and cloud computing to optimize performance. (Velmurugadass, et al., 2021) proposed a novel framework to improve security in various industries, including Electronic Health Records (EHR), Banking, Smart Applications (SA), Supply Chain Management (SCM), and the Internet of Things (IoT). The framework utilizes a combination of blockchain technology, a Cloud-based Software Defined Network (SDN), and the Elliptic Curve Integrated Encryption Scheme (ECIES) algorithm. The system starts with user registration and authentication using Harmony Search Optimization (HSO) to obtain a secret keyThe integration of ECIES encryption and blockchain technology provides robust security and privacy for data exchange in a cloud computing and IoT environment. Securing digital assets has become increasingly challenging as technologies continue to evolve rapidly, (Chavan, et al., 2013) discussed that the IaaS serves as the foundation layer for other cloud delivery models like Platform as a Service (PaaS) and Software as a Service (SaaS), any security vulnerabilities in the IaaS layer can impact the entire cloud ecosystem. Security Model for IaaS (SMI) guides security assessment and enhancement in the IaaS layer. Likewise, (Alouffi, et al., 2021) performed a Systematic Literature Review (SLR) on research published from 2010 to 2020, that probed cloud computing safety, threats, and alleviation strategies.

(Shabbir, et al., 2021) focused on Layered Security Modeling, MES, Requirement-Centric Approach, Secure HI Storage, and Multi-Layered Modular Security. It illustrated that MES outperforms other common encryption algorithms in terms of performance and security, and the performance analysis showcases the effectiveness of the proposed approach. A novel digital forensic architecture for cloud environments was described by (Pourvahab, et al., 2019). The evaluation encompasses measurements such as response time, evidence insertion time, evidence verification time, communication overhead, hash computation time, key generation time, encryption time, decryption time, and overall alteration rate. Furthermore, (Tissir, et al., 2021) proposed a 21-step framework and introduced key international standards, particularly ISO standards "27,001, 27,017, 27,032," and the NIST Cybersecurity Framework as guidelines for managing cyber risks effectively. This framework integrates the identified ISO standards and the NIST cybersecurity and addresses various aspects of cybersecurity, including identification, integrity, confidentiality, privacy, and durability. (Xu, S. et al., 2020) focused on the challenges related to data sharing in cloud-fog computing environments where data needs to be kept confidential, identifiable by ratified sources, and accessible to authorized recipients. Cloud-fog computing is a paradigm that extends the capabilities of cloud computing by utilizing edge devices (fog nodes) to provide various on-demand data services.

The authors proposed a solution with the use of bilinear maps, linear secret-sharing schemes, and hash functions to achieve its security properties. Cryptographic mechanism (MABE) combines fine-grained access control, data confidentiality, and source identification to enable efficient and secure data sharing in cloud-fog computing environments. Subsequently, (Chenthara, et al., 2019) explored security and privacy challenges in e-health solutions within cloud computing. Its retrospect's various privacy-preserving approaches for protecting Electronic Health Records (EHRs) stored on the cloud. The paper analyzed research questions and directions in cybersecurity to develop an extensive security model for EHRs. The discussion compares existing cryptographic and non-cryptographic approaches, highlighting limitations like computational costs, key management complexity, vulnerability to attacks, and lack of flexibility. The paper underscores the need to bolster security infrastructure in e-health systems for patient privacy and data security.

Security at HaaS Layer

Hardware as a Service (HaaS) is a cloud service model that provides organizations with access to physical hardware resources over the Internet. HaaS can provide benefits like cost savings and scalability, but organizations need to carefully assess the Data Protection, Physical Security, Compliance and Regulations, Service-Level Agreements (SLAs), Data Resilience and Redundancy, Monitoring and Auditing, Backup and Disaster Recovery, Incident Response, and Data Ownership and Access Control. (Singh, et al., 2020) expressed a literature review and highlighted various security issues Data Security, access for users with special privileges, Trust Issues, Data Recovery, Regulatory Compliance, and Data Locations, there are a few solutions and practices that help in solution.

