VOL. 10 NO. 9,
NOVEMBER, 2025
E-ISSN 3026-958X
P-ISSN 3027-1169

African Scholar Publications & Research International
www.africanscholarpub.com

Journal of Science Innovation & Technology Research (JSITR)

Secretary Bird-Inspired Optimization of Advanced Encryption Standard (AES) and Blowfish Encryption Algorithms for Robust Data Protection

***Obisesan, Rachael Oyeranti; **Mayowa Oyedepo Oyediran; **Ojo Olufemi Samuel; & **Obisesan, Stephen Oluwatosin**

*School of Sciences, Department of Computer Science, Kwara State College of Education, Ilorin. **Department of Computer Science, Ajayi Crowther University, Oyo, Oyo State

Corresponding Author: obisesanranti7@gmail.com

DOI: https://doi.org/10.70382/ajsitr.v10i9.053

Abstract

This study explores the hybridization of AES and Blowfish encryption algorithms to enhance data security, particularly for medical datasets. While combining these ciphers offers improved robustness, it also introduces challenges such as increased computational overhead, latency, and reduced throughput due to dual encryption processes. To address these issues, the Secretary Bird Optimization Algorithm (SBOA) was integrated to intelligently optimize key sizes, S-box configurations, and round parameters, improving both security and performance. Using twenty CT chest X-ray images from Kaggle.com, the model was implemented in MATLAB R2023a and evaluated based on encryption time, execution time, and throughput. Results showed that AES alone had an encryption time of 24.9954 seconds, execution time of 49.9260 seconds, and throughput of 0.9705 MB/s. Blowfish performed slower, with 53.2667 seconds encryption time, 79.7522 seconds execution time, and 0.6656 MB/s throughput. The hybrid AES–Blowfish model improved performance with 7.8765 seconds encryption time, 15.6502 seconds execution time, and 3.2550 MB/s throughput. However, the optimized SBOA–AES–Blowfish model outperformed all others, achieving 3.1791 seconds encryption time, 6.3386 seconds execution time, and 6.4905 MB/s throughput. In conclusion, the SBOA-enhanced hybrid encryption model demonstrated superior performance, offering the fastest

processing and highest throughput while maintaining strong security. These findings confirm that SBOA optimization significantly improves computational efficiency, making the model highly suitable for real-time and large-scale applications such as healthcare and secure communications.

Keywords: AES optimization, Secretary Bird Optimization Algorithm, bio-inspired cryptography, data security, cloud computing.

Introduction

The Advanced Encryption Standard (AES) is a trusted symmetric encryption method known for its security and efficiency. To meet growing demands for lightweight, high-performance cryptography, researchers are exploring optimization techniques like the Secretary Bird Optimization Algorithm (SBOA). Inspired by the strategic hunting behavior of the secretary bird, SBOA offers strong exploration and exploitation capabilities, making it ideal for tuning cryptographic parameters and designing secure S-boxes. Integrating SBOA with AES has shown improvements in encryption speed, reduced resource usage, and stronger resistance to attacks. This nature-inspired approach marks a promising advancement in scalable, adaptive cybersecurity solutions (Dauda & Abubakar, 2023).

Among the many strategies for securing cloud data, cryptography stands out as one of the most essential (Sasikumar & Nagarajan, 2024). Cryptography refers to the practice of designing secure communication techniques to prevent unauthorized access to confidential data, information, or messages (Adee & Mouratidis, 2022). It encompasses key principles of information security confidentiality, integrity, authentication, and non-repudiation (CIA)which are central to modern encryption systems. The strength of an encryption algorithm lies in its capacity to protect data from breaches while maintaining efficiency and speed during encryption and decryption processes (Adebayo et al., 2024).

Symmetric key encryption remains a robust defense mechanism against unauthorized data access (Shakor et al., 2024). Blowfish, a symmetric block cipher, offers unique benefits such as strong encryption and flexible key lengths (Ahmad et al., 2024). It has been effectively applied in FPGA-based systems with parallel pipelined memory to enhance power and throughput in secure Internet of Things (IoT) networks. By combining the distinctive features of Blowfish and the Advanced Encryption Standard (AES), researchers have developed improved hybrid encryption techniques that offer greater reliability and adaptability.

In cloud computing, adopting such a hybrid encryption standard provides substantial benefits. It ensures high levels of confidentiality, integrity, and authenticity, safeguarding sensitive data from unauthorized modification or access. Moreover, blending multiple algorithms, such as AES, enhances compatibility and interoperability across diverse cloud systems. Ultimately, this advancement reflects the ongoing evolution of encryption technologies to address emerging cloud security threats,

reinforcing trust in cloud-based infrastructures.

Hybridizing the AES and Blowfish encryption algorithms offers a promising approach to enhancing data security by leveraging the strengths of both ciphers. However, this technique introduces several research-level challenges, particularly in terms of performance degradation due to increased latency and reduced throughput caused by the computational demands of running two distinct algorithms either sequentially or in parallel. Inefficiencies also arise from poorly aligned parameters such as key schedules, S-box configurations, and round distributions, which can compromise system effectivenessespecially in resource-constrained environments like IoT and embedded systems. Furthermore, without careful integration, the hybrid model may suffer from security vulnerabilities and compatibility issues that weaken its resistance to cryptanalysis

The Advanced Encryption Standard (AES) remains a foundational tool in cybersecurity due to its reliability and efficiency. However, as digital systems grow more complexespecially in resource-constrained environments like IoT and embedded platformstraditional AES implementations face limitations in terms of computational overhead, latency, and adaptability. Hybrid encryption schemes, such as AES–Blowfish, aim to enhance security by combining multiple ciphers, but they often suffer from performance inefficiencies and misaligned parameters. These challenges are compounded by the lack of intelligent mechanisms for dynamically tuning cryptographic settings to suit varied operational needs.To address these issues, the Secretary Bird Optimization Algorithm (SBOA), inspired by the strategic hunting behavior of the secretary bird, offers a novel metaheuristic approach to optimizing AES configurations. SBOA systematically adjusts key schedules, S-box designs, and round allocations, enabling adaptive tuning that balances encryption strength with resource efficiency. This research explores the integration of SBOA into AES optimization, with the goal of reducing latency, increasing key entropy, and enhancing overall cryptographic performance. By applying nature-inspired intelligence to encryption design, the study presents a promising solution to modern data security challenges, particularly in dynamic and constrained computing environments (Al-Saadi et al., 2024; Arora et al., 2023; Zuo et al., 2025).

This study aim to develop a secretary bird optimized hybrid advanced encryption standard and blowfish encryption algorithms for data security. In specific terms, the study's objectives are to:

1. Design an optimized AES-BLOWFISH encryption technique for data security using Secretary Bird Optimization Algorithm **(**SBOA)
2. Implement the designed technique using MATLAB R (2023a) software.
3. Use means square error, throughput, encryption time, and execution time to assess the effectiveness of the designed technique.
4. Compare the results of the optimized AES-BLOWFISH with AES-blowfish and individual encryption technique.