Understanding cloud providers' compliance with data regulations, like the Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR), ensures secure data storage. Cloud computing gives a way to access computing resources on demand (Okorodudu, J., 2021), (Purcell, B, 2014), and (Yang et al., 2010) expressed that Platform as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Service (IaaS) are three initial cloud computing service models, Hardware as a Service (HaaS) is also included as a fourth model. It delves into different deployment models like private, public, hybrid, and community clouds. (Thanasegaran et al., 2022) defined a comparative study of cloud computing implementation in various sectors is presented, focusing on E-Health, E-Commerce, Banking, and the Construction Industry. The benefits of cloud computing in these sectors include cost savings, scalability, efficiency, and data accessibility. However, challenges like confidentiality, integrity, data privacy, and security hinder its widespread adoption. Likewise, (Brown, Tamaike) presents a Cloud Secured Services Venture (CSSV 1.0) to secure the usage of Cloud services.

It put in place the Cloud Model Security (CSM 2.0), introduing a three-layered infrastructure that enables secure data and user protection in federal laws. The prototype includes processing operators and enciphers keys to lead communication among clients and servers, ensuring protected information transmission. The paper acknowledged the benefits of Cloud-based computing and also expresses realistic issues that need to be pointed out. It presents that CSM 2.0 can be used for further effective Cloud security and resource management. Besides, (Aslam et al., 2022) analyzed cloud attacks, including compromised credentials, breaches of data, interfaces hacked, and phishing, among others. (Rohith et al., 2022) pointed out the method of protecting data and enabling confidentiality in an exposed cloud environment. The paper described a secure way to access the cloud by using 128-bit Advanced Encryption Standard (AES). The proposed procedure includes encryption with AES earlier than uploading it to the cloud, enabling data security and integrity.

(Kalagiakos, et al., 2011) introduced a cloud-based educational system that overcomes the limitation of distance learning. Cloud computing, consisting of HaaS, and SaaS expresses their possible effect on education. It points to the part of virtualization technology and Service-Oriented Architecture (SOA) in providing adaptable and useful cloud computing plans for education. Open Cloud Computing Education Federation (OCCEF) is an organization that could operate the standardization and merger of learning materials and services in the cloud. However, the lack of common cloud computing Application Programming Interface (API) standards creates a problem in accessing the interface between cloud computing suppliers. Likewise, (Suman et al., 2023) highlighted cloud computing's role and benefits in libraries, emphasizing cost reduction and modern resource provision.

Security at SaaS Layer

Securing Software as a Service (SaaS) in the context of cloud computing involves implementing a comprehensive set of measures to protect the data, applications, and infrastructure provided by the SaaS provider. It's essential to adopt a holistic approach, considering both technical and non-technical aspects of security. Regular security assessments and proactive monitoring are crucial components of an effective SaaS security strategy. (Hawedi et al., 2018) proposed a profitable and flexible Security as a Service (SaaS) model based on Intrusion Detection Systems (IDS) for cloud tenants. The proposed SaaS architecture consists of three components: Tenant Security Requirement Manager (TSRM), Lightweight IDS (LIDS), and Remote Advanced Attack Detection (RAAD). TSRM collects tenants' security needs and deploys appropriate LIDS. Furthermore, (George et al., 2023) highlighted security measures like zero-trust, authentication, encryption, and access control. Security challenges of cloud computing (IaaS, PaaS, SaaS) highlighting shared obligation and the significance of penetration testing to expose vulnerabilities in these environments. (Ouda et al., 2022) explored cloud impact on network security, focusing on hazards to organizational behaviors. Challenges in privacy and data protection due to third-party services emphasize the importance of security for processing, storage, and service availability. The cloud computing model encompasses technologies like virtualization, Web 2.0, and SOA, using the internet for online services.

The document identifies vulnerabilities, and threats, and proposes solutions to mitigate risks in cloud computing. The study used the Service Platform Infrastructure (SPI) model to classify cloud security issues, analyze vulnerabilities across SaaS, PaaS, and IaaS layers, and address major threats. (Shakir et al., 2018) emphasizes security and privacy in the public cloud, highlighting identification, authentication, authorization, confidentiality, and integrity, and stress legal compliance and user data protection with access rights. The authors analysis revealed authentication, data integration, encryption, system, and workflow layers are a common focus of security frameworks in public clouds. (Díaz de León Guillén et al., 2020) acknowledged data migration, and used the Security Assurance and Language for Software as a Service (SALSA) framework for threat analysis, and mitigation in SaaS covering threat identification, attack detection, and SaaS countermeasures. The review spotlighted SaaS traditional and novel security challenges and advocates robust authentication, encryption, and comprehensive security, and suggests research for emerging attacks and evolving cloud scenarios.

Likewise, (Rath et al., 2019) delved into security patterns for Cloud SaaS apps covering system, data security, privacy, and compliance. The aim is to offer SaaS developers best practices for creating secure apps. The paper provides solutions for security challenges, especially in AWS and Azure, and guides developers in building trustworthy Cloud SaaS apps. (Parast et al., 2022) discussed the service-based models of IaaS, PaaS, and SaaS, and emphasized the importance of addressing security concerns as cloud computing becomes increasingly dominant in various sectors. The paper introduced enabling technologies of virtualization multitenancy (VM) and service-oriented Architecture (SOA) for cloud services. Besides, (Elsayed et al., 2019) introduced Software Development as a Service (SDaaS) for SaaS app security analysis in the cloud, which tackles challenges from service-oriented, microservices, and web tech. The aim of the paper was to detect information flow vulnerabilities and assess SaaS app security. Framework components include Lifecycle Model Generator, Dependency Model Constructor, Vulnerability Detector, and Protection Diagnosis Practitioner. The paper acknowledges SaaS adoption, security challenges with web services, and APIs in cloud apps. SDaaS framework quantitatively analyzes SaaS security through static info flow analysis which aims to detect vulnerabilities and ensure data integrity, and confidentiality.

The value Computation Approach suggested by authors suggests IDE-based value computation for inter-service interactions that enhances security accuracy by resolving external service dependencies. Based on the results, the authors test SDaaS accuracy, performance, and scalability and demonstrate that SDaaS is superior with higher accuracy, and coverage of vulnerability compared to other tools Experiments confirmed the framework's effectiveness, accuracy, scalability, lifecycle, dependency modeling, and value computation for precise diagnosis. (Sharif et al., 2019) highlighted SaaS's robust security, cost-effectiveness, significance, architecture, and performance in Cloud Computing through the online questionnaire. The Methodology defines and classifies Cloud SaaS security patterns, following Open Web Application Security Project (OWASP) guidelines.

Cloud tools like Cloud Bastion, GuardDuty, CloudWatch, and Web Application Firewall (WAF) were discussed for security. The study analyzed service quality via response time, and load balancing across data centers, and explored cloud-based Enterprise Resource Planning (ERP) and SaaS advantages (e.g.) for faster implementation, and cost savings. Similarly, (Akinrolabu et al., 2019) proposed the CSCCRA model (Cloud Supply Chain Cyber Risk Assessment) as a Quantitative Risk Assessment (QRA) solution for SaaS cloud service givers. Risk recognition involves analyzing a cloud application's elemental and recognizing assets, vulnerabilities, threats, Effects, consequences, and controls preliminarily. Risk guesses defined risk through events, outcomes, frequency, and volatility using Monte Carlo simulation. Risk appraisement ranked and treats perils with security practices. Cloud Quantitative Risk Analysis (CQRA) employs possibility distributions and Monte Carlo simulation for exact assessment. Cloud Supplier Security Assessment (CSSA) evaluates supplier safety and guides decisions.

Cloud Supply Chain Mapping (CSCM) visualizes supply chains, exhibiting key suppliers and weaknesses. Mathematical methods like PERT distribution, Poisson distribution, and Monte Carlo simulation estimate risk. The CSCCRA model fills gaps in conventional assessment, addressing cloud supply chain transparency and providing a structured framework. The complete cloud computing model components are depicted in the below figure. Figure 3. depicts a comprehensive overview of three distinct cloud computing models: SaaS, HaaS, and IaaS. Each model is highlighted with its individual components and connectivity, while ordinary elements shared among all models are also emphasized. The Software as a Service (SaaS) model is depicted as a pivotal cloud computing approach connecting with servers, storage, and hosted applications. It facilitates direct internet access to software, eliminating local installations for user convenience. Hardware as a Service (HaaS) is presented as an integrated ecosystem linking main servers, storage, development tools, and databases, catering to a range of technical needs. Infrastructure as a Service (IaaS) serves as the foundation, connecting with core server and storage components while encompassing data centers and physical infrastructure, offering customization resources. Common networking and firewall components ensure seamless connectivity and security across all models. A notable feature is the shared operating system, enhancing adaptability and consistency in cloud computing environments.