Cloud Computing

Cloud computing has revolutionized how individuals and organizations access and manage data and applications by offering on-demand access to configurable resources like servers, storage, and software over the internet (Sunyaev&Sunyaev, 2020). Its flexibility, scalability, and cost-efficiency have accelerated adoption, driven by growing data volumes, real-time analytics needs, and remote work demands (George et al., 2023). Providers now offer diverse service modelsInfrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) (Kansal et al., 2023)though this shift raises concerns about privacy and data security.Virtualization enables multiple virtual environments on a single server, optimizing resource use and reducing hardware costs (Alam et al., 2020). Security features like encryption, multi-factor authentication, and monitoring help protect cloud-stored data (Almadani et al., 2023). On-demand services allow businesses to scale resources dynamically, which is especially beneficial for large-scale web applications (Wang et al., 2020). Resource pooling further enhances efficiency by distributing computing power among multiple tenants, lowering costs through shared infrastructure and economies of scale (Ravikumar et al., 2024; Gholami et al., 2024).Broad network access is another key feature, allowing users to connect to cloud resources from any device and location (Ahmad et al., 2020). This accessibility supports global operations and enables rapid service expansion. Cloud providers ensure geographic distribution of data centers for faster access and disaster recovery (Katal et al., 2023). While broad access improves usability, it also introduces potential security risks that must be managed carefully.

Cloud Deployment Models

This content explores various cloud deployment modelspublic, private, community, and hybridand their implications for data security and operational efficiency. Public clouds, offered by providers like AWS, Azure, and GCP, are cost-effective and scalable due to shared resources, making them ideal for businesses with fluctuating workloads (Ponnusamy & Spanner, 2023; Salman et al., 2024). However, they pose risks related to data breaches and compliance, necessitating strong security measures (Gade, 2020). In contrast, private clouds offer greater control and customization, making them suitable for organizations with strict regulatory and performance requirements, such as financial or healthcare institutions (Bongiovanni et al., 2022; Rauf et al., 2024).Community clouds serve multiple organizations with shared interests, such as compliance or operational needs, and are particularly beneficial for sectors like government and healthcare. They offer tailored controls while maintaining privacy (Li et al., 2019; Yang et al., 2022). Hybrid clouds combine the strengths of public and private models, offering both scalability and security (Mallo et al., 2024). Within this context, the development of a hybrid encryption system aims to enhance data protection in hybrid cloud environments by integrating symmetric and asymmetric encryption techniques. The proposed system will include secure key distribution and storage mechanisms across cloud layers to

ensure robust, scalable, and high-performance security (Martínez Guevara et al., 2024; Gupta et al., 2022).

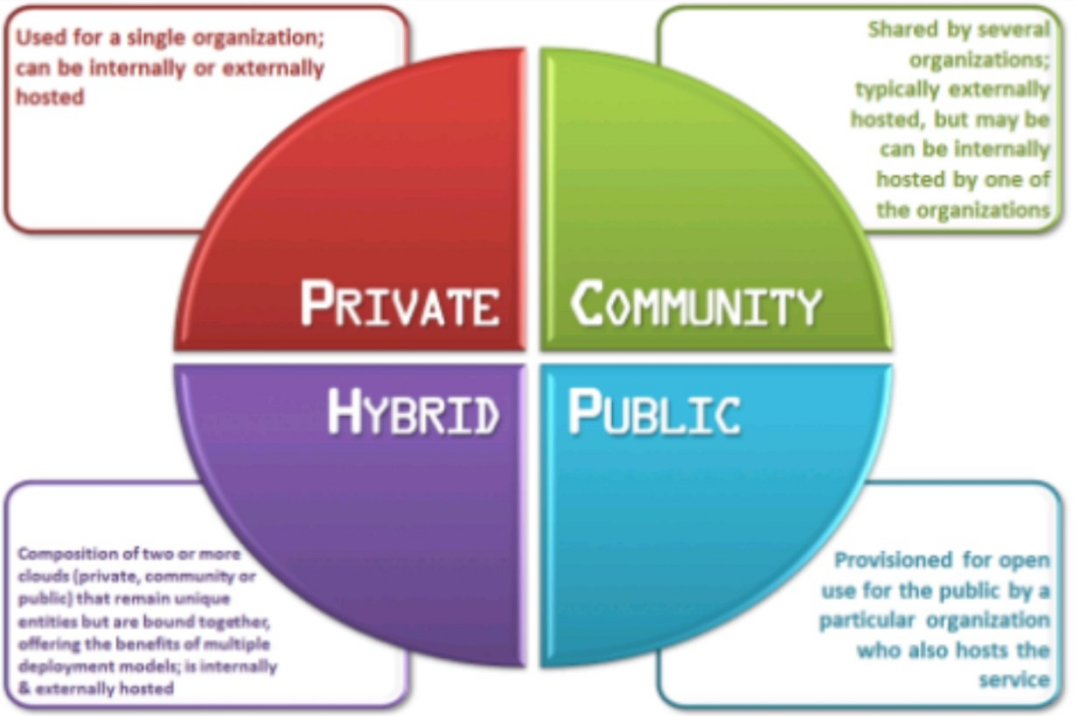


Figure 1: Cloud Deployment Models (Source: Tharak Abraham, 2013)

Cloud Service Models

Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are the three main cloud service models that offer varying degrees of abstraction and management responsibilities. According to Saraswat et al. (2020), cloud computing has transformed how businesses manage their IT resources by offering scalable and on-demand services. These approaches allow companies to concentrate on their core skills while utilizing the advantages of cloud computing, such as cost effectiveness, flexibility, and scalability. Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are shown graphically in Figure 2 in a layered hierarchy arrangement.

i. **Infrastructure as a Service (IaaS):** Virtualized computer resources are made available online through Infrastructure as a Service (IaaS). It comprises basic computing resources including networking, storage, and virtual machines. Businesses that need to manage and control their IT infrastructure but wish to avoid the cost and complexity of buying and maintaining physical servers can use Infrastructure as a Service (IaaS). IaaS allows consumers to pay just for what they use and scale resources up or down in response to demand (Darwish 2024).IaaS has many benefits, such as flexibility, scalability, and cost savings. By renting infrastructure from cloud providers, organizations can avoid upfront

capital expenses. Businesses may quickly scale resources to meet demand with this model, which is especially helpful for managing fluctuating workloads and unforeseen activity spikes.