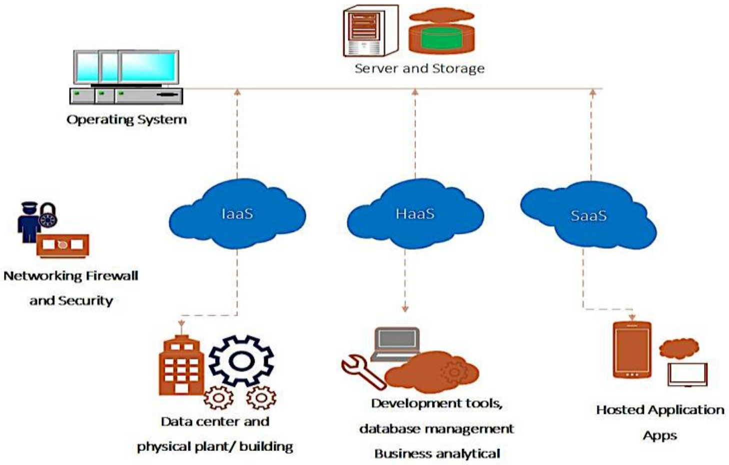
Server and Storage
Operating System
Networking Firewall and Security
IaaS
HaaS
SaaS
Data center and physical plant/ building
Development tools, database management Business analytical
Hosted Application Apps

Figure 3: Cloud Computing Models Components

Table 4. mentions a list of algorithms most used in various models of cloud computing to address different aspects of security, access control, and optimization. The Advanced Encryption Standard (AES) algorithm is broadly regarded as highly secure and efficient for symmetric encryption. It offers a good balance between security and performance. It is well-suited for encrypting data and in transit in cloud environments.

Future of Security in Cloud Computing

Cloud computing is an everlasting technology that will remain there for at least the next two decades. Data centers will generate huge revenue but will be a target of intruders, scammers, hackers, and data abusers. The next generation of fights between nations will be to attack the data centers and the clouds with data repositories, thus security is one of the most important issues that will be kept enhanced and strengthened. Any country possessing strong security, firewalls, and other software and hardware devices that are secure will survive. Security in cloud computing, regardless of the service model (SaaS, IaaS, HaaS, PaaS), involves a combination of encryption, access controls, identity management, and other measures. While specific algorithms might not always be explicitly mentioned, various cryptographic and security-related techniques are commonly applied across different cloud service models.

Table 4
Cloud Computing's Widely Used Algorithms in IaaS, PaaS, and SaaS

Reference No.	Algorithm Name
[58], [62], [76]	Advanced Encryption Standard (AES)
[40],[67]	Elliptic Curve Cryptography (ECC)
[76]	Role-Based Access Control (RBAC)
[75], [86]	Multi-Factor Authentication (MFA)
[63],[67]	Harmony Search Optimization (HSO)
[71], [81]	Intrusion Detection System
[23], [53], [67]	Hash Algorithm
[76]	128-AES/ ABE/ RBAC

In this study, we found out that the most commonly used algorithms for Encryption are Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) but in certain scenarios, homomorphic encryption allows performing computations on encrypted data without decrypting it. For Access Control, Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) are the most commonly used algorithms to make access control decisions dynamic. For Identity and Authentication, hash algorithms (SHA-256 and Multi-Factor Authentication - MFA) are frequently used. For Intrusion Detection and Prevention, Intrusion Detection Systems, Signature-Based Detection, and Anomaly-Based Detection are used to identify known patterns and normal system behavior of malicious activity using predefined signatures adapted over time. Security Information and Event Management (SIEM) systems use correlation algorithms to analyze and correlate various security events to identify potential security incidents. Key Exchange Algorithms like Diffie-Hellman are used for secure key exchange during the establishment of secure communication channels. To reduce the risk associated with data exposure Tokenization is used for securing sensitive data in SaaS applications, tokenization replaces sensitive information with tokens.

However, algorithms that are novel and a combination of these strong security algorithms will be the future of research in the cloud computing security field. Technologies and techniques such as Machine learning, Deep learning, Steganalysis and steganography, IOTs, and Big Data analytics are and will be dependent on cloud computing and thus its security is a primary concern for the upcoming generation of scientists. It's important to note that the specific algorithms and protocols used can vary based on the cloud service provider and the security features they implement. Additionally, advancements in cryptography and security practices may introduce new algorithms over time. Regularly updating and patching systems is crucial for maintaining a secure cloud environment.

References

Abood, O. G., & Guirguis, S. K. (2018). A survey on cryptography algorithms. *International Journal of Scientific and Research Publications*, *8*(7), 495-516.

Ahmad, M., Al Solami, E., Wang, X. Y., Doja, M. N., Beg, M. S., & Alzaidi, A. A. (2018). Cryptanalysis of an image encryption algorithm based on combined chaos for a BAN system, and improved scheme using SHA-512 and hyperchaos. *Symmetry*, *10*(7), 266.

Akinrolabu, O., New, S., & Martin, A. (2019). CSCCRA: A novel quantitative risk assessment model for cloud service providers. In Information Systems: 15th European, Mediterranean, and Middle Eastern Conference, EMCIS 2018, Limassol, Cyprus, October 4-5, 2018, Proceedings 15 (pp. 177-184). Springer International Publishing.

Almshari, M., Tsaramirsis, G., Khadidos, A. O., Buhari, S. M., Khan, F. Q., & Khadidos, A. O. (2020). Detection of potentially compromised computer nodes and clusters connected on a smart grid, using power consumption data. *Sensors*, *20*(18), 5075.

Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A systematic literature review on cloud computing security: threats and mitigation strategies. *IEEE Access*, *9*, 57792-57807.

Alloghani, M., Alani, M. M., Al-Jumeily, D., Baker, T., Mustafina, J., Hussain, A., & Aljaaf, A. J. (2019). A systematic review on the status and progress of homomorphic encryption technologies. *Journal of Information Security and Applications*, *48*, 102362.

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, *7*(1).

Amsyar, I., Christopher, E., Dithi, A., Khan, A. N., & Maulana, S. (2020). The challenge of cryptocurrency in the era of the digital revolution: A review of systematic literature. *Aptisi Transactions on Technopreneurship (ATT)*, *2*(2), 153-159.

Aslam, J. M., & Kumar, K. M. (2022) “Assessment of Security Attacks In Cloud”.

Artiles, J. A., Chaves, D. P., & Pimentel, C. (2019). Image encryption using block cipher and chaotic sequences. *Signal processing: image communication*, *79*, 24-31.

Brown, Tamaike. "Cloud Security Model Csm 2.0: An Autonomic Cloud Security Gateway."

Cao, Y., Zhou, Z., Sun, X., & Gao, C. (2018). Coverless information hiding based on the molecular structure images of material. *Computers, Materials & Continua*, *54*(2).

Chai, X., Zheng, X., Gan, Z., Han, D., & Chen, Y. (2018). An image encryption algorithm based on chaotic system and compressive sensing. *Signal Processing*, *148*, 124-144.

Chapman, J. (2019). *How Safe is Your Data? Cyber-security in Higher Education* (Vol. 12, pp. 1-6). Oxford, UK: Higher Education Policy Institute.

Chavan, P., Patil, P., Kulkarni, G., Sutar, R., & Belsare, S. (2013, December). IaaS cloud security. In *2013 International Conference on Machine Intelligence and Research Advancement* (pp. 549-553). IEEE.

Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy-preserving challenges of e-health solutions in cloud computing. *IEEE access*, *7*, 74361-74382.

Denis, R., & Madhubala, P. (2020). Evolutionary computing assisted visually-imperceptible hybrid cryptography and steganography model for secure data communication over cloud environment. *Int. J. Comput. Netw. Appl*, *7*, 208-230.

Díaz de León Guillén, M. Á., Morales-Rocha, V., & Fernández Martínez, L. F. (2020). A systematic review of security threats and countermeasures in SaaS. *Journal of Computer Security*, *28*(6), 635-653.

Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5-32.

Elsayed, M., & Zulkernine, M. (2019). Offering security diagnosis as a service for cloud SaaS applications. *Journal of information security and applications*, *44*, 32-48.

Faiz, M., Fatima, N., Sandhu, R., Kaur, M., & Narayan, V. (2022). Improved Homomorphic Encryption for Security in Cloud using Particle Swarm Optimization. *Journal of Pharmaceutical Negative Results*, 4761-4771.

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2020). Teaching and learning iot cybersecurity and vulnerability assessment with shodan through practical use cases. *Sensors*, *20*(11), 3048.

Furstenau, L. B., Sott, M. K., Homrich, A. J. O., Kipper, L. M., Al Abri, A. A., Cardoso, T. F., ... & Cobo, M. J. (2020, March). 20 years of scientific evolution of cyber security: A science mapping. In *International Conference on Industrial Engineering and Operations Management* (pp. 314-325). IEOM Society International.