ii. **Platform as a Service (PaaS):** With Platform as a Service (PaaS), developers can create, launch, and maintain apps without having to worry about the underlying infrastructure. PaaS enables developers to concentrate on coding and application functionality by providing middleware, operating systems, and development tools.Platform as a Service (PaaS) eliminates the need for developers to worry about the underlying infrastructure while creating, launching, and maintaining programs. Because PaaS offers operating systems, middleware, and development tools, developers can focus on coding and application functionality. This approach can help teams looking to accelerate the development process and reduce the time to market for creative apps (Sharma et al. 2023). Heroku, Google App Engine, and Microsoft Azure App Service are well-known PaaS vendors.

iii. **Software as a Service (SaaS):** Software as a Service (SaaS) is a popular model for a variety of business applications, such as CRM and collaboration tools, because of its ease of use, accessibility, and automatic updates. SaaS delivers software applications over the internet, usually on a subscription basis, eliminating the need for organizations to install and maintain software on individual machines because applications are accessed through web browsers (Rrucaj 2023).Software as a Service (SaaS) is a popular paradigm for a variety of commercial applications, such as CRM and collaboration tools, due to its ease of use, accessibility, and automatic upgrades. Because software is accessed through web browsers, SaaS eliminates the need for enterprises to install and maintain software on individual devices by delivering software programs over the internet, typically on a subscription basis (Rrucaj 2023). Google Workspace, Microsoft Office 365, and Salesforce are some of the leading SaaS vendors. Salesforce is a top CRM platform that provides marketing, sales, and customer support services.



Figure 2: Cloud Service Model

Data Security Challenges in Cloud Computing

This section lists and describes the difficulties associated with cloud computing:

Security Threats in Cloud Computing

Sensitive information may be exposed to breaches, illegal access, and cyberattacks due to the shared and remote nature of

cloud settings. This poses problems for cloud computing data security. Important problems include data breaches, insufficient encryption, loose access controls, and weaknesses in multi-tenant systems where data from multiple users may coexist. Also, cloud providers' security practices may not always align with an organization's compliance requirements, further complicating the safeguarding of data.

i. **Data Breaches**One of the biggest problems with cloud computing is still data breaches, which happen when sensitive data is accessed without authorization. Vulnerabilities in the systems of cloud service providers or insufficient security measures by users are common causes of breaches (Patel et al., 2020). Organizations may suffer financial loss, harm to their brand, and legal repercussions if sensitive data is compromised. The risk of data breaches is increased by the complexity of cloud settings, which include shared resources and multi-tenancy. Attackers frequently take advantage of misconfigurations in cloud settings to access sensitive data; improper configuration of cloud storage services can result in accidental data exposure (Singh et al., 2024). Data breaches can have long-term effects on affected organizations, such as diminished customer trust and increased regulatory scrutiny (Banerjee et al., 2023).

ii. **Insider Threats** Cloud security is seriously threatened by insider threats, which are people who work for a company and abuse their access to damage the system. These risks, which originate from workers or contractors who have access to private information, may be intentional or unintentional (Saxena et al., 2020). When workers inadvertently reveal information because of carelessness or inadequate training, this is known as an accidental insider threat. The hazards connected to these unintentional breaches can be reduced with regular training and awareness campaigns (Tariq & Miller 2024). Insider threats can be lessened by putting least privilege and role-based access control (RBAC) into practice. Organizations can lower the risk of both intentional and unintentional breaches by limiting access to only what is required for an individual's position (Lee et al., 2022).

iii. **Insecure APIs:** Cloud systems may be vulnerable to various security flaws due to insecure APIs. Attackers may target APIs, which provide communication between various software systems, if they are not well secured (Türetken& Berk 2024). Sensitive information can be accessed by unauthorized users using APIs in the absence of appropriate access restrictions (Koo et al., 2020).Security breaches can also result from flaws in API programming. Attackers can obtain unauthorized access or carry out malicious operations by taking advantage of poorly written code or unpatched vulnerabilities.

iv. **Account Hijacking:** Account hijacking is a significant risk since it allows hackers to access user accounts without authorization, which may result in data theft and system manipulation. Phishing, credential stuffing, and other methods may cause this (Otta 2023). One popular technique for account hijacking is phishing, in which perpetrators deceive victims into divulging their login information. In cloud contexts where

sensitive data access is essential, this might be very risky.Another technique for account hijacking is credential stuffing, in which hackers exploit credentials they have acquired from one breach to gain access to numerous accounts. This emphasizes the necessity of multi-factor authentication and strong, one-of-a-kind passwords. Using multi-factor authentication (MFA) can greatly improve security by preventing account hijacking.

v. **Denial of Service Attacks:** The goal of denial of service (DoS) attacks is to overload cloud services so that users cannot access them. According to Gupta et al. (2021), these attacks have the potential to seriously disrupt operations and create service failures. A more serious form of denial of service (DoS) attacks, known as distributed denial of service (DDoS) attacks, involve several computers targeting a single target. DoS and DDoS assaults take advantage of a number of vulnerabilities, such as flaws in application layers and network infrastructure. These assaults can be lessened by putting strong security measures in place, such as firewalls and rate limiting. To effectively handle possible service outages, organizations must create and update their response plans on a regular basis (Miller et al., 2023).

Cloud Security Frameworks

Cloud security frameworks and protocols are vital for safeguarding data, applications, and infrastructure in cloud environments, addressing challenges such as data protection, access control, and compliance. As cloud adoption grows, standardized approaches become essential. The Cloud Security Alliance (CSA) contributes significantly through its Cloud Controls Matrix (CCM), a cybersecurity architecture tailored for cloud systems. The National Institute of Standards and Technology (NIST) offers a comprehensive Cloud Computing Security Framework and outlines security measures in Special Publication 800-53 (NIST, 2020), applicable across government and organizational cloud platforms. Additionally, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) developed ISO/IEC 27017 (ISO, 2019), which extends ISO/IEC 27001 by providing specific cloud security guidelines and emphasizing clear contractual roles between service providers and consumers. These contributions collectively form a robust foundation for secure cloud computing practices.

Data Confidentiality, Integrity, and Availability (CIA)

A fundamental framework for guaranteeing information security in cloud systems is the CIA (Confidentiality, Integrity, and Availability) model. These three elements are the cornerstones of cloud security, directing regulations and safeguards for private information. Integrity ensures that data is accurate and consistent, availability ensures that data is available when needed, and confidentiality guarantees that only authorized people may access information. In cloud security, where data breaches can have far-reaching effects, these concepts are essential (Mishra et al., 2018).

Encryption Techniques for Data Security

A cryptographic technique called encryption transforms readable information (plaintext) into an unreadable format (ciphertext) in order to safeguard data. This conversion guarantees that without the right decryption key, unauthorized users cannot access or decipher the data. Encryption's fundamental goal is to protect data secrecy, making sure that private informationlike financial transactions, personal information, or communicationsis safe while being transmitted or stored. Pathak et al. (2024) assert that in the current digital era, encryption is crucial for safeguarding data against cyberattacks and interception.