George, A. S., & Sagayarajan, S. (2023). Securing Cloud Application Infrastructure: Understanding the Penetration Testing Challenges of IaaS, PaaS, and SaaS Environments. *Partners Universal International Research Journal*, *2*(1), 24-34.

Gruschka, N., Mavroeidis, V., Vishi, K., & Jensen, M. (2018). Privacy issues and data protection in big data: a case study analysis under GDPR. In *2018 IEEE International Conference on Big Data* (pp. 5027-5033). IEEE.

Hao, M., Li, H., Luo, X., Xu, G., Yang, H., & Liu, S. (2019). Efficient and privacy-enhanced federated learning for industrial artificial intelligence. *IEEE Transactions on Industrial Informatics*, *16*(10), 6532-6542.

Hariss, K., Noura, H., & Samhat, A. E. (2020). An efficient fully homomorphic symmetric encryption algorithm. *Multimedia Tools and Applications*, *79*, 12139-12164.

Hasan, M. K., Ghazal, T. M., Saeed, R. A., Pandey, B., Gohel, H., Eshmawi, A. A., ... & Alkhassawneh, H. M. (2022). A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. *IET Communications*, *16*(5), 421-432.

Hawedi, M., Talhi, C., & Boucheneb, H. (2018). Security as a service for public cloud tenants (SaaS). *Procedia computer science*, *130*, 1025-1030.

Jan, S., Maqsood, I., Ahmad, I., Ashraf, M., Khan, F. Q., & Imran, M. (2019). A systematic feasibility analysis of user interfaces for illiterate users. *Proc. Pak. Acad. Sci*, *56*, 75-91.

Khan, F. Q., Ishaq, M., Khan, A. I., & Soubani, B. (2014). Adapting Cloud Computing in Higher Education. *International Journal of Scientific & Engineering Research*, *5*(11), 823-830.

Khan, I. A., & Qazi, R. (2019). Data security in cloud computing using elliptic curve cryptography. *International Journal of Computing and Communication Networks*, 46-52.

Khattak, S., Jan, S., Ahmad, I., Wadud, Z., & Khan, F. Q. (2021). An effective security assessment approach for Internet banking services via deep analysis of multimedia data. *Multimedia Systems*, *27*, 733-751.

Kouchay, S. A. (2018). An Efficient Scheme of Crypto System with Steganography for Cloud Security Environment.

Kurt, M. N., Yılmaz, Y., & Wang, X. (2018). Real-time detection of hybrid and stealthy cyber-attacks in smart grid. *IEEE Transactions on Information Forensics and Security*, *14*(2), 498-513.

Kalagiakos, P., & Karampelas, P. (2011, October). Cloud computing learning. In 2011 5th international conference on the Application of information and communication technologies (AICT) (pp. 1-4). IEEE.

Li, C., Zhang, Y., & Xie, E. Y. (2019). When an attacker meets a cipher-image in 2018: A year in review. *Journal of Information Security and Applications*, *48*, 102361.

Li, T., Du, B., & Liang, X. (2020). Image encryption algorithm based on logistic and two-dimensional lorenz. *Ieee Access*, *8*, 13792-13805.

Li, Y., Wang, R., Li, Y., Zhang, M., & Long, C. (2023). Wind power forecasting considering data privacy protection: A federated deep reinforcement learning approach. *Applied Energy*, *329*, 120291.

Li, Z., Liu, F., & Bors, A. G. (2018, June). 3D steganalysis using laplacian smoothing at various levels. In *International Conference on Cloud Computing and Security* (pp. 223 232). Cham: Springer International Publishing.

Lu, X., Lei, J., Li, W., Lai, K., & Pan, Z. (2018). Physical layer encryption algorithm based on polar codes and chaotic sequences. *Ieee Access*, *7*, 4380-4390.

Luo, Y., Zhou, R., Liu, J., Cao, Y., & Ding, X. (2018). A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map. *Nonlinear Dynamics*, *93*, 1165-1181.

Mohsin, H., Zaidan, A., Zaidan, B., Ariffin, B., Albahri, S., Albahri, S., ... & Hashim, M. (2018). Real-time medical systems based on human biometric steganography: A systematic review. *Journal of medical systems*, *42*, 1-20.

Mohamed, H. G., ElKamchouchi, D. H., & Moussa, K. H. (2020). A novel color image encryption algorithm based on hyperchaotic maps and mitochondrial DNA sequences. *Entropy*, *22*(2), 158.

Mohammed, I. A. (2020). Artificial intelligence for cybersecurity: A systematic mapping of literature. *Artif. Intell*, *7*(9), 1-5.

Mondal, B., Kumar, P., & Singh, S. (2018). A chaotic permutation and diffusion-based image encryption algorithm for secure communications. *Multimedia Tools and Applications*, *77*, 31177-31198.

Namasudra, S., Chakraborty, R., Majumder, A., & Moparthi, N. R. (2020). Securing multimedia by using DNA-based encryption in the cloud computing environment. *ACM Transactions on Multimedia Computing, Communications, and Applications*, *16*(3s), 1-19.

Offner, K. L., Sitnikova, E., Joiner, K., & MacIntyre, C. R. (2021). Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. *Health Security Intelligence*, 92-121.

Okorodudu, J. (2021). An Insight into Cloud Computing Technology. Innovative Journal of Science (ISSN: 2714-3309), 3(3), 01-09.

Ouda, A. J., Yousif, A. N., Hasan, A. S., Ibrahim, H. M., & Shyaa, M. A. (2022). The impact of cloud computing on network security and the risk for organization behaviours. *Webology*, *19*(1), 195-206.

Ouda, A. J., Yousif, A. N., Hasan, A. S., Ibrahim, H. M., & Shyaa, M. A. (2022). The impact of cloud computing on network security and the risk for organization behaviors. *Webology*, *19*(1), 195-206.

Parast, F. K., Sindhav, C., Nikam, S., Yekta, H. I., Kent, K. B., & Hakak, S. (2022). Cloud computing security: A survey of service-based models. *Computers & Security*, *114*, 102580.

Pourvahab, M., & Ekbatanifard, G. (2019). Digital forensics architecture for evidence collection and provenance preservation in iaas cloud environment using sdn and blockchain technology. *IEEE Access*, *7*, 153349-153364.

Prasad, P. V. H., & Rao, K. G. (2022). A Security Approach using Steganography, Deep Learning and Conventional Neural Networks in a Cloud Environment.

Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81.

Purcell, B. M. (2014). Big data using cloud computing. Journal of Technology Research, 5, 1.

Rahman, M. O., Hossen, M. K., Morsad, M. G., & Chandra, A. (2018). An approach for enhancing security of cloud data using cryptography and steganography with e-lsb encoding. *IJCSNS*, *18*(9), 85.

Rahman, S., Masood, F., Khan, W. U., Ullah, N., Khan, F. Q., Tsaramirsis, G., & Ashraf, M. (2020). A novel approach of image steganography for secure communication based on LSB substitution technique. *Computers, Materials & Continua*, *64*(1), 31-61.

Rath, A., Spasic, B., Boucart, N., & Thiran, P. (2019). Security pattern for cloud saas: From system and data security to privacy case study in aws and azure. *Computers*, *8*(2), 34.

Rohith, S., & Pawar, M. V. (2022) "Secure Cloud Access Using AES Encryption and Decryption Algorithm".

Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. *Computers & Security*, *86*, 147-167.

Sadeeq, M., Abdulkareem, M., Zeebaree, R., Ahmed, M., Sami, S., & Zebari, R. (2021). IoT and Cloud computing issues, challenges and opportunities: A review. *Qubahan Academic Journal*, *1*(2), 1-7.

Shabbir, M., Shabbir, A., Iwendi, C., Javed, A. R., Rizwan, M., Herencsar, N., & Lin, J. C. W. (2021). Enhancing security of health information using modular encryption standard in mobile cloud computing. *IEEE Access*, *9*, 8820-8834.

Sharath, M. N., Rajesh, T. M., & Patil, M. (2019, July). Analysis of secure multimedia communication in cloud computing. In *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)* (*Vol*. 1, pp. 136-144). IEEE.

Shakir, M., Hammood, M., & Muttar, A. K. (2018). Literature review of security issues in saas for public cloud computing: a meta-analysis. *International Journal of Engineering & Technology*, *7*(3), 1161-1171.

Sharif, M. H. U., & Datta, R. (2019). Software as a service has strong cloud security. *Retrieved from URL: https://www.researchgate.net/profile/Haris_Sharif/publication/335232826_Software_as_a_Service_has_Strong_Cloud_Security/l in ks/5d6466fc299bf1f70b0eb0f2/Software-as-a-Service-has-Strong-Cloud-Security. pdf*.