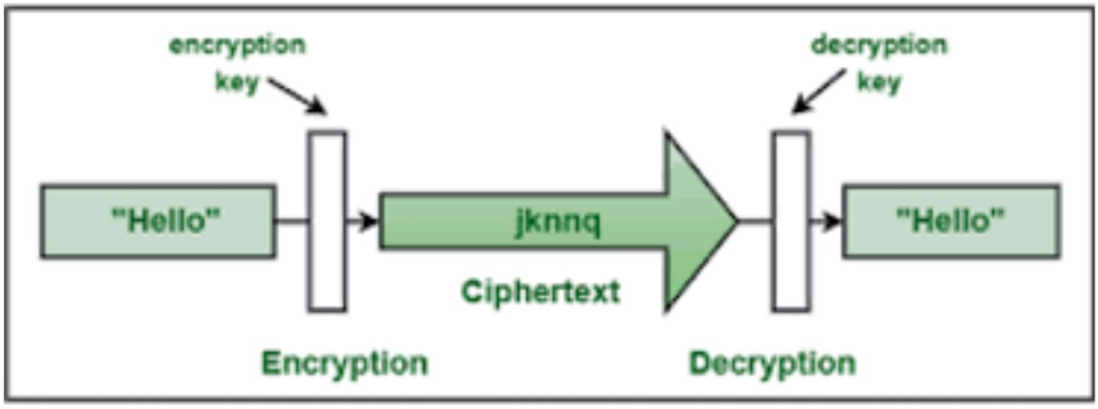


Figure 3: Cloud Service Model

Source: (Lakhichand Khushal Patil & Kalpesh A. Popat, 2024)

To hide the original data, encryption methods use mathematical calculations. Symmetric and asymmetric encryption is the two main categories. Asymmetric encryption employs two keys: a public key for encryption and a private key for decryption, whereas symmetric encryption uses a single key for both encryption and decryption.

Organizations can adhere to data privacy laws like the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) by using encryption. In order to safeguard sensitive data, these requirements mandate that firms adopt robust encryption procedures. Legal repercussions and reputational harm may arise from failing to comply. Alwin and Greyson (2024) contend that encryption is an essential legal need for guaranteeing the safe handling of financial and personal data in addition to being a technical safety measure. Symmetric encryption is one of the most used techniques for data security, according to Alenezi et al. (2020). It uses a single key for both encryption and decryption.

Secretary Bird Optimization Algorithm

This section describes the secretary bird optimization algorithm (SBOA) and provides a mathematical description of the secretary bird's behavior.

Secretary Bird Optimization Algorithm inspiration and behavior

The remarkable African raptor known as the Secretary Bird (scientific name: Sagittarius serpentarius) is well-known for its unusual look and mannerisms. It is extensively found in open riverine regions, savannas, and grasslands in Africa south of the Sahara Desert. In addition to semi-desert environments and woodland areas with open clearings, secretary birds usually live in tropical open grasslands, savannas with few trees, and open spaces with long grass. As seen in Fig. 1, secretary birds have grey-brown feathers on their wings and backs, immaculate white chests, and deep black bellies (De Swardt 2011; Hofmeyr et al. 2014).

With its long, robust legs and talons that allow it to sprint and hunt on the ground, the Secretary Bird is well known for its distinctive hunting method (Portugal et al. 2016). It usually walks or trots across grasslands, adopting the stance of a "secretary at work" by bending its head and carefully searching the ground for prey concealed in the grass. Insects, small animals, reptiles, and other prey are the main food sources for secretary birds. When they see prey, they charge at it quickly and use their razor-sharp talons to catch it. After striking the prey on the ground, they kill and eat it (Portugal et al. 2016).



Figure 4: Secretary bird (Fu *et al.,* 2024)

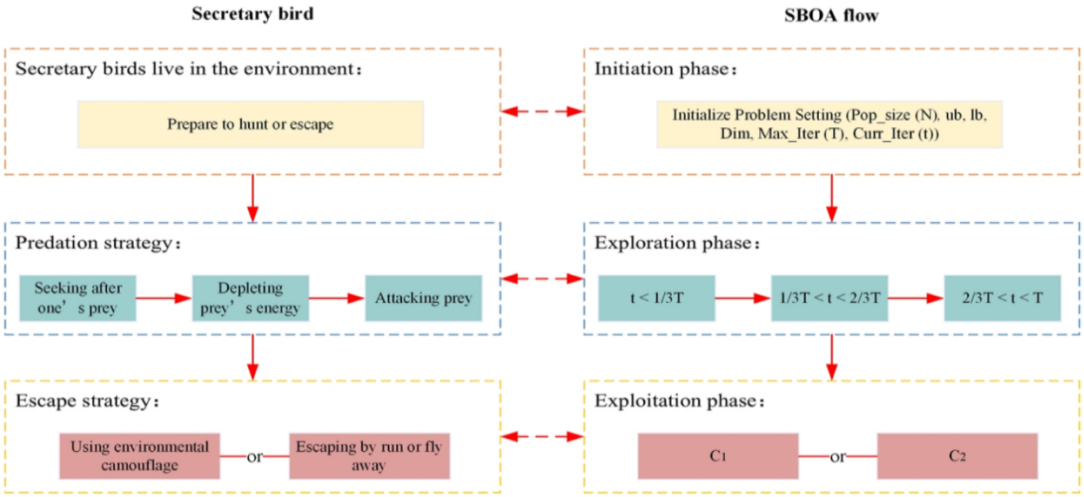


Figure 5: Secretary bird hunting and escape tactics are in line with SBOA (Fu et al., 2024).

Mathematical modeling of the secretary bird optimization algorithm

This subsection suggests that SBOA be given a mathematical model of how secretary birds naturally hunt snakes and avoid natural foes.

Initial preparation phase

Each Secretary Bird is regarded as a member of the algorithm's population in the Secretary Bird Optimization Algorithm (SBOA) method, which falls under the category of population-based metaheuristic approaches. Decision variable values are determined by each Secretary Bird's location inside the search space. As a result, the Secretary Birds' viewpoints in the SBOA technique serve as potential answers to the current issue. The placements of the Secretary Birds in the search space are randomly initialized in the first implementation of the SBOA using Eq. (2.1).

$$X_{i,j} = lb_j + r \times \left(ub_j - lb_j\right), i = 1,2,\ldots,N, j = 1,2,\ldots,\text{Dim} \qquad (2.1)$$

where X_i is the location of the i^{th} secretary bird lb_j and ub_j are the lower and upper bounds, respectively, and r is a random number between 0 and 1 .

As seen in Eq. (2.2), the secretary bird optimization algorithm (SBOA) is a population-based method in which optimization begins with a population of potential solutions. Within the upper limit (ub) and lower bound (lb) restrictions for the given problem, these candidate solutions X are created at random. In each iteration, the best solution found so far is roughly considered the optimal option.

Methodology

This study outlines a robust methodology for developing and evaluating a hybrid encryption model optimized using the Secretary Bird Optimization Algorithm (SBOA) to enhance data

security in cloud computing. The approach integrates the strengths of two symmetric key algorithms Blowfish and AES, while leveraging SBOA to optimize key scheduling and parameter selection for improved cryptographic performance. The methodology was structured into three main phases: system development, implementation, and testing. During development, a dual-layer encryption framework was designed, with Blowfish securing client-side data and AES protecting cloud-stored data. SBOA was embedded to dynamically optimize encryption keys and parameters, enhancing both speed and security.In the implementation phase, the hybrid model was deployed on cloud platforms and tested using sensitive datasets. The encryption process begins at the client's device, ensuring data is secured before transmission. SBOA plays a critical role in generating highly random and secure keys, increasing resistance to brute-force and cryptanalytic attacks. The system ensures end-to-end confidentiality by applying Blowfish encryption during data transmission and AES encryption for data at rest. Decryption occurs on the client side using SBOA-optimized keys, maintaining data integrity and confidentiality throughout the process. The mathematical formulation of the encryption and decryption processes was provided, illustrating how plaintext is transformed into ciphertext and recovered using optimized keys.

Results and Discussion

A collection of chest X-ray pictures was used to test and deploy the created Secretary Bird Optimized Hybrid AES and Blowfish encryption model for COVID-19 detection. Each of the encryption methods - AES, Blowfish, Hybrid AES–Blowfish, and Optimized Hybrid AES–Blowfish - used a total of 20 pictures, evaluating each method's performance in protecting medical photos, while preserving their quality after decryption was the key goal. Basic preprocessing procedures, like resizing and format standardization, were applied to every image to guarantee that it would work with the encryption interface. A regulated and uniform testing procedure for all four procedures was made possible by the tests being carried out in MATLAB on a personal computer setting.

Table 1: Performance Metrics of AES Algorithm

S/N	Encryption Time(s)	Execution Time(s)	Throughput	MSE	FileSize
1	35.8342	71.56514	1.022942	84.25871	73207
2	76.92051	153.6883	0.93743	59.75329	144072
3	47.68313	95.24788	0.926488	54.77678	88246
4	38.80568	77.50456	0.988639	57.16572	76624
5	12.76053	25.49184	0.89613	47.06714	22844
6	10.72622	21.41734	1.173255	44.49651	25128
7	10.79939	21.56393	1.16528	44.49651	25128
8	14.87443	29.71604	0.845604	44.49651	25128
9	4.561905	9.111992	0.877196	46.58311	7993
11	48.90427	97.68358	1.01192	63.91544	98848

S/N	Encryption Time(s)	Execution Time(s)	Throughput	MSE	FileSize
11	11.87872	23.71878	0.864673	45.83622	20509
12	10.3199	20.61216	1.003582	48.04749	20686
13	81.62309	163.0658	0.87155	70.88671	142120
14	9.535738	19.04671	0.955651	67.21144	18202
15	13.99501	27.95603	0.932035	64.04633	26056
16	14.23734	28.40944	1.030186	72.80067	29267
17	10.97007	21.90775	1.067659	76.36821	23390
18	10.12105	20.21407	0.900462	67.21144	18202
19	6.932673	13.8484	0.931732	63.64636	12903
20	28.42466	56.75091	1.006786	74.62669	57136

The table above reveals that the AES algorithm exhibited reliable encryption performance across twenty chest X-ray images, with encryption and execution times closely tied to image file sizesmaller images processed in as little as 4.56 seconds, while larger ones took up to 81.62 seconds. Execution times ranged from 9.11 to 163.06 seconds, confirming that AES scales predictably with input size. Throughput values varied between 0.84 and 1.17 MB/s, with smaller images achieving higher rates, highlighting AES's fluctuating efficiency based on data volume and complexity. Mean squared error (MSE) values ranged from 44.49 to 84.25, indicating moderate distortion during encryption but preserving visual integrity across all samples. Overall, AES proved to be a robust and scalable encryption method suitable for secure medical imaging applications.

Table 2: Performance Metrics of Blowfish Algorithm

S/N	Encryption Time (s)	Execution Time (s)	Throughput	MSE	File Size (bytes)
1	70.63624	105.7807	0.692064	168.5174	73207
2	141.9517	212.6322	0.677564	119.5066	144072
3	92.50156	138.4396	0.637433	109.5536	88246
4	90.86252	136.1604	0.562748	114.3314	76624
5	20.9763	31.40302	0.727446	94.13427	22844
6	25.6899	38.48263	0.65297	88.99302	25128
7	51.78137	77.56876	0.653781	78.52801	50713
8	63.38421	94.96063	0.574217	138.0717	54528
9	6.783159	10.15605	0.787019	93.16621	7993
10	83.62567	125.2334	0.78931	127.8309	98848
11	21.69213	32.46947	0.63164	91.67245	20509
12	23.51782	35.20528	0.587582	96.09497	20686
13	137.8168	206.1405	0.689433	141.7734	142120
14	21.36305	31.99198	0.568955	134.4229	18202
15	29.26596	43.81403	0.594695	128.0927	26056
16	26.98226	40.39857	0.724456	145.6013	29267
17	21.62433	32.34681	0.723101	152.7364	23390

S/N	Encryption Time (s)	Execution Time (s)	Throughput	MSE	File Size (bytes)
18	12.46721	18.66782	0.669708	205.5625	12502
19	60.74623	90.94502	0.689186	154.0466	62678
20	61.66466	92.24642	0.679463	154.0466	62678

The table above reveals that blowfish algorithm exhibited considerable variability in encryption and execution times when tested on 20 chest X-ray images, with processing durations strongly influenced by file size. Smaller images encrypted in as little as 6.78 seconds, while larger ones took up to 141.95 seconds, and execution times ranged from 10.15 to 212.63 seconds, indicating slower performance compared to AES, especially for high-resolution files. Throughput values were generally lower, between 0.56 and 0.78 MB/s, reflecting slower data handling, though performance remained stable for medium-sized images. MSE values ranged from 78.52 to 205.56, suggesting greater distortion between original and decrypted images than AES, yet without compromising visual integrity essential for medical diagnostics. Overall, Blowfish provided robust security but with trade-offs in speed and reconstruction accuracy.