Singh, H. P., Singh, R., & Singh, V. (2020). Cloud computing security issues, challenges and solutions (No. 2533). EasyChair.

Sloan, T., & Hernandez-Castro, J. (2018). Dismantling openpuff pdf steganography. *Digital Investigation*, *25*, 90-96.

Sirichotedumrong, W., Maekawa, T., Kinoshita, Y., & Kiya, H. (2019, September). Privacy-preserving deep neural networks with pixel-based image encryption considering data augmentation in the encrypted domain. In *2019 IEEE International Conference on Image Processing (ICIP)* (pp. 674-678). IEEE.

Sriram, G. S. (2022). Challenges of cloud compute load balancing algorithms. *International Research Journal of Modernization in Engineering Technology and Science*, *4*(1), 1186-1190.

Srivastava, G., Jhaveri, R. H., Bhattacharya, S., Pandya, S., Maddikunta, P. K. R., Yenduri, G., ... & Gadekallu, T. R. (2022). XAI for cybersecurity: state of the art, challenges, open issues and future directions. *arXiv preprint arXiv:2206.03585*.

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society*, *71*, 15-29.

Suman, A. K., Patel, M., & Vijesh, P. V. (2023). An Efficacy of Cloud Computing and Its Application in Libraries. *International Journal of Research and Analysis in Science and Engineering*, *3*(3), 15-15.

Tauqeer, O. B., Jan, S., Khadidos, A. O., Khadidos, A. O., Khan, F. Q., & Khattak, S. (2021). Analysis of security testing techniques. *Intelligent Automation & Soft Computing*, *29*(1), 291-306.

Teh, J. S., Alawida, M., & Sii, Y. C. (2020). Implementation and practical problems of chaos-based cryptography revisited. *Journal of Information Security and Applications*, *50*, 102421.

Thabit, F., Alhomdy, S., Al-Ahdal, A. H., & Jagtap, S. (2021). A new lightweight cryptographic algorithm for enhancing data security in cloud computing. *Global Transitions Proceedings*, *2*(1), 91-99.

Thanasegaran, K., & Zolkipli, M. F. (2022). Comparative Study on Cloud Computing Implementation and Security Challenges. Borneo International Journal eISSN 2636-9826, 5(3), 14-26.

Tissir, N., El Kafhali, S., & Aboutabit, N. (2021). Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. *Journal of Reliable Intelligent Environments*, *7*, 69-84.

Tikkinen-Piri, Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134-153.

Tvaronavičienė, M., Plėta, T., Della Casa, S., & Latvys, J. (2020). Cyber security management of critical energy infrastructure in national cybersecurity strategies: Cases of USA, UK, France, Estonia and Lithuania. *Insights into regional development*, *2*(4), 802-813.

Vaseghi, B., Hashemi, S. S., Mobayen, S., & Fekih, A. (2021). Finite time chaos synchronization in time-delay channel and its application to satellite image encryption in OFDM communication systems. *Ieee Access*, *9*, 21332-21344.

Velmurugadass, P., Dhanasekaran, S., Anand, S. S., & Vasudevan, V. (2021). Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm. *Materials Today: Proceedings*, *37,* 2653-2659.

Vinoth, S., Vemula, L., Haralayya, B., Mamgain, P., Hasan, M. F., & Naved, M. (2022). Application of cloud computing in banking and e-commerce and related security threats. *Materials Today: Proceedings*, *51*, 2172-2175.

Wang, W., Si, M., Pang, Y., Ran, P., Wang, H., Jiang, X., ... & Jeon, G. (2018). An encryption algorithm based on combined chaos in body area networks. *Computers & Electrical Engineering*, *65*, 282-291

Xu, S., Ning, J., Li, Y., Zhang, Y., Xu, G., Huang, X., & Deng, R. H. (2020). Match in my way: Fine-grained bilateral access control for secure cloud-fog computing. *IEEE Transactions on Dependable and Secure Computing*, *19*(2), 1064-1077.

Yamin, M., & Tsaramirsis, G. (2012). Cloud economy & its implications for Saudi Arabia. In *2012 Proceedings of Fourth Annual American Business Research Conference, New York*.

Yang, J., & Chen, Z. (2010, December). Cloud computing research and security issues. In 2010 International Conference on Computational Intelligence and Software Engineering (pp. 1-3). IEEE.