Table 3: Performance Metrics of Hybrid AES–Blowfish Algorithm

S/N	Encryption Time (s)	Execution Time (s)	Throughput	MSE	File Size (bytes)
1	14.0544	28.0498	2.6099	39.4098	73207
2	23.4755	46.7242	3.0835	27.0731	144072
3	12.6081	25.0009	3.5297	24.705	88246
4	13.8455	27.499	2.7864	25.874	76624
5	3.4287	6.827	3.3461	20.8375	22844
6	3.8839	7.7321	3.2498	19.533	25128
7	9.1625	18.2298	2.7819	16.7783	50713
8	8.4125	16.7454	3.2563	31.8488	54528
9	1.2657	2.5127	3.1811	20.5726	7993
10	12.2273	24.2199	4.0813	29.1513	98848
11	3.0045	5.9632	3.4393	20.081	20509
12	3.1232	6.1885	3.3427	21.3895	20686
13	26.6197	52.8321	2.69	32.7932	142120
14	2.3952	4.7519	3.8304	30.8856	18202
15	3.2463	6.4288	4.053	29.3582	26056
16	4.4094	8.7415	2.6757	35.5851	23390
17	3.1191	6.2031	3.4967	31.2245	21690
18	2.9329	5.7919	4.0242	34.8754	23308
19	3.7771	7.5029	3.0916	33.5706	23196
20	2.5383	5.059	2.5505	29.0869	12903

The table above reveals that the Hybrid AES–Blowfish algorithm demonstrated a balanced performance across encryption time, execution time, throughput, and mean squared error (MSE) when applied to twenty X-ray images. Encryption times ranged from 1.2657 to 26.6197 seconds, generally increasing with file size, though some smaller files showed moderate delays due to the algorithm's complexity. Execution times followed a similar pattern, peaking at 52.8321 seconds for larger files, reflecting the dual-layer encryption overhead, yet remaining

efficient for smaller images. Throughput values, spanning 2.5505 to 4.0813 MB/s, indicated strong processing capability, especially for medium-sized files. MSE values between 16.7783 and 39.4098 confirmed effective image distortion for security, with higher values signifying stronger encryption impact. Overall, the hybrid algorithm successfully balanced speed, security, and image fidelity, making it suitable for secure medical imaging applications.

Table 4: Performance Metrics of Optimized AES–Blowfish Algorithm

S/N	Encryption Time (s)	Execution Time (s)	Throughput	MSE	File Size (bytes)
1	2.1786	4.3457	5.2567	16.6512	22844
2	2.3709	4.7286	5.314	15.5956	25128
3	4.3474	8.6758	5.8454	13.4304	50713
4	3.1739	6.3104	8.0364	13.4799	50713
5	0.5166	1.0315	7.7486	16.586	7993
6	8.2425	16.4229	6.0189	23.3878	98848
7	1.9752	3.9382	5.2078	16.0933	20509
8	1.762	3.5144	5.8861	17.0772	20686
9	12.7047	25.3397	5.6086	26.2187	142120
10	1.7306	3.4569	5.2654	24.8079	18202
11	1.948	3.8773	6.7201	23.3417	26056
12	2.0061	4.0051	7.3075	26.8405	29267
13	1.5211	3.0354	7.7057	28.4216	23390
14	1.8229	3.6328	5.9707	24.923	21690
15	1.4863	2.9632	7.8658	27.9776	23308
16	1.7317	3.4504	6.7227	26.7478	23196
17	2.1557	4.3042	5.3826	26.2594	23168
18	1.8956	3.7758	7.0264	28.0914	26530
19	3.8858	7.7379	8.1002	28.6114	62678
20	4.2209	8.4193	7.4445	28.6138	62678

The table above reveals that the performance evaluation of the Optimized AES–Blowfish Algorithm (SBOA) revealed its superior efficiency and reliability across key parameters such as encryption time, execution time, throughput, and mean squared error (MSE). Encryption times ranged from 0.5166 to 12.7047 seconds, with faster speeds observed for smaller image files, indicating a direct correlation between file size and processing time. Execution times followed a similar trend, mostly staying under 5 seconds, demonstrating the algorithm's suitability for time-sensitive applications like medical imaging. Throughput values ranged from 5.2078 to 8.1002 MB/s, with higher rates for smaller files, reflecting SBOA's robust data handling capacity. MSE values remained within an acceptable range (13.4304 to 28.6138), ensuring high image fidelity post-encryption. When compared to AES, Blowfish, and the Hybrid AES–Blowfish algorithm, SBOA consistently outperformed them in speed and throughput, while also maintaining lower MSE values. These results affirm SBOA's effectiveness in balancing computational efficiency and security, making it ideal for real-time and large-scale encryption tasks.

Overall, the comparison clearly establishes SBOA as the most efficient and reliable algorithm among the four. Its combination of minimal encryption and execution times, highest throughput, and lowest MSE values makes it well-suited for applications requiring both speed and accuracy. While AES and Blowfish offer strong security foundations, they are hindered by slower processing. The Hybrid AES–Blowfish offers a balance between the two, but SBOA's optimization strategies deliver a marked improvement in performance. This positions SBOA as the optimal choice for scenarios where computational efficiency and low error rates are critical.

Table 5: Mean Performance Metrics of the Four Encryption Algorithms

Algorithm	Mean Encryption Time (s)	Mean Execution Time (s)	Mean Throughput (MB/s)
AES	24.9954	49.926	0.9705
Blowfish	53.2667	79.7522	0.6656
Hybrid AES–Blowfish	7.8765	15.6502	3.255
Optimized AES–Blowfish	3.1791	6.3386	6.4905

Discussion of Finding's

This study compared the encryption performance of AES, Blowfish, Hybrid AES–Blowfish, and the Optimized AES–Blowfish Algorithm (SBOA) across twenty samples. AES demonstrated moderate encryption times, balancing speed and security through its efficient key scheduling, though performance varied with input complexity. Blowfish, while offering strong cryptographic robustness, showed the highest encryption times due to its complex key setup and multiple encryption rounds, making it less suitable for time-sensitive applications. The Hybrid AES–Blowfish algorithm significantly reduced encryption times by combining AES's speed with Blowfish's security, though it still exhibited some variability. SBOA outperformed all other methods, achieving the lowest encryption times and highest efficiency, thanks to targeted optimization techniques that streamline processing and reduce overhead.These findings are reinforced by existing literature, which highlights the complementary strengths of AES and Blowfish and supports hybrid approaches for improved performance. Studies confirm that AES generally encrypts faster, while Blowfish excels in specific contexts like text-based or resource-constrained environments. Hybrid models, especially those optimized like SBOA, align with the broader research trend of enhancing encryption systems to meet the demands of real-time and large-scale data security. SBOA's consistent reduction in encryption time without compromising security validates the effectiveness of algorithmic optimization and hybridization, offering a promising direction for future cryptographic development.

Conclusion

This study evaluated the performance of four encryption techniques AES, Blowfish, Hybrid AES–Blowfish, and the Optimized AES–Blowfish Algorithm (SBOA) across metrics such as encryption time, execution time, throughput, and image reconstruction quality. The findings revealed that SBOA significantly outperforms the others, offering the fastest processing and highest throughput without compromising security, making it well-suited for real-time and large-scale applications. The hybrid AES–Blowfish method also demonstrated notable improvements over individual algorithms, suggesting that combining encryption methods can effectively balance speed and robustness. While AES and Blowfish remain reliable, their slower speeds and lower throughput limit their efficiency in demanding environments. The study further emphasized that encryption performance is influenced by input data characteristics like file size and complexity, though all algorithms maintained acceptable image reconstruction quality.

Recommendations

The Optimised AES–Blowfish Algorithm (SBOA) is suggested for future encryption implementations in high-performance environments based on the study's findings since it offers better speed and throughput without compromising security. To increase efficiency, businesses that handle a lot of sensitive data, including financial institutions and healthcare providers, should look at combining hybrid and optimal encryption solutions. Additionally, further research should be conducted to refine optimization methods and explore their impact on other types of data and real-world applications. It is also advised to investigate hardware acceleration and parallel processing approaches to further improve encryption and decryption speeds.

Contributions to Knowledge

By introducing the Secretary Bird Optimization Algorithm (SBOA) with hybrid AES and Blowfish cryptography, the study significantly advances the field of data security. In contrast to traditional AES or Blowfish models, the created system makes use of SBO's exploration–exploitation balance to improve the scheduling and substitution of encryption keys, strengthening defenses against cryptanalytic and brute force attacks. AES and Blowfish hybridization guarantees a synergy between the computational efficiency of Blowfish and the strong security of AES, improving performance across a number of evaluation metrics like lower mean square error, higher throughput, and shorter encryption and execution times.

REFERENCES

Adebayo, A., Adeniyi, A. E., Ajao, J., Isiaka, R., Gbolagade, K., & Abdulsalam, S. (2024). *Development of a Multi-Level Data Encryption Standard with Residue Number System for Data Security*. In Conference Organising Committee (p. 14).

Adee, R., & Mouratidis, H. (2022). *A dynamic four-step data security model for data in cloud computing based on cryptography and steganography*. Sensors, 22(3), 1109.

Ahmad, N., Hoda, N., &Alahmari, F. (2020). *Developing a cloud-based mobile learning adoption model to promote sustainable education*. Sustainability, 12(8), 3126.

Alam, I., Sharif, K., Li, F., Latif, Z., Karim, M. M., Biswas, S., ... & Wang, Y. (2020). A survey of network virtualization techniques for Internet of Things using SDN and NFV. *ACM Computing Surveys (CSUR)*, 53(2), 1-40.

Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric encryption algorithms: Review and evaluation study. *International Journal of Communication Networks and Information Security,* 12(2), 256-272.

Almadani, M. S., Alotaibi, S., Alsobhi, H., Hussain, O. K., & Hussain, F. K. (2023). Blockchain-based multi-factor authentication: A systematic literature review. *Internet of Things*, 23, 100844.

Al-Saadi, S. S., & Al-Muthanna, A. H. (2023). Performance analysis of a hybrid security algorithm. *Technium Science,* 11, 72–86. https://doi.org/10.47577/technium-science.v11i.123

Alwin, G. (2024). *Balancing Cryptography, Privacy, and Individual Freedom: A Comparative Study of OECD Guidelines and Islamic Legal Principles.*

Arora, S., Singh, M., & Sood, M. (2025). *Augmented secretary bird optimization algorithm for wireless sensor network deployment.* PLOS ONE, 20(8), e0329705. https://doi.org/10.1371/journal.pone.0329705

Banerjee, S., Barik, S., Das, D., & Ghosh, U. (2023). *EHR security and privacy aspects: A systematic review*. In IFIP International Internet of Things Conference (pp. 243-260). Cham: Springer Nature Switzerland.

Bongiovanni, I., Renaud, K., Brydon, H., Blignaut, R., & Cavallo, A. (2022). A *quantification mechanism for assessing adherence to information security governance guidelines. Information & Computer Security*, 30(4), 517-548.

Darwish, D. (Ed.). (2024*). Emerging trends in cloud computing analytics, scalability, and service models.*

Dauda, M., & Abubakar, A. (2023).Secretary Bird Optimization Algorithm: A novel bio-inspired metaheuristic for global optimization*. Journal of Computational Intelligence and Neuroscience.

De Swardt DH (2011). *Late-summer breeding record for Secretary birds Sagittarius serpentarius in the free state*. Gabar 22:31–33

Fu, Y., Liu, D., Chen, J., & He, L. (2024). *Secretary bird optimization algorithm: a new metaheuristic for solving global optimization problems*. Artificial Intelligence Review, 57(5), 123.

Gade, K. R. (2020). *Data governance and risk management: Mitigating data-related threats. advances in computer sciences*, 3(1).

George, A. S., George, A. H., & Baskar, T. (2023). Edge computing and the future of cloud computing: A survey of industry perspectives and predictions. *Partners Universal International Research Journal*, 2(2), 19-44.

Gholami, B., Dasgupta, S., Uustalu, T., Gerndt, M. (2024). *Economy-based greedy bidding for resources for CAE Workflows in hybrid cloud infrastructure*. In 2024 IEEE 20th International Conference on e-Science (e-Science) (pp. 1-7). IEEE.

Gupta, B. B., & Dahiya, A. (2021). *Distributed Denial of Service (DDoS) attacks: classification, attacks, challenges and countermeasures*. CRC press.

Gupta, I., Singh, A. K., Lee, C. N., &Buyya, R. (2022). *Secure data storage and sharing techniques for data protection in cloud environments:* A systematic review, analysis, and future directions. IEEE Access, 10, 71247-71277.

Hofmeyr SD, Symes C. T, Underhill L. G (2014) *Secretarybird Sagittarius serpentarius population trends and ecology: Insights from South African citizen science data*. PLoS ONE 9:e96772

Iting, R. L., Isahac, L. M., Ajuram, M. J., Kimar, J. D., Awad, S. A., Salahuddin, D., & Latorre, N. J. (2024). *Understanding the critical role of information assurance in mitigating cybercrime risks.*

Kansal, M., Singh, P., Singh, M. K., & Varshney, S. (2023). *A systematic study of services and security model in cloud computing: A brief overview*. Convergence of Cloud Computing, AI, and Agricultural Science, 1-16.

Katal, A., Dahiya, S., & Choudhury, T. (2023). *Energy efficiency in cloud computing data centers: a survey on software technologies*. Cluster Computing, 26(3), 1845-1875.

Koo, J., Oh, S. R., Lee, S. H., & Kim, Y. G. (2020). *Security architecture for cloud-based command and control system in IoT environment*. Applied Sciences, 10(3), 1035.

Kumar, M., Sharma, S. C., Goel, A., & Singh, S. P. (2019). A comprehensive survey for scheduling techniques in cloud computing. *Journal of Network and Computer Applications*, 143, 1-33.

Kumar, R., & Singh, A. (2024). Hybrid cryptographic approach for data security in IoT devices. *International Journal of Computer Network and Information Security*, 16(2), 51 - 60.

Lee, J., de Guzman, M. C., Wang, J., Gupta, M., & Rao, H. R. (2022). *Investigating perceptions about risk of data breaches in financial institutions: A routine activity-approach*. Computers & Security, 121, 102832.

Li, Z., Liu, X., Wang, W. M., VatankhahBarenji, A., & Huang, G. Q. (19). *CKshare: secured cloud-based knowledge-sharing blockchain for injection mold redesign*. Enterprise Information Systems, 13(1), 1-33.

Liu, G., Lin, W., Zhang, H., Lin, J., Peng, S., & Li, K. (2025). *Public datasets for cloud computing: A comprehensive survey*. ACM Computing Surveys, 57(8), 1-38.

Ma, S., Li, J., Li, J., & Xie, M. (2024). *Cloud-integrated cyber–physical systems: Reliability, performance and power consumption with shared-servers and parallelized services.* Frontiers of Engineering Management, 1-19.

Mallo, S. F., Abdulqader, D. M., Abdullah, R. M., Ismael, H. R., Rashid, Z. N., & Sami, T. M. G. (2024). A review on feasibility of web technology and cloud computing for sustainable ES: leveraging AI, IoT, and security for green operations. *Journal of Information Technology and Informatics,* 3 (2).

Martínez Guevara, L. M., Vidal, P. J., Olivera, A. C., & Millán, E. N. (2024). Analysis and comparison of encryption and verification algorithms applied to a fog computing architecture. *Journal of Information and Telecommunication*, 1-17.

Miller, F. A., & Davis-Howard, V. (2023). It is time for organizations to take a leap forward. *Organization Development Journal,* 41(3).

Mishra, A. A., Surve, K., Patidar, U., &Rambola, R. K. (2018). *Effectiveness of confidentiality, integrity and availability in the security of cloud computing: A review.* In 2018 4th International Conference on Computing Communication and Automation (ICCCA) (pp. 1-5). IEEE.

NIST (2020) Cybersecurity and Privacy Annual Report: https://www.nist.gov/

Otta, S. P., Panda, S., Gupta, M., & Hota, C. (2023). *A systematic survey of multi-factor authentication for cloud infrastructure*. Future Internet, 15(4), 146.

Patel, A., Shah, N., Ramoliya, D., & Nayak, A. (2020). *A detailed review of cloud security: issues, threats & attacks*. In 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA) (pp. 758-764). IEEE.

Pathak, M., Mishra, K. N., & Singh, S. P. (2024). *Data security and privacy preservation in cloud-based IoT technologies: An analysis of risks and the creation of robust countermeasures*. Recent Advances in Computer Science and Communications.

Ponnusamy, A., & Spanner, A. (2023). *Technology operating models for cloud and edge: create your purpose-built distributed operating model for public, hybrid, multicloud, and edge*. Packt Publishing Ltd.

Portugal SJ, Murn CP, Sparkes EL, Daley MA (2016). *The fast and forceful kicking strike of the secretary bird.* Curr Biol 26:R58–R59

Prasad, V. K., Dansana, D., Bhavsar, M. D., Acharya, B., Gerogiannis, V. C., & Kanavos, A. (2023). *Efficient resource utilization in IoT and cloud computing. Information*, 14(11), 619.

Rani, R., & Kaur, J. (2025). Comparative analysis and performance evaluation of cryptographic algorithms. *International Journal of Enhanced Research in Science, Technology & Engineering*, 13(12).

Rao, V., & Prema, K. V. (2021). A review on lightweight cryptography for Internet-of-Things based applications. *Journal of Ambient Intelligence and Humanized Computing*, 12(9), 8835-8857.

Rauf, A., Tariq, U., Tang, H., & Shishir, M. A. (2024). *Bibliometric analysis: research trends of privacy in big data and its applications.* In 2024 7th International Conference on Data Science and Information Technology (DSIT) (pp.1-6). IEEE.

Ravikumar, D., Yeo, A., Zhu, Y., Lakra, A., Nagulapalli, H., Ravindran, S. K., & Krishnan, S. (2024*). Intelligent pooling: proactive resource provisioning in large-scale cloud service.*arXiv preprint arXiv:2411.11326.

Rrucaj, A. (2023). *Creating and sustaining competitive advantage in the software as a service (SaaS) Industry: best practices for strategic management*.

Salman, Z., Alomary, A., & Hammad, M. (2024). A secure cloud framework for big data analytics using a distributed model. *International Journal of Computing and Digital Systems,* 15(1), 1-11.

Sana, M. U., Li, Z., Javaid, F., Liaqat, H. B., & Ali, M. U. (2021). *Enhanced security in cloud computing using neural network and encryption*. IEEE Access, 9, 145785-145799.

Saraswat, M., & Tripathi, R. C. (2020). *Cloud computing: analysis of top 5 CSPs in SaaS, PaaS and IaaS platforms*. In 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART) (pp. 300-305). IEEE.

Sasikumar, K., & Nagarajan, S. (2024). *Comprehensive review and analysis of cryptography techniques in cloud computing*. IEEE Access.

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K R., & Burnap, P. (2020). *Impact and key challenges of insider threats on organizations and critical businesses*. Electronics, 9(9), 1460.

Shakor, M. Y., Khaleel, M. I., Safran, M., Alfarhood, S., & Zhu, M. (2024). *Dynamic AES encryption and block chain key management: a novel solution for cloud data security*. IEEE Access, 12, 26334-26343.

Sharma, M., Gupta, R., & Acharya, P. (2023). Adoption and forecasting of technology: modeling the dynamics of cloud adoption using a system approach. *Journal of Enterprise Information Management*, 36(6), 1647-1676.

Sharma, P., Jindal, R., & Borah, M. D. (2020). *Blockchain technology for cloud storage: A systematic literature review*. ACM Computing Surveys (CSUR), 53(4), 1-32.

Singh, M. M. K., Chandna, M., &Kongala, V. Y. Y. (2024). *Risk management framework for cloud migration and selection of suitable cloud service provider*. Advances in Enterprise Technology Risk Assessment, 283.

Sunyaev, A., &Sunyaev, A. (2020). *Cloud computing. Internet computing: Principles of distributed systems and emerging internet-based technologies,* 195-236.

Tariq, Miller, U. (2024). *Data breach incidents and prevention in the hospitality industry. In* Corporate Cybersecurity in the Aviation, Tourism, and Hospitality Sector (pp. 181-199). IGI Global.

Türetken, &Berk. (2024). *Enhancing security with cloud-based API management: Best practices and implementation.*

Wang, X., Ren, X., Qiu, C., Cao, Y., Taleb, T., & Leung, V. C. (2020). *Net-in-AI: A computing-power networking framework with adaptability, flexibility, and profitability for ubiquitous AI.* IEEE Network, 35(1), 280-288.

Yang, X., Zhou, D., Liu, S., Ye, J., & Wang, X. (2022). *Deep model reassembly: Advances in neural information processing systems,* 35, 25739-25753.